Cadernos NIC.br
Estudos Setoriais

SEGURANÇA DIGITAL:
uma análise de gestão de risco em empresas brasileiras

nic.br
Núcleo de Informação e Coordenação do Ponto BR

Núcleo de Informação
e Coordenação do Ponto BR – NIC.br

Cadernos NIC.br
Estudos Setoriais

SEGURANÇA DIGITAL:
uma análise de gestão de risco em empresas brasileiras

Comitê Gestor da Internet no Brasil – CGI.br
São Paulo 2020

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Segurança digital : uma análise da gestão de riscos em empresas brasileiras [livro eletrônico] / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2020.
PDF Bibliografia
ISBN 978-65-86949-20-9
1. Computadores - Medidas de segurança 2. Gestãode risco 3. Internet -Legislação - Brasil 4. Mídiadigital 5. Proteção de dados 6. Tecnologia da informação I. Núcleo de Informação e Coordenação do Ponto BR..

20-43419 CDD-658.478

Índices para catálogo sistemático:

1. Gestão de riscos : Segurança digital 658.478
Maria Alice Ferreira - Bibliotecária - CRB-8/7964

Comitê Gestor da Internet no Brasil – CGI.br

(EM DEZEMBRO DE 2020)

COORDENADOR

Marcio Nobre Migon

CONSELHEIROS

Beatriz Costa Barbosa
Cláudio Benedito Silva Furtado
Demi Getschko
Domingos Sávio Mota
Evaldo Ferreira Vilela
Franselmo Araújo Costa
Heitor Freire de Abreu
Henrique Faulhaber Barbosa
José Alexandre Novaes Bicalho
Laura Conde Tresca
Leonardo Euler de Morais
Luis Felipe Salin Monteiro
Marcos Dantas Loureiro
Maximiliano Salvadori Martinhão
Nivaldo Cleto
Percival Henriques de Souza Neto
Rafael De Almeida Evangelista
Rafael Henrique Rodrigues Moreira
Rosauro Leandro Baretta
Tanara Lauschner

SECRETÁRIO EXECUTIVO

Hartmut Richard Glaser

SUMÁRIO

13 **APRESENTAÇÃO –** *Demi Getschko*

19 **PRÓLOGO –** *Laurent Bernat*

35 **CAPÍTULO 1 –** A nova agenda de cibersegurança: desafios econômicos e sociais para uma Internet segura. *Johannes M. Bauer e William H. Dutton*

65 **CAPÍTULO 2 –** Gestão de riscos cibernéticos para pequenas e médias empresas. *Éireann Leverett*

101 **CAPÍTULO 3 –** Onde investir para reduzir o risco: um retrato a partir dos incidentes de segurança reportados e dos dados de sensores e fontes externas agregados pelo CERT.br. *Cristine Hoepers*

129 **CAPÍTULO 4 –** Segurança digital e gestão de riscos: uma análise de empresas brasileiras. *Stefania L. Cantoni, Leonardo M. Lins e Tatiana Jereissati*

171 **CONCLUSÕES –** Contexto regional da segurança cibernética. *Georgina Núñez e Jorge Alejandro Patiño*

AGRADECIMENTOS

O Núcleo de Informação e Coordenação do Ponto BR (NIC.br), por meio do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), agradece a todos os profissionais envolvidos na presente publicação. Especialmente, agradecemos a contribuição de Laurent Bernat, da Organização para a Cooperação e Desenvolvimento Econômico (OCDE); de Johannes M. Bauer, do Centro Quello da Michigan State University, e William H. Dutton, do Oxford Internet Institute da Oxford Martin School; do pesquisador Eireann Leverett, do Centre for Risk Studies, da University of Cambridge; e de Georgina Núñez e Jorge Alejandro Patiño, da Comissão Econômica para a América Latina e o Caribe (Cepal).

Agradecemos à equipe do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br|NIC.br), que também contribuiu para esta publicação.

APRESENTAÇÃO

Adotada no dia-a-dia para as mais diversas aplicações, a Internet tem experimentado um crescimento vigoroso em todos os setores da sociedade brasileira na última década, em grande medida devido à sua infraestrutura de rede ser muito atraente para indivíduos, organizações e governos. Especificamente no campo das aplicações corporativas e domésticas (Internet das Coisas – IoT), também há um desenvolvimento notável, o que traz inúmeros benefícios tanto para as empresas como para os indivíduos.

Do ponto de vista social e econômico, devemos celebrar que há cada dia mais pessoas utilizando a rede, fato bastante benéfico para a sociedade como um todo. No entanto, tal expansão torna seu uso cada vez mais complexo, incluindo sua associação a diversas ameaças de riscos digitais e possíveis incidentes de segurança, tendência que envolve dispositivos conectados à Internet e que, em alguma medida, torna seus usuários mais vulneráveis.

Ainda que soluções técnicas possam mitigar os riscos de vulnerabilidade, naturais em qualquer ambiente de rede descentralizado e aberto, elas não bastam para que essas questões sejam resolvidas. Nesse contexto, faz-se antes necessário separar o que é a Internet em si do que são as aplicações que se apoiam sobre a rede.

Dessa forma, precisamos observar os impactos dos diferentes tipos de ameaças digitais, para que possamos desenvolver uma cultura da segurança que enfrente esses riscos. Embora, por exemplo, o uso de criptografia na camada de aplicações seja uma forma de a tecnologia tornar a comunicação via rede mais segura, ela não é suficiente: muitos incidentes de segurança têm origem em uma "engenharia social" que explora vulnerabilidades do comportamento humano.

Educar os usuários da rede nas boas normas de conduta é, portanto, componente importante na busca de soluções que minimizem as consequências dos riscos digitais. Ao mesmo tempo, é fundamental preservarmos e mantermos os princípios originais de abertura, colaboração e cooperação, presentes desde a criação da rede e que a tornaram uma infraestrutura tão atraente para a miríade de aplicações que hoje suporta.

O Comitê Gestor da Internet no Brasil (CGI.br) debateu, adotou e publicou, em 2009, os Princípios para a Governança e Uso

da Internet no Brasil, também voltados a embasar e a orientar suas ações e decisões. Um dos princípios, em particular, recomenda que a estabilidade, a segurança e a funcionalidade globais da rede sejam preservadas de forma ativa, por meio de medidas técnicas compatíveis com os padrões internacionais e do estímulo ao uso das boas práticas de segurança. São pontos que devem ser observados por todos aqueles conectados à rede.

A segurança digital é fator instrumental na preservação de direitos humanos, como privacidade e liberdade de expressão, além de ser fundamental para o bom funcionamento da rede e de toda a cadeia envolvida, desde sua infraestrutura de acesso e de serviços, até aplicações nela apoiadas.

No âmbito das empresas, esse tema tem se intensificado com o debate público sobre a digitalização da economia, sobretudo a partir da aprovação de novas leis e da definição de estratégias nacionais e setoriais. A Estratégia Brasileira para a Transformação Digital (E-Digital), por exemplo, reforça o sentido de urgência no processo de transformação digital que engloba governo, setor privado e sociedade, e que considera a confiança no ambiente digital um de seus eixos habilitadores.

Outro fator que aumentou a relevância do debate sobre segurança digital foi a crise desencadeada pela COVID-19. A pandemia evidenciou ainda mais a importância das tecnologias digitais, tornando a Internet uma infraestrutura essencial para as empresas, suas operações logísticas e comerciais, além de propiciar um aumento notável na demanda de teletrabalho. Por conseguinte, à medida que a conectividade se torna cada vez mais crítica para o funcionamento das empresas, a segurança digital para todo o conjunto de dispositivos, *software*, práticas e normas mostra-se um ativo crucial, voltado a mitigar incidentes de segurança e suas consequências que, em muitos casos, são de difícil recuperação.

Nesse cenário, a presente publicação da série de Cadernos NIC.br de Estudos Setoriais busca endereçar questões ligadas à gestão de incidentes de segurança e aos riscos digitais. O tema abordado está alinhado às estratégias do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), em prol do desenvolvimento da Internet no país, produzindo e difundindo indicadores sobre as tecnologias de informação e comunicação (TIC) que sirvam para apoiar políticas públicas no tema da segurança digital, bem como na ampliação do debate sobre o assunto.

Desenvolvida conjuntamente pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) e pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), esta publicação originou-se na cooperação do NIC.br com a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), em força-tarefa dirigida à elaboração de um instrumento para medição das práticas de gestão de riscos digitais nas empresas. Os cinco capítulos apresentam diferentes temas: os desafios econômicos e sociais para uma Internet segura; o cenário de incidentes de segurança no Brasil; a gestão de riscos digitais para as empresas; um estudo qualitativo sobre riscos digitais em empresas brasileiras; e uma proposta de agenda para políticas públicas. A partir dessas discussões, esperamos contribuir com sólidos indicadores sobre segurança digital e suas implicações para as empresas.

Finalmente, desejamos que o modelo multissetorial de governança protagonizado pelo CGI.br possa ser inspirador para o engajamento das múltiplas partes interessadas nessa discussão, tanto para que se enfrentem as ameaças de segurança digital, quanto para a observância de boas práticas na gestão de risco de segurança digital.

Boa leitura!

Demi Getschko
Núcleo de Informação e Coordenação do Ponto BR — NIC.br

PRÓLOGO

Laurent Bernat[1]

1 Laurent Bernat é analista de políticas no Secretariado da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) na Divisão de Política de Economia Digital. Ele lidera a equipe de apoio ao Grupo de Trabalho sobre Segurança na Economia Digital (SDE), no âmbito do Comitê sobre Políticas de Economia Digital (CDEP). Ele liderou o desenvolvimento das Recomendações da OCDE sobre Gestão de Risco de Segurança Digital para a Prosperidade Econômica e Social (2015) e sobre Segurança Digital de Atividades Críticas (2019). Atualmente, ele também lidera o Fórum Global da OCDE sobre Segurança Digital para a Prosperidade e coordena o trabalho de políticas sobre segurança digital de produtos, tratamento de vulnerabilidade e "resposta responsável" por atores privados. Antes de ingressar na OCDE em 2003, ele trabalhou na agência francesa de proteção de dados, a Commission nationale de l'informatique et des libertés (CNIL), e foi diretor associado em uma empresa de consultoria em Internet. Laurent é mestre em Ciência Política e Relações Internacionais.

Ao longo das últimas três décadas, preocupações com a segurança digital têm evoluído desde questões técnicas até se tornarem uma prioridade-chave para tomadores de decisão de governos e organizações. Entretanto, o que é a segurança digital e quais são os principais desafios para formuladores de políticas e outras partes interessadas? Este prólogo apresenta uma introdução abrangente dos desafios às políticas nesse campo, sob o ponto de vista econômico e social. O texto começa com uma discussão sobre o escopo e o significado da segurança digital em comparação com a cibersegurança. Em seguida, apresenta os fundamentos do risco de segurança digital e a gestão de risco de segurança digital, com a introdução de alguns dos principais desafios no tocante às políticas de segurança digital para governos.

SEGURANÇA DIGITAL OU CIBERSEGURANÇA?

O primeiro desafio relativo ao tema da segurança digital talvez seja a terminologia nessa área. O termo "cibersegurança" tem sido utilizado para se referir a qualquer elemento associado aos perigos de se usar as tecnologias de informação e comunicação (TIC): desde roubos *on-line* até possíveis conflitos armados que ocorrem no "domínio cibernético", espionagem, exércitos de *trolls* que desestabilizam eleições ou disseminam *fake news* e violações de dados que prejudicam a privacidade de indivíduos.

De fato, não há uma definição oficialmente aceita do que seja cibersegurança em âmbito internacional, em virtude de ser usada como um termo guarda-chuva conveniente para uma questão multifacetada que inclui diferentes dimensões, dependendo dos papéis e dos objetivos dos atores envolvidos: (*i)* a dimensão técnica abordada por especialistas de TIC que fazem a manutenção de *hardware*, *software*, redes e, de forma mais geral, sistemas de informação; (*ii)* a dimensão econômica e social, abordada por organizações e indivíduos que visam otimizar a probabilidade de sucesso de suas atividades; (*iii)* a dimensão do cumprimento da lei criminal, abordada pela polícia ou por outros atores de aplicação da lei, que lutam contra o crime *on-line*; e (*iv)* a dimensão de segurança nacional e internacional

abordada por militares, agências de inteligência e outros, como diplomatas envolvidos na prevenção de conflitos.

Na prática, especialistas que buscam esses diferentes objetivos tendem a usar diferentes termos. Por exemplo, especialistas de segurança das TIC, geralmente, apontam a "segurança da informação", "*infosec*", ou "segurança informática". Forças policiais e juízes criminais referem-se ao "cibercrime". Atores de segurança nacional indicam "ciberguerra", "ciberdefesa", "operações cibernéticas", "ciberespionagem" e, às vezes, simplesmente "ciber". De forma geral, o termo "ciber" (que, atualmente, pode ser considerado um prefixo) tende a conotações com funções soberanas do Estado: polícia e aplicação da lei, defesa e segurança nacional. Por esse motivo, os países-membros da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) concordaram em usar a expressão "segurança digital", em vez de "cibersegurança", a fim de fazer referência aos esforços das partes interessadas para protegerem suas atividades econômicas e sociais. O termo "digital" ecoa outras expressões familiares para civis com formação econômica e que não são especialistas técnicos, como "economia digital", "transformação digital" e a "digitalização". Ele também está ancorado na realidade técnica, pois a segurança digital se preocupa, em primeiro lugar, com questões relativas a tecnologias digitais, enquanto o significado exato de "ciber" não é claro de imediato, mesmo entre profissionais de TIC.

Essas distinções terminológicas são importantes porque ajudam a reconhecer diferenças significativas nas culturas, nas ferramentas, no jargão e, principalmente, nas abordagens de segurança adotadas por essas categorias de atores. Embora todos esses atores devam trabalhar juntos dada a natureza complementar e a sobreposição de suas missões, eles também competem e seus métodos podem entrar em conflito e até prejudicar um ao outro.

RISCOS DE SEGURANÇA DIGITAL PARA EMPRESAS

A segurança digital[2] visa aumentar a probabilidade do sucesso de atividades econômicas e sociais. Mais precisamente, é a forma como atores abordam incertezas que afetam a Confidencialidade, a Integridade e a Disponibilidade (tríade CID) de *hardware*, *software*, redes e dados dos quais dependem suas atividades econômicas e sociais.

Essas atividades vão desde as mais simples e banais até as extremamente complexas e críticas; por exemplo, postar uma mensagem em uma rede social ou fazer compras *on-line* até o fornecimento de energia elétrica a milhões de empresas e domicílios ou administrar hospitais e aeroportos. Considerando que toda a economia tem se tornado dependente digital em graus variados, a segurança digital refere-se a todas as atividades econômicas e sociais, incluindo aquelas críticas à segurança dos cidadãos, assim como ao funcionamento do governo e da sociedade (OECD, 2020).

Eventos potenciais que podem prejudicar atividades econômicas e sociais ao violarem a tríade CID são causados por **ameaças** intencionais ou não intencionais que se aproveitam de **vulnerabilidades**. Ameaças intencionais incluem, por exemplo, ataques de criminosos para roubar ou extorquir dinheiro, ao passo que ameaças não intencionais podem ser erros humanos ou eventos naturais, como incêndios, tempestades e enchentes. Vulnerabilidades são fraquezas exploradas por um ator de ameaça e compreendem, por exemplo, erros (*bugs*) em *hardware*, *software* ou redes; falta de treinamento humano; proteção insuficiente, seja ela digital (*firewalls*) ou física (câmaras e fechaduras no *data center*); assim como procedimentos inapropriados (processos de *backup* ou planos de recuperação de desastres).

Uma violação em uma dimensão da tríade CID pode prejudicar atividades econômicas e sociais que dependam dos sistemas de informação afetados. Uma **violação de disponibilidade** pode tornar o sistema inutilizável e parar atividades empresariais. Os chamados ataques de negação de serviço (do inglês *Denial of Service* – DoS), que inundam um sistema conectado com requisições inúteis, são típicos de disponibilidade. Em 2016, um

2 Como se concentra nos aspectos econômicos e sociais da cibersegurança, este prólogo usa o termo segurança digital em vez de cibersegurança.

ataque massivo de negação de serviço afetou milhares de servidores em partes da América do Norte e da Europa, incluindo os da Amazon, da CNN, da BBC e do Twitter[3]. Um simples apagão pode ter um efeito parecido em um sistema de informação.

Violações de integridade podem modificar dados ou a forma como um sistema de informação se comporta para interromper operações comerciais e a prestação de um serviço, como demonstrado pelos apagões que afetaram mais de 200 mil pessoas na Ucrânia, em 2015 e 2016[4]. Ataques de *ransomware* são exemplos típicos de violações tanto de integridade quanto de disponibilidade, nos quais dados de um sistema são criptografados (violação de integridade) e se tornam inutilizáveis por usuários legítimos (violação de disponibilidade): os invasores, geralmente, informam que vão descriptografá-los (mas nem sempre o fazem) até que um pagamento seja feito a eles. Em outubro e novembro de 2019, três hospitais nos Estados Unidos, sete na Austrália e um na França enfrentaram ataques graves de *ransomware* que atrapalharam suas operações em níveis diferentes[5]. Os terríveis incidentes de *ransomware* WannaCry e NotPetya de 2017, que levaram a um total de bilhões de dólares em prejuízos[6], atingiram milhares de empresas e organizações do mundo todo. Outros ataques causaram danos a governos locais, como em Johanesburgo, Baltimore e o estado americano de Louisiana[7].

Por último, **violações de confidencialidade** permitem que usuários não autorizados acessem dados e potencialmente violem a privacidade das pessoas, às vezes em escala muito ampla. No Brasil, um servidor publicamente acessível expôs a privacidade de 120 milhões de cidadãos devido a um problema de má-configuração[8]. Em outubro de 2019, a imprensa revelou

---

3 Disponível em https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

4 Disponível em https://www.bbc.com/news/technology-38573074 e https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/

5 Disponível em https://arstechnica.com/information-technology/2019/10/hamstrung-by-ransomware-10-hospitals-are-turning-away-some-patients/ e https://www.bloomberg.com/news/articles/2019-11-28/france-not-ruling-out-response-to-cyber-attack-on-hospital

6 Disponível em https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

7 Disponível em https://arstechnica.com/information-technology/2019/10/johannesburgs-network-shut-down-after-second-attack-in-3-months/, https://arstechnica.com/information-technology/2019/11/louisiana-was-hit-by-ryuk-triggering-another-cyber-emergency/ e https://arstechnica.com/information-technology/2019/05/baltimore-city-government-hit-by-robbinhood-ransomware/

8 Disponível em https://www.zdnet.com/article/over-half-of-brazils-population-exposed-in-security-incident/

que uma base contendo dados de 92 milhões de brasileiros estava à venda na *dark web*[9]. O ataque ao Escritório de Gestão de Pessoal dos EUA, em 2014, demonstrou que os governos também podem ser alvos, com a violação de dados de mais de 20 milhões de funcionários governamentais, incluindo arquivos sensíveis com habilitação de segurança e 5,6 milhões de impressões digitais[10]. Violações de confidencialidade também podem afetar dados não pessoais, como nos casos em que os invasores buscam roubar segredos comerciais; exemplos incluem o gigante alemão da indústria pesada ThyssenKrupp[11], o fabricante europeu de aeronaves Airbus[12] e as empresas americanas de energia Westinghouse e SolarWorld[13]. Apesar de frequentes, ataques contra a propriedade intelectual não tendem a ser relatados, pois as empresas afetadas não querem expor sua reputação. De acordo com o relatório de 2019 da empresa de consultoria PwC para a Comissão Europeia, o roubo digital relativo à segurança de segredos comerciais na Europa, em 2018, resultou em perdas de 60 bilhões de euros para o crescimento econômico e quase 289 mil empregos perdidos; além disso, projeções para 2025 ascendem a um milhão de perdas de empregos[14]. O roubo de segredos comerciais pode levar a custos significativos de oportunidade, impactos negativos na inovação, aumento de gastos em segurança e danos à reputação (ver p. 26). De maneira geral, as pequenas e médias empresas (PME) são alvos fáceis e estão sujeitas à falência quando sofrem roubos de inovação ou de segredos comerciais que comprometem sua vantagem competitiva.

9 Disponível em https://www.cpomagazine.com/cyber-security/citizen-data-of-92-million-brazilians-offered-for-sale-on-underground-forum/

10 Disponível em https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

11 Disponível em https://www.cbronline.com/cybersecurity/breaches/thyssenkrupp-cyber-attack-hackers-steal-trade-secrets/

12 Disponível em https://www.ibtimes.com/hackers-target-airbus-suppliers-quest-commercial-secrets-2833721

13 Disponível em https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

14 Disponível em https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

O IMPACTO DE ROUBOS DE SEGREDOS COMERCIAIS NA EUROPA

- **Custos de oportunidade:** incluem perdas de oportunidades de negócios, de vendas ou redução de produtividade, da vantagem de ser primeiro no mercado, de rentabilidade ou até mesmo de linhas inteiras de negócios para concorrentes. Em 2016, 23% das organizações vivenciaram uma perda de oportunidade devido a invasões; destes, 42% registraram uma perda de oportunidade equivalente a mais de 20% do valor da empresa.
- **Impacto negativo na inovação:** vantagens competitivas são geradas por Pesquisa e Desenvolvimento (P&D) caso seus resultados sejam apropriados por aqueles que investiram em P&D. Caso os resultados sejam perdidos ou livremente utilizados por todos, incluindo a concorrência, P&D não resultarão em vantagens competitivas substantivas. Ademais, embora a ameaça do roubo cibernético continue a crescer, empresas podem se tornar menos propensas a investirem em inovação devido ao risco da apropriação indevida de suas atividades de P&D.
- **Maiores custos de segurança:** incluem o gasto global anual com *software* de cibersegurança, assim como o custo de limpar sistemas afetados e do seguro para cibersegurança. Nesse sentido, a SSP Blue estima que empresas do mundo todo gastarão aproximadamente 170 bilhões de dólares com cibersegurança até 2020 (com uma taxa de crescimento de quase 10% desde 2015).
- **Danos à reputação:** as empresas podem sofrer uma depreciação significativa de valor caso uma invasão se torne fato público, incluindo a perda de valor do relacionamento com clientes, de contatos e a desvalorização da marca. Seiscentas empresas de médio porte, em seis países europeus, relataram a ocorrência de dano à reputação em 48% dos incidentes e perda financeira em 33% de casos.

FONTE: PWC (2019).

GESTÃO DE RISCO DE SEGURANÇA DIGITAL

Desde os primórdios da computação e, até recentemente, a maioria das partes interessadas, incluindo formuladores de políticas e a OCDE, abordava a segurança digital primariamente como uma questão técnica: o foco estava no risco de segurança para sistemas e redes. No entanto, à medida que as perdas por incidentes de segurança digital aumentaram, o foco da atenção mudou dos incidentes técnicos para suas consequências econômicas e sociais: perdas financeiras e de reputação, de oportunidades de negócio e de competitividade, de confiança

e o impacto na privacidade, assim como, em alguns casos, a destruição de bens materiais e possíveis perdas de vida.

Ademais, as partes interessadas também perceberam que as medidas para reduzir o risco de segurança digital podem ter efeitos negativos sobre as atividades econômicas e sociais que devem proteger: além de aumentar custos, elas podem fechar o ambiente digital e reduzir seu dinamismo, limitando as oportunidades do uso das TIC para a inovação. Elas também podem ampliar o tempo da comercialização e reduzir o desempenho e a facilidade de uso para os consumidores. Para as organizações, a gestão de riscos de segurança digital deve ser centrada mormente nas atividades econômicas e sociais, e não no ambiente digital que as apoia; como resultado, deve ser encabeçada pela liderança da empresa com o apoio de especialistas técnicos, e não o contrário.

Por perceberem os benefícios econômicos e sociais do ambiente digital, os gestores responsáveis estão mais bem posicionados do que especialistas técnicos para *(i)* estabelecer o "apetite de risco" da organização, ou seja, o nível de risco econômico e social tolerável; *(ii)* avaliar as possíveis consequências do risco de segurança digital nos objetivos econômicos e sociais os quais eles devem alcançar; e *(iii)* assegurar que medidas de segurança não prejudiquem essas atividades e reduzam o potencial das TIC para inovar e contribuir para a competitividade.

Contudo, esses gestores dependem de especialistas técnicos para entenderem as possíveis ameaças, vulnerabilidades, incidentes e opções de redução de risco (como segurança técnica e medidas de continuidade dos negócios). Portanto, ambos devem trabalhar juntos, ao passo que as decisões e a responsabilidade de gestão de riscos precisam, em última instância, serem assumidas pelos tomadores de decisão da empresa, e não delegadas a especialistas técnicos.

O risco de segurança digital tem um conjunto de características que, por sua vez, definem a gestão de risco de segurança digital[15]:

- Esse tipo de risco não pode ser extinto completamente sem, ao mesmo tempo, eliminar as oportunidades

15 Recomendação do Conselho da OCDE de 2015 sobre a Gestão do Risco de Segurança Digital para a Prosperidade Económica e Social. Disponível em https://oe.cd/dsrm

oferecidas pelas TIC; portanto, algum nível de risco de segurança digital precisa ser aceito. As organizações devem definir e atualizar seu apetite de risco de segurança digital para reduzir o risco até o nível aceitável por elas.
- Em virtude de o risco ser extremamente dinâmico, a gestão de risco de segurança digital nunca para, o qual deve ser avaliado e tratado de forma contínua, como parte de um ciclo de gestão de risco permanente.
- Ele não é fundamentalmente distinto de outros tipos de riscos. Portanto, a gestão de risco de segurança digital deve ser integrada à estrutura mais ampla da gestão de risco da empresa e não coexistir em paralelo como algo especial.

DESAFIOS PARA POLÍTICAS DE SEGURANÇA DIGITAL

Ao considerar os elementos que compõem a segurança digital, é importante refletir a respeito das diferenças entre as dimensões da segurança digital introduzidas anteriormente e os desafios apresentados para o estabelecimento, nos governos, de um *framework* de governança apropriado.

Quando se examina o cumprimento da lei criminal, verifica-se que as forças policiais e, de forma mais geral, os marcos e instituições de cibercrimes desempenham um papel importante na redução do risco, em âmbito geral, por lidarem com ameaças, ou seja, impedindo criminosos de cometerem crimes e também efetuando prisões. Apesar de não serem essenciais para a estratégia de gestão de risco de uma organização, a cooperação com forças policiais é importante por motivos jurídicos e para desencadear e apoiar investigações após os fatos. De modo geral, a polícia não está na melhor posição para dar conselhos às organizações sobre como se proteger de criminosos cibernéticos, além de conselhos genéricos sobre a "ciberhigiene", os quais dificilmente consideram toda a complexidade dos ambientes digitais industriais, empresariais e organizacionais. Dessa forma, o sutil exercício de equilíbrio para determinar quais medidas de segurança protegerão as operações da empresa sem inibir a inovação não é uma preocupação para o cumprimento da lei.

A cultura das instituições e dos atores responsáveis pela segurança nacional e internacional também é, de forma geral, diferente daquela de líderes e tomadores de decisão de

empresas e outras organizações. A aceitação de risco está no cerne da cultura empresarial, enquanto a segurança é um entre muitos outros parâmetros na equação de riscos a serem tomados, incluindo custos, concorrência, satisfação do consumidor, qualidade, tempo de comercialização e muitos outros. Em contraste, a cultura de segurança nacional é avessa ao risco porque seu objetivo é proteger bens de valor extremamente altos para o Estado, como o território nacional ou a independência do país. De acordo com essa perspectiva, a segurança está acima de tudo, pois se presume que, caso a segurança falhe, o resto falhará também. Essa situação explica por que a cultura de segurança nacional não se focaliza nas possíveis consequências negativas das medidas de segurança nas atividades econômicas e sociais. Por exemplo, soluções como desativar sistemas ou banir tecnologias tendem a ser consideradas meios razoáveis, do ponto de vista da segurança nacional, para eliminar um risco, apesar de poderem levar a consequências muito negativas na competitividade se outros atores no mercado global continuarem com acesso a esses sistemas e tecnologias. Uma decisão de segurança nacional que se sobrepõe a um desafio econômico ou social pode facilmente comprometer a prosperidade.

Portanto, é importante fazer uma distinção clara entre essas áreas e não misturar as diferentes dimensões da segurança digital em um único conceito quando se formula políticas públicas. Ao mesmo tempo, também é relevante adotar uma abordagem holística que considere inteiramente o governo, incluindo todas as dimensões para assegurar coerência e otimizar sinergias. Esclarecer a estrutura de governança à luz de uma visão holística que observe essas diferenças é o principal objetivo de estratégias nacionais de segurança digital, as quais, de forma geral, designam claras responsabilidades às agências relevantes, de acordo com suas missões centrais, e estabelecem liderança intragovernamental e mecanismos de colaboração para facilitar a tomada de decisão quando há um conflito de interesses.

Um aspecto muito importante dessas estratégias é reconhecer o papel das empresas, da sociedade civil, da comunidade técnica e da academia, bem como garantir que essas vozes sejam ouvidas, entendidas e consideradas, não apenas durante a formulação da estratégia, mas também ao serem implementadas em longo prazo, no decurso dos planos de ação. O diálogo e as parcerias públi-

co-privadas sustentáveis, baseadas em confiança, são essenciais para a formulação de políticas públicas de segurança, pois decisões desequilibradas podem ter um impacto significativo em competitividade, inovação, direitos humanos, liberdade de expressão, privacidade e outros valores centrais a uma sociedade democrática. Em última instância, a efetividade das políticas depende da habilidade de grandes e pequenas empresas, de organizações governamentais e das pessoas entenderem e implementarem as medidas das políticas em longo prazo. Outro desafio-chave para os governos é determinar qual agência deve encabeçar a política de segurança digital, que inclui várias áreas importantes.

Por exemplo, é preciso conscientizar e aumentar a força de trabalho de segurança digital, ou seja, garantir que organizações públicas e privadas, empresas e pessoas estejam cientes dos riscos de segurança digital e entendam como lidar com eles. Além de comunicações e informações públicas, essa área inclui o desenvolvimento de currículos no Ensino Fundamental e no Ensino Superior, visando treinar futuros profissionais para que preencham a lacuna de habilidades de segurança digital enfrentada pela maioria dos países. Habilidades de segurança não são apenas técnicas: elas incluem a capacidade de gestores entenderem o risco de segurança digital e integrarem sua gestão em seus planos gerais para a transformação digital das atividades econômicas e sociais.

Outra área importante é o desenvolvimento de uma indústria de segurança digital, estabelecendo ecossistemas de inovação em segurança digital, além de incentivá-la. Vários países têm assumido um papel de liderança nessa área; em particular, Israel tem o CyberSpark, empreendimento conjunto da agência de cibersegurança, do município de Be'er Sheva, da Universidade Ben Gurion e das principais empresas na indústria de cibersegurança, que aglomera um centro de pesquisa, um *hub* de P&D, um centro de treinamento, uma incubadora e um centro de inteligência, reunidos no mesmo local. Ele está acoplado à Initiative CyberSpark Industry, uma organização sem fins lucrativos (ONG) que atua como entidade coordenadora central para atividades industriais de segurança digital com todas as partes interessadas. Seus objetivos são impulsionar a região de Be'er Sheeva e otimizar seu potencial como centro de segurança digital, incentivar parcerias entre a academia e

a indústria, e atrair outras empresas nacionais e estrangeiras. Outras iniciativas público-privadas de inovação de segurança digital estão no Reino Unido, com a London Office for Rapid Cybersecurity Advancement (LORCA), escritório de Londres para investimentos rápidos em cibersegurança; na Espanha, com o Basque CyberSecurity Centre (BCSC); e em Singapura, com o Innovation Cybersecurity Ecosystem (ICE71). Muitas delas fazem parte da rede internacional Global Epic de ecossistemas de inovação em cibersegurança[16].

A OCDE adotou, em dezembro de 2019, a *OECD Recommendation on Digital Security of Critical Activities*, uma recomendação para a segurança digital de atividades críticas que estabelece diretrizes, a fim de garantir que as políticas públicas direcionadas a operadores de atividades críticas focalizem situações críticas para a economia e a sociedade, sem inibir suas capacidades de melhorar serviços e de se beneficiar da transformação digital.

As atuais tendências das principais políticas públicas incluem a promoção do desenvolvimento de produtos mais seguros (ou seja, bens e serviços) e o estímulo da adoção de políticas responsáveis de divulgação de vulnerabilidades por todas as empresas e organizações.

PROJETO DA OCDE: MEDIÇÃO DA GESTÃO DE RISCO DE SEGURANÇA DIGITAL EM EMPRESAS (*MEASURING DIGITAL SECURITY RISK MANAGEMENT IN BUSINESSES*)

A recomendação do Conselho da OCDE sobre a Gestão do Risco de Segurança Digital para a Prosperidade Econômica e Social de 2015 enfatiza as dimensões econômicas e sociais dos riscos de segurança digital (OECD, 2015).

Em 2016, a OCDE iniciou um projeto com o intuito de aumentar o entendimento e medir as práticas de gestão de risco de segurança digital de empresas. O primeiro passo dessa iniciativa foi revisar pesquisas anteriores que procuraram fornecer dados relativos aos riscos de segurança digital, para analisar que tipos de dados estavam sendo produzidos sobre o tema. A

16 Recuperado de https://globalepic.org/

conclusão geral foi que havia poucas perguntas sobre as práticas empresariais de gestão de risco de segurança digital e, quando presentes, limitavam-se a medidas técnicas.

Em seguida, a OCDE buscou melhorar a medição nessa área ao desenvolver um *framework* para avaliar as práticas de gestão de risco de segurança digital em empresas. Esse *framework* de medição, composto por seis módulos e 18 indicadores associados, guiou o desenho de um instrumento de pesquisa, desenvolvido pelo Cetic.br|NIC.br, com o objetivo de entender as práticas de gestão de risco de segurança digital, especialmente entre a população específica de gestores de riscos. O instrumento de pesquisa foi submetido a testes cognitivos no Brasil, também realizados pelo Cetic.br|NIC.br, cujos resultados – o instrumento de pesquisa junto com as recomendações – foram revisados e pré-testados pela Federação de Associações Europeias de Gestão de Risco (FERMA)[17].

Esta publicação aprofundará questões relativas à gestão de risco de segurança digital, especialmente entre empresas, assim como abordará os desafios associados à medição desse tema. Como parte do esforço, a publicação será baseada nos resultados do trabalho qualitativo realizado pelo Cetic.br|NIC.br no Brasil, no processo de contribuir com o desenvolvimento de um instrumento de pesquisa para o Projeto da OCDE para a medição da gestão de risco de segurança digital em empresas.

Laurent Bernat[18]
Organização para a Cooperação
e Desenvolvimento Econômico – OCDE

17 Um relatório sintetizando as três fases do projeto da OCDE está disponível em: https://www.oecd-ilibrary.org/science-and-technology/measuring-digital-security-risk-management-practices-in-businesses_7b93c1f1-en

18 As opiniões expressas neste documento não representam necessariamente as opiniões da OCDE e de seus membros.

REFERÊNCIAS

Organisation for Economic Co-operation and Development (OECD). (2015). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion*. Recuperado de https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm

Organisation for Economic Co-operation and Development (OECD) (2020). *Recommendation of the Council on Digital Security of Critical Activities*. Recuperado de https://legalinstruments.oecd.org/api/print?ids=659&lang=en

PricewaterhouseCoopers (PwC). (2019). *Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber*. Recuperado de https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

CAPÍTULO 1

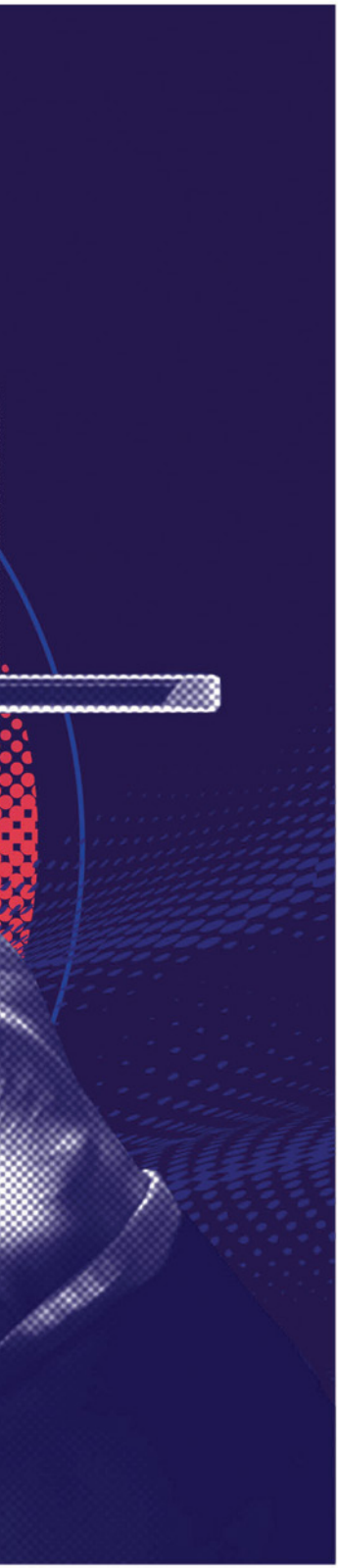
A nova agenda de cibersegurança: desafios econômicos e sociais para uma Internet segura[1]

Johannes M. Bauer[2] e William H. Dutton[3]

1 Este capítulo é uma atualização e revisão de um documento publicado originalmente em 2 de junho de 2015, preparado como apoio ao Relatório de Desenvolvimento Mundial, do Banco Mundial. Os autores agradecem ao Banco Mundial e a David Satola, em particular, porém enfatizam que os pontos de vista e as opiniões manifestados são de responsabilidade dos autores e não representam, necessariamente, aqueles do Banco Mundial ou de qualquer outra organização.

2 Johannes M. Bauer é o Diretor do Centro Quello para Políticas de Mídia e Informação e Professor no Departamento de Mídia e Informação da Michigan State University.

3 William H. Dutton é pesquisador sênior para o Instituto de Internet de Oxford e pesquisador da Oxford Martin School, dando suporte para o Centro de Cibersegurança Global da Universidade de Oxford. É também ex-Diretor do Centro Quello e Professor Emérito da University of Southern California.



INTRODUÇÃO

A cibersegurança refere-se "às tecnologias, aos processos e às políticas que ajudam a prevenir e/ou reduzir o impacto negativo de eventos no espaço cibernético que podem ocorrer como resultado de ações deliberadas contra a tecnologia da informação por um ator hostil ou malicioso" (Clark, Berson, & Lin, 2014, p. 2). Os esforços para aumentar a cibersegurança têm enfrentado uma gama crescente de desafios à medida que a Internet continua a desempenhar um papel cada vez mais central no desenvolvimento social e econômico de nações no mundo todo. Esse é o caso em todos os países, porém é especialmente verdadeiro em nações em rápido desenvolvimento, onde a função da Internet apresenta um potencial moderno e ainda maior para fortalecer seu papel global (Dutta, Dutton, & Law, 2011).

A variedade de problemas associados à segurança no mundo *on-line* é ampla e crescente, e tem se tornando cada vez mais intensa, apesar dos esforços ao longo dos anos para melhorar a cibersegurança. Isso se deve, em parte, ao papel cada vez mais central da Internet no desenvolvimento econômico e social, tornando-a um alvo mais valioso, mas também a novas dinâmicas do problema. Tentativas de endereçar essas questões têm tido sucesso parcial em muitos casos e não têm conseguido impedir a inovação de invasores para criar novas estratégias e evitar que usuários sejam vítimas dessas estratégias. Ademais, os mesmos avanços da Internet que, por um lado, permitem que mais usuários consigam usufruir de serviços bancários ou fazer compras *on-line*, por exemplo, por outro, também facilitam o uso mal-intencionado da Internet, generalizando, assim, o crime cibernético.

Embora as preocupações sobre a cibersegurança tenham gerado uma vasta gama de iniciativas, os problemas persistem e crescem em frequência e significância. Algumas questões, tal como o *spam*, já foram abordadas com sucesso, muitas vezes devido à possibilidade de disseminar amplamente soluções técnicas; todavia, mesmo nesse caso, o problema deve ser constantemente atualizado: os *spammers* criam novas maneiras de atingir usuários, e os incentivos por trás do *spamming* continuam a evoluir, tal como o "*spamdexing*", que visa otimizar a visibilidade de um *site* em mecanismos de busca.

O reconhecimento desses problemas crescentes tem levado um grande número de indivíduos, comunidades e instituições a elevarem a prioridade da cibersegurança. Por exemplo, o lançamento do Centro de Cibersegurança Global (Global Cyber Security Capacity Centre), da Universidade de Oxford, foi recebido com interesse mundial e gerou muitos compromissos de participação para enfrentar um problema amplamente reconhecido[4]. Em alguns casos, essas iniciativas obtiveram sucesso temporário em reduzir questões específicas de cibersegurança, todavia elas ainda não conseguiram ter um impacto duradouro em uma ampla gama de problemas que parecem se agravar, à medida que a tecnologia tem sido mais valorizada. Além disso, nem todas as respostas têm sido efetivas: é preciso reconsiderar as abordagens à cibersegurança mais sensíveis e conscientes dos aspectos econômicos e sociais dos problemas, como os motivos pelos quais usuários nem sempre seguem as boas práticas recomendadas pela comunidade técnica de segurança.

Nesse sentido, o que pode ser feito para apoiar abordagens mais efetivas a ações globais e multissetoriais com o intuito de aprimorar a cibersegurança na era digital? A cibersegurança tem tido prioridade na agenda de governos, de atores das indústrias de tecnologia de informação (TI) e de muitos grupos civis que participam da governança da Internet. Contudo, paradoxalmente, os problemas estão crescendo e tornam-se cada vez mais urgentes. Considerando a ineficácia de algumas abordagens convencionais para lidar com o problema, é importante questionar a sabedoria convencional e repensar as maneiras de como lidar com a cibersegurança.

NOVAS CARACTERÍSTICAS DO CENÁRIO DE CIBERSEGURANÇA EM DESENVOLVIMENTO

A segurança das telecomunicações sempre foi um problema ao longo dos séculos, desde o uso do pombo-correio até o advento da Internet das Coisas (IoT). Embora a Internet tenha sido projetada para apoiar o compartilhamento de recursos de informática, incluindo computadores e dados por meio de redes (e não para fornecer segurança), a partir de seu surgimento e de

4 Mais informações em: http://www.oxfordmartin.ox.ac.uk/research/programmes/cybersecurity/

seu uso para atividades mais básicas, como o acesso à bancos e compras *on-line*, o reconhecimento da cibersegurança como um problema central aumentou, apesar de não ser uma questão nova (NRC, 1991; NRC, 2002; Clark et al., 2014, p. ix)[5].

Dessa forma, desenvolvimentos técnicos, pesquisas, iniciativas de políticas públicas e medidas práticas para usuários têm evoluído nos últimos anos para fortalecer a cibersegurança, tal qual a comunidade global de governança da Internet, que tem se centrado em questões de segurança, o que resultou em muitas iniciativas regionais e nacionais. Exemplos disso incluem inovações organizacionais, como a formação de um Comitê Consultivo de Segurança e Estabilidade (Security and Stability Advisory Committee – SSAC), em 2002, pela Corporação da Internet para Atribuição de Nomes e Números (Internet Corporation for Assigned Names and Numbers – ICANN); o desenvolvimento da Agência da União Europeia para a Cibersegurança (European Union Agency for Cybersecurity – ENISA); a criação de Grupos de Resposta a Incidentes de Segurança (Computer Emergency Response Teams – CERTs), projetadas para melhorar a segurança de um país; e Grupo de Tratamento de Incidentes de Segurança (Computer Security Incident Response Teams – CSIRTs), que costumam ser organizados com várias partes interessadas (DeNardis, 2014, p. 90-95). Em 2004, fundou-se o Plano de Ação de Londres (London Action Plan – LAP), uma rede de supervisão de cibersegurança; centrada na questão do *spam*, a rede cresceu e, atualmente, inclui 47 organizações governamentais de 27 países, 28 organizações do setor privado de 27 países e seis organizações observadoras[6]. Também houve iniciativas lideradas especialmente por empresas, como o Grupo de Trabalho Anti-Abuso de Mensagens (Messaging Anti-Abuse Working Group – MAAWG), formado por membros da indústria de mensagens para abordar questões como o *spam*; ocorreram colaborações globais, como o Fórum Mundial para Grupos de Respostas a Incidentes de Segurança em Computadores (Forum of Incident Response and Security Teams – FIRST.org), que

5 Vários relatórios sobre cibersegurança feitos pelo Conselho de Ciência da Computação e Tecnologia do Conselho Nacional de Pesquisa dos EUA fornecem um contexto histórico das preocupações emergentes sobre a questão. Recuperado de http://sites.nationalacademies.org/CSTB/CSTB_059144

6 Recuperado de http://londonactionplan.org/

conseguiu cadastrar mais de 300 membros de todos os continentes; além de várias iniciativas intergovernamentais, como a Convenção sobre o Cibercrime do Conselho Europeu, adotada em 2001, que, até abril de 2015, foi ratificada por 45 países, incluindo seis nações não europeias[7].

Contudo, a escala e a severidade dos problemas parecem aumentar junto com a centralidade e a ubiquidade crescente da Internet em um mundo hiperconectado e que se fundamenta na rede. Portanto, paralelamente à ascensão da Internet, houve um crescimento proporcional do crime cibernético: problemas como o *spam* continuam a ser uma questão para Provedores de Serviços de Internet (PSI) e seus usuários (Krebs, 2014) e ameaças à privacidade têm crescido com o desenvolvimento da mídia social e a análise de *Big Data*, dramaticamente expostas pelas revelações de Edward Snowden, em 2014[8].

No entanto, os esforços para abordar os problemas não têm sido suficientes para reduzir o que parece ser uma variedade crescente de problemas de cibersegurança. Existem vários motivos por trás das dificuldades enfrentadas para tal. A adoção de práticas que poderiam melhorar a segurança *on-line* por muitos atores-chave, incluindo usuários, tem sido lenta; logo, motivar uma ampla gama de atores em todo o mundo, o que representa mais de quatro bilhões de usuários, a mudarem a maneira como fazem as coisas não é apenas uma questão técnica. Isso também exige uma compreensão sobre como cada ator entende a cibersegurança, seu nível de consciência e como é incentivado a ignorar ou adotar práticas que poderiam proteger a si mesmo e a outras pessoas no ambiente *on-line*. De forma geral, o modo como a cibersegurança é oferecida é difícil e caro, o que pode significar que seja economicamente racional aceitar certo nível de insegurança (Anderson & Moore, 2006; Moore, Clayton, & Anderson, 2009), como quando indivíduos aceitam os riscos potenciais do comércio *on-line*, ou organizações decidem aceitar os custos de compensar as vítimas em vez de impor precauções de segurança que possam ser trabalhosas ou desagradáveis para os consumidores.

Vários avanços do lado do crime cibernético também contribuem para a natureza potencialmente maliciosa do problema

7 Recuperado de http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG
8 Recuperado de http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html

(*wicked problem*)[9]. A virtude da conectividade global permite, por exemplo, que criminosos lancem ataques remotamente, usando servidores e máquinas em diferentes países; além disso, a anonimidade levanta outra limitação para iniciativas de cibersegurança: a necessidade de equilibrar a segurança com outros objetivos valiosos, como a privacidade e a liberdade de expressão. Um risco real da promoção da cibersegurança é o potencial de prejudicar outros valores e interesses-chave que podem ser ampliados pela Internet. Portanto, é preciso equilibrar esses objetivos por vezes compatíveis, mas às vezes concorrentes, tais como as "tensões entre a cibersegurança e a vigilância" associadas à segurança nacional (Clark et al., 2014, p. 104-105).

Uma consequência desses desenvolvimentos é um foco cada vez mais centrado no papel das questões sociais e comportamentais ao se abordar cibersegurança. Frequentemente, esse tema é atribuído a especialistas de informática nas áreas de ciência e engenharia da computação, ou à equipe de tecnologia de informação de uma organização. Embora seu conhecimento técnico e suas contribuições para uma organização segura, assim como para uma Internet segura, aberta e global, têm sido e continuarão sendo valiosos, as iniciativas para abordar os problemas progressivos da cibersegurança enfrentam novos desafios que exigem contribuições de muitas outras disciplinas e de diversos atores.

DESAFIOS PARA ABORDAR A CIBERSEGURANÇA

1. Uma nova gama de atores e motivações

A Internet e as tecnologias de informação e comunicação (TIC), tais como as mídias sociais, a Internet móvel e a IoT, estão expandindo a variedade de atores envolvidos na proteção da segurança, incluindo usuários em particular que raramente têm como foco a segurança, exceto como um passo necessário para seguir adiante com o que desejam realizar *on-line*. Ao mesmo tempo, o leque de atores capazes e dispostos a atacarem sistemas de informação também está crescendo, incluindo uma vasta série de motivações, desde ataques à segurança nacional até outros motivos criminosos.

9 O conceito de "*wicked problem*" serve para enfatizar problemas demasiadamente complexos, dinâmicos e difíceis, inclusive impossíveis, de resolver.

2. Uma gama crescente de plataformas e aplicações

Há bastante tempo, a segurança era protegida por meio do computador *mainframe* de uma organização; atualmente, uma variedade crescente de plataformas – desde as mídias sociais na World Wide Web até as plataformas móveis, a computação em nuvem, o *Big Data* e a IoT – estão criando um conjunto de plataformas tecnológicas e ambientes sociais muito mais complexos e com características diferentes que exigem abordagens distintas de segurança. Alguns dependem do elo mais fraco de um sistema de nós conectados, como o uso de *botnets*; outros, dos esforços de atores específicos, como no caso de ataques direcionados a uma empresa ou a um Estado (Varian, 2004).

O crescimento da disponibilidade da Internet de banda larga, a partir do final dos anos de 1990, não só aumentou consideravelmente o uso da Internet, mas também multiplicou suas vulnerabilidades. Ademais, a rápida adoção de telefones celulares e dispositivos móveis e a formação de redes entre um número cada vez maior de objetos na IoT têm aumentado o número de pontos de ataque e expandido a presença do crime cibernético a países em desenvolvimento (Orji, 2012; Shalhoub & Al Qasimi, 2010).

Com o uso massivo de aparelhos móveis e mídias sociais, novas estratégias de ataques estão em ascensão. O mercado de aplicativos móveis também tem sido cada vez mais usado e é frequente o uso de versões falsas de aplicativos populares. Os dispositivos móveis costumam fornecer detalhes das permissões exigidas por um aplicativo, à medida que os usuários tendem a aceitar um aplicativo sem realizar um exame crítico desses termos. Além disso, o acesso a outras funções, como *bluetooth*, GPS e uma câmera, assim como a dados pessoais, oferece uma base de ataque mais ampla do que por meio de computadores tradicionais.

3. Equilíbrio entre uma gama mais ampla de questões

A segurança não pode mais ser entendida pontualmente, pois está intimamente conectada a outras questões, como a privacidade e a vigilância, conforme supracitado; também está conectada, de forma geral, aos riscos associados com as novas mídias, como as ameaças e os danos vinculados ao uso das mídias sociais. Considerando essa interdependência, é preciso identificar e considerar os *tradeoffs* que podem ocorrer em razão de outros objetivos, por exemplo, quando o aumento de

segurança pode comprometer a liberdade de expressão ou a privacidade individual. Isso é uma tarefa difícil, pois usuários podem sacrificar alguns valores, como a privacidade em nome da segurança ou mesmo conveniência (Dutton & Meadow, 1987). Portanto, é relevante que governos e outras partes interessadas garantam a proteção desses direitos e dessas responsabilidades, ao mesmo tempo que assegurem maior cibersegurança.

4. Questões interdependentes de governança multinível

Questões de governança estão entrelaçando empresas, agências governamentais, países, regiões e atores globais em uma série cada vez mais interdependente de processos de governança. O reconhecimento da escala global e da interdependência dessas questões é fundamental para evitar os riscos da fragmentação da governança, que poderiam prejudicar iniciativas locais e globais, não apenas relativas à cibersegurança, mas também a todas as questões vinculadas à Internet – tanto a privacidade das pessoas como a vitalidade do comércio global. A Internet não tem fronteiras nacionais delimitadas, o que torna o sucesso da cibersegurança um desafio cada vez mais mundial, que não pode ser contido dentro de única fronteira organizacional ou nacional.

5. Conscientização às práticas e aos problemas

Há décadas, realizam-se campanhas de conscientização pública e organizacional, cujo objetivo costuma ser amedrontar os usuários. É preciso centrar mais esforços no fornecimento de dicas e de diretrizes aos usuários sobre boas práticas para que possam proteger sua própria segurança e ajudar a proteger a segurança de outros usuários. Para que sejam bem-sucedidas, tais campanhas precisam que os sistemas sejam desenhados com fácil utilização para as pessoas.

6. Melhorar o *design* de interfaces de usuário de aplicações de segurança

Muitos sistemas de segurança formulados pela comunidade técnica têm se tornado cada vez mais inviáveis para a adoção por usuários. É preciso que novos *designs* sejam desenvolvidos e implementados de forma muito mais ampla, visando promover mais facilidade para os usuários se protegerem e protegerem seus computadores contra violações de seguran-

ça, ao mesmo tempo que não comprometam outros valores e interesses como a proteção da anonimidade, conveniência ou velocidade em obter um serviço.

7. Os efeitos duplos dos avanços tecnológicos

Uma última questão central, que não é nova mas está cada vez mais evidente, são os efeitos duplos do empoderamento. As ameaças cibernéticas estão evoluindo rapidamente em uma corrida técnica a fim de aumentar a segurança contra tentativas de encontrar novas formas de violá-la por atores mal-intencionados. Esses atores hostis também variam muito, incluindo *hackers* maliciosos[10] e criminosos comuns que encontram no crime cibernético uma forma cada vez mais fácil e segura do que a realização física de um crime, como o roubo.

OS CUSTOS E BENEFÍCIOS DISTRIBUÍDOS DA CIBERSEGURANÇA

Para entender as dinâmicas da cibersegurança, é essencial saber quem ganha e quem perde com resultados de níveis maiores ou menores de segurança. Entretanto, os custos e benefícios reais da cibersegurança continuam a evadir esforços para desenvolver indicadores quantitativos confiáveis e válidos. Embora existam muitas estimativas dos custos do crime cibernético, muitos relatórios são baseados em evidências fracas ou em pressupostos fortes muito simplistas. Frequentemente, os métodos empregados não estão publicamente disponíveis; por conseguinte, complicam uma avaliação quanto à validade e confiabilidade da informação. Logo, os prejuízos são tipicamente avaliados em um nível altamente agregado e são difíceis de vincular a incidentes específicos.

Desenvolvimentos recentes de métodos mais robustos de medição concentram-se em organizações e empresas individuais, e não em toda a cadeia de valor ou nos custos à sociedade como um todo, o que seria uma métrica relevante para políticas

10 Inicialmente, o termo "*hacker*" era definido como uma pessoa obsessivamente focada em resolver um problema de programação, ao que Joseph Weizenbaum (1976, p. 111-131) se referiu como um "programador compulsivo". A preocupação desse autor era que tal compulsão poderia prejudicar o conhecimento humanístico de um problema e criar técnicos em vez de programadores. Desde Weizenbaum (1976), o termo tem sido usado mais frequentemente para definir pessoas que buscam invadir, "*hackear*" ou decifrar sistemas de computador, cada vez mais, por meio da Internet.

públicas e decisões relativas ao cumprimento da lei. Muitas vezes, os números relatados são confusos, e as explicações detalhadas para suas variações estão ausentes.

Devido à natureza altamente interconectada da Internet, incidentes de segurança não somente afetam os alvos imediatos de um ataque, mas também têm efeitos secundários e terciários em outras partes interessadas. Do ponto de vista de políticas públicas, o custo relevante é o custo total para a sociedade, que também inclui os custos que foram incorridos por outras partes interessadas que não as diretamente afetadas.

Uma avaliação ampla dos custos e benefícios da cibersegurança, portanto, deve incluir todo o ecossistema de atores, abrangendo:

- usuários (indivíduos, domicílios e grandes, pequenas e microempresas);
- organizações do setor privado presentes no comércio eletrônico (comerciantes *on-line*, serviços financeiros, serviços de seguros, saúde etc.);
- organizações do setor público (serviços de governo eletrônico);
- fornecedores de infraestrutura de TI (fornecedores de *software*, PSIs, provedores de serviços de hospedagem, registradores de domínios);
- unidades de resposta a incidentes (CSIRTs, autoridades policiais);
- a sociedade em geral (incluindo custos de oportunidade, ganhos de eficiência perdidos, menor confiança e uso da Internet etc.); e
- criminosos e atores maliciosos (incluindo criminosos cibernéticos, *hackers* maliciosos e todos aqueles que buscam lucrar ao prejudicar a segurança da Internet).

Ao avaliar o impacto de um incidente de segurança em particular, por exemplo, é útil distinguir entre custos diretos e indiretos (Gordon & Loeb, 2005). Danos diretos são os custos causados por uma violação específica de segurança; por sua vez, os custos indiretos, ao mesmo tempo que, claramente, são causados pelo fato de que ocorreu uma violação de segurança, não são a simples consequência de uma violação específica: ao contrário, refletem custos mais genéricos, como o custo das medidas para prevenir violações de segurança ou de treinar funcionários para que adotem práticas de segurança.

Os custos diretos e indiretos podem ser explícitos ou implícitos (Gordon & Loeb, 2005). Custos explícitos, como gastos com segurança, são bem-definidos e, em princípio, diretamente visíveis a partir de dados da contabilização dos custos. Os custos implícitos são os impactos conhecidos das violações de segurança que tendem a escapar a medições inequívocas, embora seja possível encontrar indicadores substitutos. Os custos implícitos, no âmbito da sociedade em geral, ocorrem, por exemplo, se os problemas de segurança desaceleram a adoção de serviços *on-line* por atores do mercado e usuários finais, postergando, assim, à sociedade os possíveis benefícios do uso da Internet.

Com base nessa categorização, diferentes custos específicos podem ser identificados. Ao usar esse marco de referência, avaliações sistemáticas do custo total da cibersegurança podem ser desenvolvidas em um processo passo-a-passo. As etapas individuais são repetidas até que todas as categorias de custo sejam analisadas, a fim de averiguar se são relevantes para cada um dos atores; em caso afirmativo, pode-se estimar a dimensão do impacto direto, indireto ou implícito. A soma de cada tipo de custo para todos os atores e todas as categorias de custos resulta em uma estimativa do custo direto total, do custo indireto total e dos custos implícitos totais.

Pesquisas recentes têm observado um relacionamento interessante entre o aumento da conectividade e das ameaças à segurança da informação. Inicialmente, à medida que a conectividade de um país cresce, também aumentam os problemas de cibersegurança. Entretanto, essa relação não é linear: conforme as taxas de adoção aumentam, essa tendência é revertida, e o desempenho da segurança volta a melhorar (Burt, Nicholas, Sullivan, & Scoles, 2014). Essa observação enfatiza os desafios enfrentados por países em desenvolvimento: ao mesmo tempo que a capacitação e a educação, bem como as políticas públicas esclarecidas, são fatores importantes para reverter essa tendência, esses resultados também oferecem motivação e um caminho para seguir, pois a situação pode inclusive piorar em vez de melhorar.

ESTRUTURAS DE (DES)INCENTIVO ENTRE MÚLTIPLAS PARTES INTERESSADAS

Os custos e benefícios distribuídos podem criar grandes incentivos para alguns usuários se envolverem em atividades mal-intencionadas, como o *phishing*: um *site* malicioso pode tentar muitas vezes (20 ou mais) acessar um computador em particular por meio do *phishing*. Em contraste, como os incentivos são relativamente baixos para muitos usuários, podem não ter cautela, ocasionalmente, ao abrir *e-mails* duvidosos ou mensagens suspeitas.

ENTENDENDO A DIVERSIDADE DE INCENTIVOS

A multiplicidade de motivos entre os usuários precisa ser considerada para que se entenda seu comportamento. Por exemplo, as motivações dos *hackers* variam consideravelmente, desde *hackers* chapéu branco ("*white hat*" – com objetivos principalmente "benéficos") e *hackers* chapéu preto ("*black hat*" – mal-intencionados). Da mesma forma que a Internet tendeu a democratizar o acesso à informação, ela também possibilitou a democratização de algumas atividades criminosas, pois facilitou o seu uso por leigos no intuito de cometerem crimes, como fraude, levando alguns a mencionarem a "democratização do crime cibernético".

Por exemplo, *hackers* "*white hat*" podem se envolver no ataque a sistemas com o objetivo de torná-los mais seguros, ou na prestação de contas de organizações, por exemplo, ao expor fraudes. Governos podem ter um interesse em manter suas vulnerabilidades para poderem penetrar nos sistemas operados por seus adversários, exemplo de como a cibersegurança pode entrar em conflito com a segurança nacional, como demonstrado pelas polêmicas contínuas sobre a criptografia. Nessa interação, os esforços para proteger sistemas e aparelhos e educar usuários para que adotem comportamentos seguros *on-line* são regularmente prejudicados por meios técnicos e sociais, novos e inovadores. A redução das ameaças de uma geração de vetores de ataque pode ser um sucesso temporário até o surgimento de novas formas, ao passo que o cenário de ameaças também varia em resposta a dispositivos e plataformas de comunicação empregados, a serviços usados por empresas e indivíduos, assim como ao marco econômico, legal e institucional em vigor.

As ameaças têm se alterado: de uma época de ataques altamente visíveis por invasores em busca de fama, glória e notoriedade, para ataques, em sua grande parte, invisíveis, realizados por motivos fraudulentos e criminosos. Por um tempo, os vírus eram a preocupação principal, e o *spam* de *e-mail*, o grande veículo para a disseminação de códigos maliciosos; à medida que fabricantes de *hardware*, desenvolvedores de *software*, PSIs e usuários se adaptaram a esses desafios, as estratégias dos ataques também mudaram.

A ECONOMIA POLÍTICA DA CIBERSEGURANÇA[11]

Um dos principais motivos pelos quais esforços de múltiplas partes interessadas para lidar com problemas de cibersegurança não tiveram um impacto mais duradouro associa-se à particular "estrutura do problema" dos desafios de segurança da informação (Asghari, Van Eeten, & Bauer, 2016). A Internet é uma rede densa, com várias interdependências tecnológicas e econômicas entre os atores-chave; além disso, a segurança da informação tem fortes características de "bem comum", visto que seus benefícios agregam à comunidade de usuários em geral. Dessa forma, tanto os custos como os benefícios frequentemente afetam múltiplos atores sem transações de mercado que lhes compensem: em outras palavras, a segurança da informação é tipicamente atingida por externalidades positivas e negativas.

Ademais, os mercados de segurança, assim como aqueles para muitos serviços de mídia e informação, sofrem de problemas de informações incompletas e assimetricamente distribuídas. Os usuários, geralmente, não estão em posição de avaliar o desempenho de segurança de um PSI, um aparelho, um *software* ou uma aplicação; logo, a natureza exata de como as externalidades e assimetrias de informação afetam a segurança varia de acordo com o tipo de risco de segurança, a natureza dos ataques e as melhores defesas.

Um exemplo é o caso de ataques sem alvo. Se um usuário não investe em *software* de segurança para um dispositivo conectado à Internet e essa máquina for infectada, seu desempenho pode

11 Esta seção foi fortemente embasada nas pesquisas de Van Eeten, Bauer, Asghari, & Tabatabaie (2010) e Van Eeten & Bauer (2013).

ser afetado; entretanto, o principal custo de incidentes de segurança será daqueles que recebem *malware*. Assim, um usuário desprotegido ou malprotegido causa uma externalidade negativa para outros. Se, por sua vez, o usuário investe em cibersegurança, alguns benefícios serão usufruídos por outros usuários, pois suas máquinas terão menos chances de ser infectadas.

Desse modo, o usuário causa uma externalidade positiva. Verifica-se, portanto, que, em virtude de apenas parte dos custos associados a uma externalidade negativa ser assumida por quem a causar, e apenas parte dos benefícios de uma externalidade positiva ser sentida pelo usuário que a causa, a tomada de decisão decentralizada por usuários individuais não refletirá sistematicamente em repercussões mais amplas no ecossistema maior. Contudo, o contrário é verdadeiro para ataques com alvos: uma organização que fortalece suas defesas contra os ataques direcionados, sem querer, exerce uma externalidade negativa em outras organizações que não tomaram medidas de segurança similares; consequentemente, haverá um risco maior de sofrer um ataque.

Um volume crescente de pesquisas defende que muitos problemas de cibersegurança são causados por estruturas de incentivo desalinhadas, o que (des)incentiva atores individuais. Assim, considerando essas interdependências, isso resulta em maiores problemas de segurança para todos. Literalmente, todos os participantes do ecossistema da Internet trabalham com incentivos mistos, alguns contribuindo para o reforço de esforços de segurança, outros enfraquecendo-os. O efeito final dessas forças conflitantes tende a ser ambíguo, mas precisa ser objeto de estudo.

A seguir, apresenta-se uma breve explicação das principais iniciativas para atores importantes no ecossistema da Internet.

O ECOSSISTEMA DA INTERNET: PRINCIPAIS ATORES E INCENTIVOS

FORNECEDORES DE *HARDWARE*

Fabricantes de *hardware* operam em um mercado altamente competitivo. A testagem de *hardware* e de seus componentes para possíveis vulnerabilidades pode aumentar o tempo de comercialização e, diante da existência de vantagens para quem é

pioneiro no mercado e de efeitos em rede, um atraso pode resultar em desvantagens duradouras. Ao mesmo tempo, fabricantes de equipamentos precisam se preocupar com a reputação. O primeiro fator reduz a atenção dada para a segurança; já o segundo, aumenta-a, caso a reputação também seja dependente do desempenho de segurança: se os efeitos da reputação forem mais fortes, o efeito final será maior segurança. Outra vulnerabilidade introduzida no ecossistema da Internet é a prática de se vender *hardware* com versões experimentais de *software* de segurança e outros. Esses incentivos conflitantes podem ser mitigados caso haja aumento das práticas de *design* de equipamentos de segurança, estabelecimento de padrões mínimos para equipamentos, adoção de regras de responsabilidade do fabricante e mudança da configuração padrão para que sejam realizadas renovações e atualizações automáticas de *software*.

FORNECEDORES DE *SOFTWARE*

Da mesma forma que os fornecedores de *hardware*, os de *software* trabalham sob estruturas de incentivo ambíguas. Os custos e o tempo (de comercialização) de testagem de *software* constituem um fator que pode reduzir a segurança. O desejo do usuário para altos níveis de funcionalidade, compatibilidade e discrição, geralmente, tem um custo em termos de características de segurança. Termos de licenciamento de *software* que contêm cláusulas de isenção de responsabilidade protegem fornecedores de qualquer processo legal e, portanto, em um cenário semelhante, enfraquecem o incentivo para que vendedores de *software* invistam em segurança. Ademais, programas de *software* são desenvolvidos em uma ampla gama de formas institucionais, desde empresas comerciais até produções entre pares e programadores amadores individuais; assim, nem todos os aplicativos ou *plug-ins* e programas são desenvolvidos levando em consideração a segurança.

PROVEDORES DE SERVIÇOS DE INTERNET (PSIs)

Os PSIs são atores-chave no ecossistema da Internet, com várias opções para melhorar a segurança da informação. Os custos do serviço de atendimento ao consumidor e da gestão de abuso, assim como o custo de infraestrutura adicional que

pode ser necessária para lidar com tráfego malicioso, têm um efeito imediato no resultado final e têm aumentado os incentivos para que PSIs tomem medidas para fortalecer a segurança. Ainda que a perda de reputação e o prejuízo à marca funcionem indiretamente (e provavelmente, mais lentamente), exercem pressão na mesma direção. Os PSIs fazem parte de um sistema interdependente de provedores de serviços que podem tomar uma gama de medidas progressivas de retaliação em resposta a práticas ruins de segurança, como a inclusão em listas de bloqueio, mesmo se a origem for um usuário individual. Por outro lado, os custos para aumentar a segurança, as cláusulas de isenção de responsabilidade legal de PSIs e os custos da aquisição por consumidores constituem fatores que tendem a reduzir investimentos na segurança da informação.

USUÁRIOS

Grandes empresas (com 250 funcionários ou mais) que usam a Internet formam um grupo heterogêneo; muitas adotaram ferramentas de análise de risco para tomarem decisões de segurança, porém a diligência que exercem pode variar de acordo com seu porte (cuja escala lhes permite ter maior capacidade de cibersegurança) e outros fatores, tais como os produtos e serviços específicos fornecidos. Pequenas e médias empresas (PME, tipicamente definidas como empresas com menos de 250 funcionários), microempresas e usuários residenciais são um grupo grande e diversificado. Como outros participantes, eles trabalham sob incentivos múltiplos e potencialmente conflitantes; logo, muitos têm recursos insuficientes para criar capacidade de cibersegurança para prevenir ou responder a ataques sofisticados. Grandes empresas e usuários individuais podem ter a percepção de que sua exposição ao risco é baixa, ao passo que muitas PME e usuários residenciais investirão em segurança – e alguns podem até investir demasiadamente –; dessa forma, não há garantias de que o nível de esforço será ideal. Por exemplo, muitos países têm altos níveis de *software* pirateado que não podem ser atualizados automaticamente, o que demonstra um risco inerente de segurança.

O GOVERNO

O governo e as agências governamentais, em princípio, são atores que poderiam alinhar os incentivos de diferentes atores por meio da formulação de políticas públicas efetivas. Por exemplo, "Cyber Essentials"[12], política adotada no Reino Unido que incentiva fornecedores que desejem trabalhar com contratos governamentais para implementar práticas de segurança mínimas, sugere que essas políticas de contratação podem ajudar a melhorar a segurança. Contudo, governos nem sempre são os atores neutros ou benéficos que poderiam ser: agências governamentais são os maiores compradores de "explorações de dia zero" – vulnerabilidades de *software* que, por exemplo, ainda não são conhecidas pelo fornecedor –, por lhes permitirem acesso aos bens estratégicos de forças rivais. Portanto, podem existir conflitos de interesse dentro de organizações de serviços secretos, do exército e de outras organizações governamentais que resultem em tensões desconfortáveis e incentivos gerais ambíguos.

A NOVA AGENDA PARA O NOVO CENÁRIO DE CIBERSEGURANÇA

O tema corrente ao longo de todo este capítulo, ao examinar os aspectos sociais e econômicos da cibersegurança, é a necessidade de que uma gama mais ampla de atores reconsidere as abordagens para se alcançar uma maior cibersegurança. As abordagens convencionais, desenvolvidas desde a era do *mainframe*, seguidas por computadores pessoais, eram dominadas pela comunidade técnica de segurança computacional e relativamente centradas nas equipes de suporte de informática de governos, empresas e da indústria, bem como prestadores de serviços, como os bancos. A Internet do século XXI tem colocado os usuários cada vez mais no centro das abordagens à cibersegurança, enquanto o papel do especialista de computação está sendo limitado pelo entendimento dos usuários.

Usuários de Internet são diversificados e, talvez, tenham modelos mentais muito simplistas ou até equivocados sobre comportamentos *on-line* seguros e inseguros (Dutton, 2017); toda-

12 Recuperado de https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

via, precisam ser compreendidos pela comunidade de segurança, como operadoras de redes, que são outro ator-chave para aumentar a segurança (Wash & Rader, 2011). Similarmente, desenvolvedores de aplicativos e de *software* têm um papel crítico, mas nem sempre seguem práticas de *design* seguras ou estão cientes sobre o conhecimento e as práticas de seus usuários. Além disso, abordagens em desenvolvimento estão sendo organizadas na era da Internet da computação decentralizada e centrada no usuário, em que o papel de especialistas de computação está cada vez mais limitado, e o papel do usuário e de uma ampla gama de outros atores cresce consideravelmente no novo ecossistema da Internet.

Perante tais circunstâncias, existem novas formas de abordar os desafios emergentes para a cibersegurança ao aumentar o foco nas dimensões econômicas e sociais dos problemas, as quais incluem:

- entender o papel de uma multiplicidade de usuários no novo cenário da Internet;
- aprender sobre os custos e benefícios reais e percebidos que moldam o comportamento desses atores;
- mapear a estrutura de incentivos subjacente às respostas de cibersegurança, de forma a nortear iniciativas de políticas públicas projetadas para reestruturar incentivos; e
- descrever as atitudes, as crenças e as práticas de usuários para permitir que *software* e sistemas de cibersegurança sejam projetados em harmonia com as expectativas e os comportamentos de usuários.

RUMOS PARA O FUTURO: A NOVA AGENDA DE CIBERSEGURANÇA

CAPACITAÇÃO EM CIBERSEGURANÇA

Em todos os âmbitos – nacional, organizacional e individual – há uma necessidade de capacitação para manter a segurança *on-line*. Atualmente, os elementos da capacitação em cibersegurança são identificados por meio de vários projetos e esforços colaborativos, como o Modelo de Capacitação em Cibersegurança de Oxford (Oxford Cybersecurity Capacity Building Model), grupo que defende uma abordagem de múltiplos níveis, incluindo: o uso das tecnologias para controlar riscos; a construção de habi-

lidades cibernéticas, desde a força de trabalho até a liderança; a criação de marcos legais e regulatórios efetivos, incluindo defesas e políticas públicas cibernéticas; e o incentivo a uma cultura cibernética responsável dentro da sociedade[13].

Existe uma crescente percepção da falta de conhecimento sobre cibersegurança. Muitos departamentos de ciência da computação na América do Norte e na Europa Ocidental têm um programa de cibersegurança ou segurança computacional há anos, e um número cada vez maior de cursos tem como foco essa questão. Entretanto, ainda existem lacunas de habilidades, na maioria dos países, e uma clara necessidade de aumentar o número de especialistas em cibersegurança em todo o mundo e de expandir o currículo para aumentar o foco nos usuários e nos aspectos sociais e econômicos da cibersegurança.

De forma semelhante, o montante dos orçamentos corporativos e de outros orçamentos organizacionais alocados diretamente à cibersegurança costuma ser insuficiente. Essa função tende a ser considerada não só como de baixa prioridade, mas também como uma ameaça à atividade principal da organização e uma "unidade de prevenção de negócios"[14]. Logo, há uma necessidade óbvia de mudar a imagem da cibersegurança, à medida que se torna cada vez mais um aspecto central da reputação da corporação ou organização.

DESIGNS DE SEGURANÇA MAIS REALISTAS CENTRADOS NO USUÁRIO

Em vez de culpar os usuários por não aderirem a diretrizes impossíveis de proteção de sistemas, como a memorização de múltiplas senhas, os sistemas precisam ser projetados para que usuários consigam manejá-los melhor. Usuários, desde estudantes até aposentados, quase nunca estão interessados na cibersegurança em si: querem fazer o que precisam fazer *on-line*, seja ouvir música, declarar impostos ou entrar em contato com a família. Se é preciso lidar com segurança, desejam algo conveniente, simples, fácil de usar e que funcione

13 Essas dimensões estão descritas em detalhes no *website* do projeto. Recuperado de http://www.oxfordmartin.ox.ac.uk/cybersecurity/dimensions/

14 Esse argumento foi abordado por um especialista de cibersegurança em uma conferência, mas ao qual não conseguimos atribuir a citação.

em todos os lugares, objetivo que, talvez, seja impossível de ser atingido por completo, embora seja nessa direção que o *design* dos sistemas deve convergir.

De forma mais geral, é necessário que mais trabalhos sejam direcionados à interação humanos-computadores, que abordem a área da segurança e envolvam pesquisas comportamentais sobre o que os usuários fazem de fato.

APRENDIZAGEM E EDUCAÇÃO: A TRANSIÇÃO DA PROMOÇÃO DO MEDO À EDUCAÇÃO DOS USUÁRIOS

Não obstante iniciativas de cibersegurança, comumente, possuam um componente de conscientização pública, este tende a assustar os indivíduos para que aumentem a proteção de sua segurança *on-line*. De forma geral, campanhas de medo não funcionam, em parte porque não dão instruções claras e práticas sobre o que fazer. Essa abordagem é difícil, pois há poucas estratégias convencionais para que os usuários sigam. Ademais, as campanhas podem ter consequências negativas, como minar a confiança no uso da Internet para atividades sociais e comerciais, o que comprometeria o seu uso em geral; ou, diferentemente, podem levar a brechas digitais crescentes, à medida que os usuários que restam à margem, como os idosos, podem assustar-se, enquanto usuários mais experientes permanecem confiantes.

Além disso, é importante encontrar formas para ir além de "campanhas" que tornem a cibersegurança uma parte essencial de uma educação e uma aprendizagem básicas e duradouras.Ensinamos as pessoas como escrever, elaborar cartas, falar para um grupo; porém raramente treinamos as crianças para usarem *e-mails*, mídias sociais e tecnologias relacionadas de forma segura, ética e apropriada. A aprendizagem de como usar a Internet apropriadamente, de forma a reduzir o dano potencial a outros e respeitar a dignidade dos demais usuários, precisa ser uma parte central de programas educacionais permanentes. Alguns riscos inerentes à mídia social, como o *cyberbullying* e o *sexting*, exigem que usuários identifiquem e entendam os riscos potenciais e saibam como minimizá-los. Assim, todos os aspectos da cibersegurança precisam ser incorporados nessa aprendizagem permanente sobre o uso apropriado e seguro da Internet e das TIC relacionadas.

De modo ideal, o aprendizado e a educação, reforçados por meio de normas e pressões sociais, poderiam levar ao desenvolvimento de uma "mentalidade de cibersegurança" (Dutton, 2017). Usuários da Internet podem desenvolver uma mentalidade que torne a segurança um aspecto automático de seu uso. Esta é uma mudança cultural, mas é possível e será facilitada se a segurança for melhor concebida para os usuários.

Além de usuários individuais, a educação e o aprendizado são cada vez mais importantes para micro, pequenas e médias empresas. Uma proporção muito grande de empresas é classificada nessa categoria, cujo uso da Internet e do comércio *on-line* é vital para o desenvolvimento econômico. Sendo assim, organizações nacionais e internacionais podem ter um papel essencial ao fornecer a essas empresas um senso genuinamente mais forte de segurança e um entendimento sobre como se proteger na área da cibersegurança.

REESTRUTURANDO OS INCENTIVOS

Alguns atores no ecossistema de cibersegurança têm fortes incentivos. Os *spammers* têm incentivos financeiros concretos (Krebs, 2014); analogamente, compara-se ao operador de *telemarketing*, que pode obter uma resposta positiva de uma baixa porcentagem dos alvos de uma mensagem de *marketing*; porém, considerando o baixo custo de se alcançar esse mercado e o valor das vendas, o esforço é altamente rentável. De igual modo, muitos *spammers* continuam devido a incentivos econômicos por trás de suas atividades. Além disso, é evidente que a equipe de TI encarregada de proteger a segurança de computadores também é altamente motivada, pois seus empregos dependem de seu desempenho.

Contudo muitos atores na ecologia da Internet não têm fortes incentivos para priorizar a cibersegurança, ou exigem que outros, na cadeia de valor, forneçam-lhes segurança (por exemplo, operadoras de rede argumentam que os usuários são responsáveis, enquanto os usuários dizem o contrário). Frequentemente, os custos da falta de segurança são externalizados, em virtude de os indivíduos perceberem que alguns se beneficiam enquanto outros pagam os custos, como o banco ou a empresa de cartão de crédito, ou a sociedade como um todo.

Além disso, a experiência costuma ser mais forte que preocupações racionais. Nossas próprias pesquisas apontaram que a Internet é uma "tecnologia de experiência", ou seja, usuários confiam mais na Internet à medida que adquirem mais experiência com ela. Entretanto, experiências ruins *on-line* podem diminuir essa confiança (Blank & Dutton, 2011), e há evidências de preocupações crescentes sobre privacidade e vigilância que podem erodir a confiança na Internet (Dutton, Law, Bolsover, & Dutta, 2014).

Novos mecanismos, como seguros de cibersegurança, precisam ser elaborados para reestruturar esses incentivos, a fim de que mais atores percebam ser de seu interesse proteger sua própria cibersegurança. Um seguro, por exemplo, torna os usuários mais responsabilizados por sua própria segurança, como prêmios de seguro que dependem de sua habilidade de autoproteção; dessa forma, cria um incentivo para bons comportamentos. Pode haver outros incentivos além de se ganhar ou perder dinheiro, como perder um serviço associado a práticas inseguras ou ser forçado a atualizar uma senha para restaurar um serviço de *e-mail*. Todas essas estratégias têm riscos potenciais, como prejudicar usuários marginalizados e aprofundar o hiato digital, por isso é crítico explorar formas de reestruturar os incentivos por trás da cibersegurança.

TORNANDO A CIBERSEGURANÇA UM ASPECTO DA GOVERNANÇA DA INTERNET LOCAL E GLOBAL

A cibersegurança não pode ser alcançada sem políticas e práticas cada vez mais globais: isso é um desafio tanto cultural como de governança, pois os países não priorizam da mesma forma valores-chave e interesses e práticas, por exemplo, a importância da anonimidade. Logo, é preciso criar espaços para resolver essas diferenças culturais e coordenar respostas internacionais.

Embora algumas medidas na direção da "localização de dados" sejam restritivas e prejudiquem os benefícios da Internet global (Bauer, Lee-Makiyama, van der Marel, & Verschelde, 2014), outras podem permitir mais flexibilidade local e internacionalmente. Por exemplo, a Internet não exige que todos os países operem usando um menor denominador comum; às vezes, os bancos precisam garantir ao governo e a seus clientes que estão sujeitos a certo regime regulatório; dessa forma, contratam serviços em nuvem para manterem seus dados nas

suas fronteiras nacionais. Governos também podem regionalizar alguns serviços que tenham atributos não permitidos por outras jurisdições, como o direito à anonimidade para o discurso político. Logo, em vez de tratar todos os dados e as informações da mesma maneira, a Internet tem uma maleabilidade enorme que permite soluções criativas para abordar questões locais e internacionais de privacidade, liberdade de expressão e cibersegurança.

EQUILIBRANDO A CIBERSEGURANÇA COM A ECOLOGIA MAIS AMPLA DE ESCOLHAS DE POLÍTICAS DE INTERNET

É impossível abordar a cibersegurança como uma questão pontual quando, de fato, está ligada a muitos fatores relacionados em uma ecologia ampla de escolhas de políticas, como aquelas relativas à privacidade, vigilância e liberdade de expressão. A maioria das partes interessadas não quer apenas promover uma Internet segura, mas sim uma Internet global, aberta e segura; portanto, um desvio do foco na cibersegurança pode comprometer outros valores e interesses.

A missão e o conhecimento de especialistas de cibersegurança precisam ser cada vez mais equilibrados com os objetivos e o conhecimento daqueles com outros papéis e outros tipos de especialidade nas áreas do Direito, de políticas públicas e do uso da Internet e mídias relacionadas. Algumas grandes empresas comerciais, por exemplo, têm conseguido fornecer acesso prático para compras *on-line* e pagamentos seguros, de formas relativamente confiáveis e fáceis de usar.

Finalmente, é necessário demonstrar claramente que a cibersegurança tem se tornado um requisito ou uma condição necessária para proteger a privacidade, por exemplo, assim como a vitalidade financeira e a reputação de uma empresa. A cibersegurança precisa ser percebida como um facilitador de outros objetivos, em vez de conflitante com a sua realização; no entanto, requer desenhos de sistemas que considerem as habilidades, as atitudes e os comportamentos de seus usuários.

CONCLUSÃO

A Internet e as TIC relacionadas são cada vez mais centrais à prosperidade econômica de países desenvolvidos e daqueles em desenvolvimento. Contudo, os benefícios da Internet e de tecnologias relacionadas dependem da manutenção de um alto nível de segurança, confiança e abertura de uma Internet global. Ao mesmo tempo que a Internet pode empoderar indivíduos, organizações e países do mundo em desenvolvimento, em uma economia cada vez mais global, ela também parece ter a mesma capacidade de empoderar atores hostis e maliciosos, com fortes incentivos econômicos e sociais para seguir com seus ataques. Claramente, êxito requer esforços globais para endereçar os desafios da cibersegurança; assim, uma pergunta central, no âmbito mundial, é: como o mundo pode usufruir dos enormes benefícios econômicos e sociais da Internet ao mesmo tempo que garante sua segurança?

Não há uma solução para a cibersegurança – nenhum *Deus Ex Machina* no horizonte. Ela é um alvo dinâmico e exige um conjunto de processos em contínua evolução para conter os riscos de segurança associados ao uso da Internet e das mídias digitais relacionadas. Seguir adiante com o desenvolvimento desses processos será inevitavelmente uma questão de adaptar e melhorar progressivamente abordagens existentes, situação apontada por organizações como "incremental", em vez de buscar uma solução abrangente e racional.

Há diversos atores e problemas de segurança em todo o mundo e em todas as plataformas; dessa forma, não é possível uma solução global simples e única para a cibersegurança. Considerando a natureza dinâmica e a complexidade dos avanços na área, é preciso aceitar um processo de longo prazo de decisões incrementais que permitam a atores encontrar, produtivamente, melhores soluções no decurso do tempo. Nesse sentido, o presente artigo aponta algumas possibilidades para avançar nas abordagens atuais de cibersegurança, incluindo a revitalização de campanhas de conscientização pública, ao mudar o foco da promoção do medo entre usuários ao fornecimento de dicas para lidar com os problemas. Essas abordagens sugerem uma nova agenda para um cenário dinâmico de cibersegurança.

Apesar de o potencial econômico e social da Internet ser bastante extenso para todos os países – tanto os desenvolvidos como

aqueles em desenvolvimento, cada vez mais esses benefícios estão em risco de falhar diante dos perigos associados à falta de segurança e aos níveis decrescentes de confiança na Internet e naqueles que administram e exploram essa tecnologia em todo o mundo. Há diversas abordagens que questionam se estaríamos em uma "bolha de confiança" na Internet (Dutton et al., 2014); todavia, há também caminhos óbvios pelos quais a cibersegurança pode ser melhor abordada, uma vez reconhecidos os novos aspectos da cibersegurança em um mundo digitalmente conectado e a centralidade dos usuários nessa nova ecologia de escolhas que moldam o futuro da Internet.

REFERÊNCIAS

Anderson, R., & Moore, (2006, 27 de outubro). The economics of information security. *Science,* 314(5799), 610-613. doi 10.1126/science.1130992.

Asghari, H., Van Eeten, M. J. G., & Bauer, J. M. (2016). The Economics of Cybersecurity. In Bauer, J. M., & Latzer, M. (Eds.). *Handbook on the Economics of the Internet* (pp. 262-287). Cheltenham, UK; Northampton, MA: Edward Elgar.

Bauer, M., Lee-Makiyama, H., van der Marel, E., & Verschelde, B. (2014). *The Costs of Data Localisation: Friendly Fire on Economic Recovery.* ECIPE Occasional Paper, n. 3. Bruxelas, BE: ECIPE. Recuperado de https://ecipe.org/publications/dataloc/

Blank, G., & Dutton, W. H. (2011). Age and Trust in the Internet: The Centrality of Experience and Attitudes Toward Technology in Britain. *Social Science Computer Review, 30*(2), 135-151.

Burt, D., Nicholas, P., Sullivan, K., & Scoles, T. (2014). *The Cybersecurity Paradox: Impact of Social, Economic, and Technological Factors on Rates of Malware.* Microsoft Security Intelligence Report. Recuperado de http://download.microsoft.com/download/E/1/8/E18A8FBB-7BA6-48BD-97D2-9CD32A71B434/Cybersecurity-Risk-Paradox.pdf

Clark, D., Berson, T., & Lin, H. S. (Eds.). (2014). *At the Nexus of Cybersecurity and Public Policy.* Computer Science and Telecommunications Board, National Research Council, Washington DC, VA: The National Academies Press.

DeNardis, L. (2014). *The Global War for Internet Governance.* New Haven, CT; Londres, UK: Yale University Press.

Dutta, S., Dutton, W. H., & Law, G. (2011, abril). *The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online: The Global Information Technology Report 2010-2011*. New York City, NY: Fórum Econômico Global. Recuperado de http://ssrn.com/abstract=1810005

Dutton, W. (2017). Fostering a Cyber Security Mindset. *Internet Policy Review, 6*(1). DOI: 10.14763/2017.1.443. Recuperado de https://policyreview.info/node/443/pdf

Dutton, W. H., & Meadow, R. G. (1987). A Tolerance for Surveillance: American Public Opinion Concerning Privacy and Civil Liberties. In Levitan, K. B. (Ed.). *Government Infostructures* (pp. 147-170). Westport, CT: Greenwood Press.

Dutton, W. H., Law, G., Bolsover, G., & Dutta, S. (2014). *The Internet Trust Bubble: Global Values, Beliefs and Practices*. New York City, NY: Fórum Econômico Global. Recuperado de http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf

Gordon, L. A. & Loeb, M. P. (2005). *Managing Cybersecurity Resources: A Cost-Benefit Analysis*. Columbus, OH: McGraw-Hill.

Krebs, B. (2014). *SPAM Nation*. Naperville, IL: Sourcebooks, Inc.

Moore, T., Clayton, R. & Anderson, R. (2009). The Economics of Online Crime. *Journal of Economic Perspectives, 23*(3), 3-20.

National Research Council (NRC). (1991). *Computers at Risk: Safe Computing in the Information Age*. System Security Study Committee, Commission on Physical Sciences, Mathematics, and Applications. Washington DC: The National Academies Press. Recuperado de https://www.nap.edu/catalog/1581/computers-at-risk-safe-computing-in-the-information--age

National Research Council (NRC). (2002). *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Computer Science and Telecommunications Board, Division of Engineering and Physical Sciences. Washington, DC: National Academy Press. Recuperado de https://citadel-information.com/wp-content/uploads/2012/08/cybersecurity-today-and-tomorrow-pay-now-or-pay-later-national-research-council-2002.pdf

Orji, U. J. (2012). *Cybersecurity Law and Regulation*. Nijmegen, NL: Wolf Legal Publishers.

Shalhoub, Z. K., & Al Qasimi, S. L. (2010). *Cyber Law and Cyber Security in Developing and Emerging Economies*. Cheltenham, UK; Northampton, MA: Edward Elgar.

Van Eeten, M. J. G., & Bauer, J. M. (2013). Enhancing Incentives for Internet Security. In Brown, I. (Ed.). *Handbook of Internet Governance* (pp. 445-484). Cheltenham, UK: Edward Elgar.

Van Eeten, M. J. G., Bauer, J. M., Asghari, H., & Tabatabaie, S. (2010). *The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data*. STI Working Paper 2010/5. Paris, FR: OECD.

Varian, H. (2004). System Reliability and Free-Riding. In Camp, L. J., & Lewis, S. (Eds.), *Economics of Information Security* (pp. 1-15). Berlin, DE; New York City, NY: Springer.

Wash, R., & Rader, E. (2011, setembro). Influencing Mental Models of Security. *Proceedings of the New Security Paradigms Workshop (NSPW), 11,* 57-66. Recuperado de https://dl.acm.org/doi/10.1145/2073276.2073283

Weizenbaum, J. (1976). *Computer Power and Human Reason: From Judgment to Calculation*. San Francisco, CA: W. H. Freeman and Company.

CAPÍTULO 2

Gestão de riscos cibernéticos para pequenas e médias empresas

Éireann Leverett[1]

Medir é saber.
JAMES CLERK MAXWELL, 1831-1879

1 Éireann Leverett é fundador da Concinnity Risks, uma consultoria boutique sobre risco cibernético. Ele também é pesquisador sênior de Risco do Centro de Estudos de Risco da Universidade de Cambridge e coautor de Solving Cyber Risk. Éireann gosta de quantificar os riscos cibernéticos, colaborar com equipes de resposta a incidentes, fazer longas caminhadas na floresta e aprender sobre forrageamento e navegação natural.

Para jogar melhor, é preciso marcar pontos; para marcar pontos, é preciso medir. Embora pareça óbvio, qual abordagem pode ser usada para medir a gestão de riscos cibernéticos para pequenas e médias empresas (PME)? Muito do que se passa com computadores e dados é invisível, e só é possível gerir os riscos corretamente quando se encontra uma maneira fácil de medi-los.

Este artigo é uma introdução à gestão de riscos cibernéticos; nesse sentido, embora investigue parte da quantificação e da literatura acadêmica por trás dessa ideia, também é um guia prático e útil para aqueles que têm interesse na gestão de riscos cibernéticos.

POR QUE MEDIR DANOS CIBERNÉTICOS?

Se você nunca foi *hackeado,* é difícil acreditar que isso possa acontecer. Caso você não tenha perdido sua empresa devido a ataques cibernéticos, isso pode lhe parecer apenas um inconveniente e não uma ameaça existencial. A maioria das pessoas acredita que o dano cibernético seja apenas virtual, sem consequências no mundo real, contudo certamente não é o caso.

Há pessoas que já perderam centenas de milhões de dólares[2], todo o seu negócio[3] e até suas vidas devido a erros de *software*[4]. Os marca-passos apresentam falhas de codificação e segurança[5], bondes já sofreram acidentes causados por crianças[6] e centenas de milhares de pessoas já passaram por apagões de eletricidade[7] [8], assim como milhares de galões de esgoto foram liberados[9], *drones* desviados de seu caminho[10] e o enri-

2 Recuperado de https://www.bbc.co.uk/news/business-19116715
3 Recuperado de https://en.wikipedia.org/wiki/DigiNotar
4 Recuperado de https://en.wikipedia.org/wiki/Therac-25
5 Recuperado de https://cra.org/ccc/wp-content/uploads/sites/2/2015/11/Kevin-Fu-Medical-Device-Security.pdf
6 Recuperado de https://www.wired.com/2008/01/polish-teen-hac/
7 Recuperado de https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack
8 Recuperado de https://www.bbc.com/news/technology-38573074
9 Recuperado de https://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill
10 Recuperado de https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident

quecimento nuclear interrompido[11]. É essencial que as pessoas compreendam que os riscos cibernéticos podem causar danos: têm consequências de amplo alcance no mundo real porque os computadores estão continuamente sendo colocados no centro dos sistemas construídos no mundo (Anderson, Leverett, & Clayton, 2017).

A medição dos danos é essencial para essas questões; sem ela, esses prejuízos não são documentados e pode-se criar uma sensação geral de que os danos cibernéticos não existem. Os exemplos citados deixam claro que os danos cibernéticos podem ser reais e físicos, e representar ameaças existenciais, visto que impactam empresas, grupos da sociedade civil e indivíduos. O primeiro passo para se entender a dimensão do problema é medir ou buscar medições já implementadas.

O QUE ESTÁ SENDO MEDIDO ATUALMENTE E O QUE DEVERIA SER MEDIDO?

Grupos de Resposta a Incidentes de Segurança, como o CERT.br[12], mantêm registros de incidentes cibernéticos, amplificadores de DDoS[13], servidores de DNS maliciosos[14], *honeypots*[15] e *spam*. Embora essas métricas possam ser úteis para oferecer um panorama mais amplo sobre o tema do dano cibernético, que outras medidas estão faltando? Como seria possível coletar mais métricas de forma que continuem a ser úteis em longo prazo?

O Quadro 1 apresenta sete princípios da construção de métricas para o risco cibernético que podem ser úteis para

---

11 Recuperado de https://en.wikipedia.org/wiki/Stuxnet

12 O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br) – braço executivo do Comitê Gestor da Internet no Brasil (CGI.br). O CERT.br é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil. O centro atua como um ponto central para notificações de incidentes de segurança, provendo a coordenação e o apoio necessários para as organizações envolvidas em incidentes. Recuperado de https://www.cert.br/stats/

13 Um amplificador DDoS é um computador que responde com mais dados do que aqueles enviados pelo usuário. Fundamentalmente, ele também deve estar aberto a desvios: por exemplo, se eu enviar uma carta fingindo ser você e assinando milhares de revistas gratuitas, minha única carta é "amplificada" e você estará fazendo muitas viagens para o centro de reciclagem. Pense nisso como alguém maliciosamente fazendo você trabalhar duro para limpar sua bagunça. Recuperado de https://www.cert.br/stats/amplificadores/

14 Um servidor DNS malicioso fornece respostas incorretas para nome(s) de domínio(s) de instituições-vítima, em geral instituições financeiras, de comércio eletrônico, redes sociais e/ou domínios bastante conhecidos. Seu propósito é direcionar os usuários para *sites* falsos. Recuperado de https://www.cert.br/stats/dns-malicioso/

15 Um *honeypot* é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido. Recuperado de https://www.cert.br/stats/honeypots/

gerenciar riscos e começar a quantificá-los. Por exemplo, a pergunta "A contagem de incidentes é um efeito do número de incidentes ou do número de respostas a incidentes?" pode ser respondida ao aplicar de forma hábil os sete princípios da construção de métricas para o risco cibernético, que podem ser usados em sobreposição.

QUADRO 1 - SETE PRINCÍPIOS DA CONSTRUÇÃO DE MÉTRICAS PARA O RISCO CIBERNÉTICO

Princípio 1: Razões
É essencial que os dados corretos sejam medidos e que as medições sejam feitas de forma que continuem úteis à medida que novos riscos e danos surgirem. O método utilizado para medir o risco cibernético e as inevitáveis implicações e vieses relativos a essa escolha são muito importantes e devem ser considerados. De acordo com Eric Jardine (2018), é essencial "considerar o denominador". Em outras palavras, ao contabilizar os incidentes cibernéticos, é preciso contrabalançar o número de incidentes com o tamanho da população daquela equipe, ou melhor, com o tamanho da população de usuários de Internet[16] [17].

Princípio 2: Considerar o crescimento do denominador
As métricas de risco precisam de proporções; dessa forma, é importante considerar o crescimento tanto do numerador como do denominador dessas razões. Nesse contexto, ao medir os riscos cibernéticos, é preciso considerar que a população cresce de três maneiras diferentes: *(i)* de forma geral, a população mundial: consequentemente, o número de usuários de Internet também; *(ii)* o número total de computadores de todos os tipos – computadores de mesa, *notebooks*, telefones celulares, dispositivos conectados à Internet das Coisas; *(iii)* o número de computadores conectados à Internet. Verificam-se três motivos também distintos: primeiro, a cada dia, mais conexões de Internet se tornam possíveis; segundo, os endereços de IPv6 – uma nova forma de endereços usada na Internet – são vastamente maiores que espaços de IPv4[18]; terceiro, há uma série cada vez mais vertiginosa de domínios genéricos de primeiro nível e entradas de DNS[19]. Todos esses fatores podem contribuir para o veloz crescimento do número total de incidentes, os quais criam um denominador muito dinâmico que deve ser registrado cuidadosamente.

16 Ao considerar o número de usuários da Internet, é preciso ter em mente que isso inclui a grande quantidade de pessoas que usam serviços por meio do telefone celular, mas que não têm conexão à Internet em casa.
17 Uma fundamentação estatística e teórica das medidas está disponível em: https://www.statsdirect.com/help/basics/measurement_scales.htm
18 IPv6 é a versão mais atual do Protocolo de Internet. O principal motivo para a implantação do IPv6 na Internet é a necessidade de mais endereços, porque a disponibilidade de endereços livres IPv4 terminou.
19 Um domínio genérico de primeiro nível (DPN) é a parte depois do ponto, por exemplo, org ou net. Uma entrada de DNS é uma base de dados que mapeia os URL para uso humano a endereços de IP. Quando alguém digita um URL, como google.com, essa entrada é enviada a um provedor de serviço de Internet, para ser encaminhada a servidores DNS e, em seguida, direcionada ao servidor Web correto, usando o endereço correspondente de IP como rótulo.

Princípio 3: Registros de trabalho
Além de manter medições com uma estrutura reconhecida de razões, também é importante ter métricas sobre dinheiro, esforço e tempo dispendidos. Isso inclui a duração de um incidente, a quantidade de recursos gastos e o número de partes externas envolvidas na reparação.

Princípio 4: Classificação
Às vezes, não é possível quantificar um risco, ou múltiplos riscos, de forma precisa. Quando não é possível dar um escore ao risco, outra possibilidade é classificá-lo em uma ordem. Isso pode ser realizado com a opinião de especialistas ou de grupos de discussão. Uma classificação simples de dano, risco, ameaça ou impacto é, geralmente, o primeiro passo no sentido da quantificação do risco.

Princípio 5: Redução e desativação
Uma boa métrica de risco deve ser capaz tanto de crescer como de decrescer. Uma lista de perigos deve permitir a exclusão de itens, assim como sua inclusão. Na prática, ao combinar medidas para formar uma métrica ou um escore de risco, um trabalho teórico básico deve ser realizado de forma a mostrar que os números podem cair e também aumentar. Isso pode ser feito ao elencar os critérios a serem atendidos antes de um risco ser acrescentado à lista, como também os critérios para que o risco seja removido, podendo retornar posteriormente como dado, o que é aceitável. Porém, o ponto principal da gestão de risco é priorizar os riscos incertos, especialmente aqueles com o maior impacto. A certeza pode, portanto, ser acrescentada aos riscos possíveis, assim como para tomar as melhores decisões.

Princípio 6: Cuidado com a média, considere a variância
Embora médias possam servir como atalhos úteis, nem sempre podem ser aplicadas com sucesso para alcançar um resultado preciso. Ao tentar aplicar uma média, é importante sempre relatar a variância[20] e entender que tipo de distribuição está sendo estudada (por exemplo, se é uma distribuição normal padronizada).

Princípio 7: Reconhecer os vieses
Os vieses existem em todas as medidas e devem ser reconhecidos e documentados; desse modo, um bom analista de risco sempre observa os vieses presentes em uma métrica antes de aplicá-la a uma decisão. É preciso estudar tanto as falácias lógicas[21] como os vieses cognitivos[22] para entender seus impactos sobre as medidas: em vez de negar o viés ou a ocorrência de uma falácia lógica, é necessário aprender a identificá-los, documentá-los e reconhecer quando terão impacto sobre uma tarefa determinada.

---

20 A variância mede o nível médio em que cada dado difere da média aritmética – a média de todos os pontos de dados.
21 Recuperado de https://yourlogicalfallacyis.com/
22 Recuperado de https://yourbias.is/

RISCO DE *COMPLIANCE*

Uma das primeiras coisas que a maioria das organizações aborda na gestão de riscos é *compliance*. Este é um risco conhecido e que geralmente tem consequências mensuráveis, ou pelo menos limitadas.

Estar em *compliance* costuma ser uma questão de criar bons hábitos ou um procedimento seguido por todos na organização. A auditoria ou outros métodos podem ser usados para verificar *compliance* regularmente, assim como para comunicar a importância do risco para outros na organização[23]. Um bom exemplo são as organizações que processam cartões de créditos *on-line*, as quais devem cumprir com os requisitos do PCI-DSS, o que significa, em suma, que seguem uma maneira prescrita de processar dados de cartões de crédito e outros dados de pagamento. Na prática, o risco de *compliance* é muito importante, visto que os criminosos cibernéticos no Brasil se concentram muito nas fraudes de cartão de crédito. Isso significa que, se os dados do cartão de crédito de uma pessoa forem roubados, eles provavelmente são armazenados ou transferidos como parte das operações da organização.

MARCOS LEGAIS

É importante que as organizações verifiquem se estão agindo de acordo não apenas conforme leis e os regulamentos locais, mas também de acordo com leis estrangeiras e padrões internacionais. Elas precisam conhecer a legislação relevante, a fim de considerar o funcionamento de sua organização e o que poderia dar errado caso entrem em conflito com essas leis. Se esse processo for feito o suficientemente bem, as organizações podem começar a manter um escore por meio da medição do risco e, mais importante, de quanto esforço é preciso para reduzir esses riscos a uma quantidade mensurável. Essa ideia está no cerne da gestão de risco: quanto trabalho deveria ser feito para quanta redução de risco?

Conhecer as leis e suas sanções é, portanto, muito importante para entender os riscos de violação de dados mais comuns. No contexto brasileiro, as leis que se aplicam à maioria das pequenas empresas são:

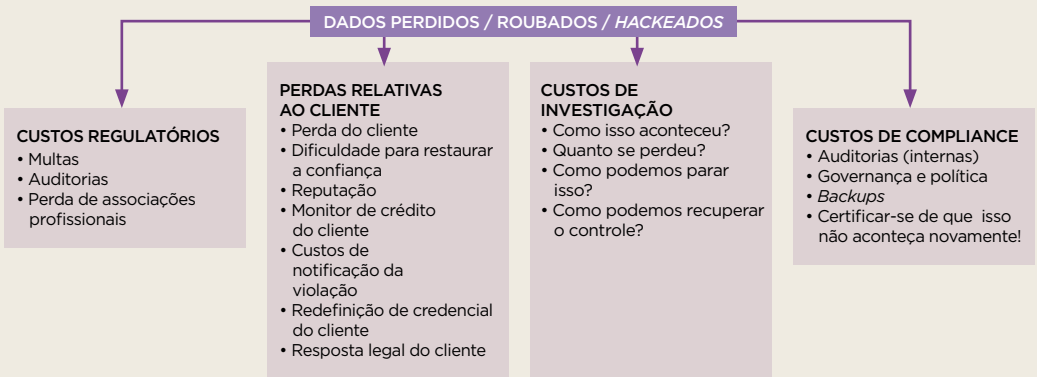
- O Marco Civil da Internet (Lei nº 12.965);

23 Há uma vasta literatura sobre a gestão de riscos de *compliance*. Por exemplo, Romanosky, Ablon, Kuehn e Jones (2017) analisam os conteúdos de apólices de seguro para riscos cibernéticos para entender o que é ou não coberto e como as seguradoras abordam o risco por meio de questionários que enviam a potenciais clientes.

- A Lei da Propriedade Industrial (Lei nº 9.279);
- A Lei do *Software* (Lei nº 9.609);
- A Lei Geral de Proteção de Dados Pessoais (LGPD);
- O Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation – GDPR[24]) da União Europeia; e
- O Padrão de Segurança de Dados da Indústria de Pagamentos com Cartões de Crédito (Payment Card Industry Data Security Standard – PCI-DSS[25]).

É importante mapear como essas leis podem se aplicar a empresas ou organizações específicas. Por exemplo, ao considerar os clientes de uma organização e todos os dados sobre eles, incluindo o valor que pagam para essa organização, deve-se verificar como esse tipo de informação provavelmente será coberto pela LGPD e quantos dados são manejados e armazenados. Nesse contexto, o que poderia dar errado e como seria possível consertar esse problema? Quanto que a reparação custaria em comparação com a prevenção? Se o risco não puder ser prevenido, é possível reduzir as perdas por meio de um guia pré-elaborado de resposta a violações? Essas são perguntas essenciais que precisam ser respondidas pelas organizações.

COMO A PERDA DE DADOS TRAZ CUSTOS FINANCEIROS PARA MINHA ORGANIZAÇÃO?



FONTE: ELABORADO PELO AUTOR.

24 O GDPR é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia (UE) e Espaço Económico Europeu (EEE), criado em 2018. Regulamenta também a exportação de dados pessoais para fora da UE e EEE. O regulamento tem como objetivo dar aos cidadãos e residentes formas de controlar os seus dados pessoais e unificar o quadro regulamentar europeu.

25 Padrão de segurança da informação para organizações que lidam com cartões de crédito de marca dos principais esquemas de cartões.

Nesse cenário, o primeiro passo para gerenciar os riscos cibernéticos é descobrir a quais leis que a organização deve obedecer. Também é essencial considerar as leis nos países de residência dos clientes ou fornecedores da organização, como o GDPR.

QUADRO 2 - GESTÃO DE RISCOS DE *COMPLIANCE*

O *checklist* a seguir pode ser usado como um ponto de partida para gerenciar os riscos de *compliance* de uma organização:

- Realizar *backups* de dados críticos;
  - *On-line*
  - *Off-line*
- Realizar verificação dupla de contas bancárias e faturas por telefone;
- Treinar funcionários sobre fraudes locais comuns e incentivar discussões;
- Usar um antivírus e entender que nem sempre é suficiente;
- Formar uma cooperativa para discutir riscos cibernéticos com outras pequenas empresas locais;
- Pensar sobre como a empresa conseguiria funcionar sem dados ou sem Internet;
- Pensar sobre como restaurar a empresa a partir de uma pequena quantidade de dados ou como reconstruir algo em funcionamento.

O último item é particularmente importante, pois muitas empresas se importam tanto com o crescimento e a continuação das operações que não praticam a reconstrução quando algo não sai como o esperado. Lipson e Fisher (2001) enfatizam essa ideia:

> Muitas empresas têm planos de contingência para lidar com interrupções de negócios causadas por desastres naturais ou acidentes. Embora a maioria dos ciberataques seja de dimensão relativamente menor, um ataque aos sistemas críticos de informação em rede de uma organização tem o potencial de causar graves e prolongadas perturbações aos negócios, quer a empresa tenha sido um alvo específico ou uma vítima aleatória de um ataque amplo. Se um ciberataque perturbar as funções críticas da empresa e interromper os serviços essenciais de que dependem os clientes, então o que está em risco é a sobrevivência do próprio negócio. (p. 3)

Contudo, o tempo e os esforços para planejar uma reconstrução do zero se tornam mais simples cada vez que são praticados. Exercícios de continuidade de negócios são úteis para muitas situações e, de forma geral, trata-se de imaginar como

a organização poderia se reconstruir a partir de *backups* ou de planos antigos. Um plano de continuidade de negócios consiste em contemplar e estudar eventos antes de ocorrerem; logo, normalmente, basta passar apenas meia hora por semana lendo e entendendo os atuais riscos cibernéticos a fim de desenvolver um plano para preveni-los ou se recuperar deles.

LGPD

A nova Lei Geral de Proteção de Dados Pessoais (LGPD) foi aprovada em agosto de 2018, com vigor a partir de agosto de 2020. Empresas que já estão em conformidade com o GDPR estão no bom caminho para cumprir suas obrigações da LGPD[26]; entretanto, é necessário que todas as organizações se prepararem.

No contexto da LGPD, na próxima seção explica-se como transformar uma avaliação de risco qualitativa em uma avaliação quantitativa rapidamente. Primeiro, é preciso considerar que as multas pelo não cumprimento da legislação vão desde 2% da receita de uma organização até R$ 50 milhões, o que já revela a gravidade desse risco. Mesmo se a frequência da fiscalização de *compliance* e das multas for desconhecida, uma abordagem baseada em princípios pode ser usada para desenvolver um programa de gestão de risco melhor. Existem dois grandes princípios que podem ser usados na ausência de mais dados: *(i)* gaste até 37% do custo de um incidente que deseje prevenir (Gordon & Loeb, 2002); e, *(ii)* se não puder gastar dinheiro com o problema, dedique mais do seu tempo.

A título de exemplo, para uma organização que processa dados de cidadãos europeus como parte de suas atividades, a avaliação quantitativa dos riscos é extremamente simples. No pior dos casos, na perda de uma grande quantidade de dados, ela precisaria pagar 10 milhões de euros ou 2% de seu faturamento global, ou, se tiver um impacto ainda maior nas liberdades e direitos dos indivíduos, 20 milhões de euros ou 4% de seu faturamento global. Embora seja improvável que uma pequena empresa no Brasil incorra nessas multas, não é impossível, o que leva à seguinte reflexão sobre a proteção de dados: a organização gastaria um pouco de dinheiro extra

26 Mais informações sobre as semelhanças entre o GDPR e a LGPD estão disponíveis em: https://gdpr.eu/gdpr-vs-lgpd/

para evitar ter de, algum dia, pagar essas multas? Ou, se não for possível gastar dinheiro com isso, dedicaria um tempo extra?

Quanto deve ser gasto pela organização para a proteção de dados, segundo o GDPR? 37% de 4% é aproximadamente 1,5% de seu faturamento global, um bom começo para pequenas empresas em geral, não apenas no caso do GDPR. Também é muito próximo dos 2% da multa que podem ser aplicados sobre a LGPD: se uma organização está gastando para estar em conformidade com o GDPR, provavelmente está muito próxima de cumprir com a LGPD.

Esses gastos podem ser embutidos nos preços cobrados pela organização, e a prática de gestão de risco digital deve ser comunicada aos clientes, o que é uma forma simples de gestão da reputação. É possível também usar o tempo com atividades básicas, tais como a exclusão de senhas antigas, a verificação de arquivos de registros, a atualização de *firewalls* e a realização de *backups*. Alternativamente, uma organização poderia usar esse tempo realizando uma auditoria própria e observando o que está e não está sendo realizado para ajudar com *compliance*. Ainda que essas ações possam representar apenas 1% do tempo, é preciso que se torne um hábito regular, já que, quando feito corretamente, será possível reconstruir a empresa dentro de poucos dias após alguma possível ocorrência.

Atualmente, antigos modelos de negócios podem ser ilegais sob a LGPD: as novas regras podem afetar o modelo de negócios de uma organização, assim como seu armazenamento de dados. Por exemplo, se uma empresa armazenar dados sobre pessoas físicas ou seus hábitos de consumo, a organização deverá dedicar um tempo para entender se é possível adequar essa atividade conforme a nova legislação.

O impacto máximo de uma multa do GDPR é de 4% para uma violação grave de dados sobre clientes europeus, mais que a LGPD; entretanto, é concebível que uma organização possa ser multada sob ambas as legislações ao mesmo tempo.

Despesas para cumprir com uma legislação provavelmente ajudam a cumprir com a outra e vice-versa; assim, as organizações não precisam gastar 1,3% de seu orçamento com ambas, pois podem simplesmente focar na mitigação e redução de riscos que impactam as duas. Expresso da forma mais simples possível: **ou a empresa gasta 1,3% de seu fa-**

turamento global, ou meia hora por semana para evitar multas de até 4%.

COMPLIANCE COM O PCI-DSS

Existem regulamentos globais para qualquer organização que lida com pagamentos, tanto para assuntos internos quanto em nome de outros, cujo foco é em pagamentos com cartão de débito ou crédito, tanto *on-line* como *off-line*.

Embora estar em *compliance* com o PCI não garanta que uma organização não seja *hackeada* e perca dados de cartão de crédito ou débito de seus clientes, certamente pode protegê-la de mais multas se tal evento ocorrer. Estar em *compliance*, nesse contexto, simplesmente significa aderir às boas práticas atuais, o que representa uma defesa significativa em um tribunal ou diante de entidades regulatórias. Isso significa que a organização cobriu tudo que poderia se esperar de forma razoável. Inversamente, a falta de *compliance* implica que, além de lidar com o incidente, a organização também possa se deparar com multas e outras pressões regulatórias, como auditorias ou atrasos de pagamentos.

Como saber se uma organização precisa estar em compliance com o PCI-DSS

Como citado no Guia do Payment Card Industry[27], "o PCI é aplicável a qualquer empresa que transmita, processe ou armazene informações sobre titulares de cartões de crédito – sem exceção". Essencialmente, é muito simples saber se uma organização precisa estar em conformidade com o PCI-DSS. O uso de dados de cartão de pagamento de **qualquer** tipo, mesmo para um simples cafezinho, implica dedicar um pouco de tempo, considerando a necessidade de estar em *compliance* com o PCI. A boa notícia é que a maioria das empresas é classificada como nível 4, o que significa que processa menos de 20 mil pagamentos por ano *on-line* ou até um milhão *off-line*; assim, não são muitas exigências.

Se uma organização tem mais dinheiro do que tempo, ela pode terceirizar essas tarefas para outras organizações especializadas. Contudo, o uso de um fornecedor terceirizado não é suficiente por si só, pois será necessária uma autodeclaração, além de entender o propósito desse exercício.

---

27 Recuperado de https://www.pcicomplianceguide.org/pci-myths/

COMO CALCULAR O CUSTO DO IMPACTO

Você quer uma válvula que não vaze e você faz tudo o possível para criar uma. Mas o mundo real lhe oferece válvulas furadas. É preciso determinar quanto vazamento é tolerável.

ARTHUR RUDOLPH (1996)

A citação que abre esta seção captura uma crua realidade com a qual qualquer organização pode se identificar; mesmo caso quando se trata de risco cibernético. Como não é possível prevenir todas as coisas ruins que podem dar errado na Internet, é importante descobrir o nível de tolerância de um programa de risco cibernético. As organizações podem até alterar estrategicamente a sua tolerância ao risco cibernético em momentos diferentes do seu ciclo de vida; entretanto, para chegar a essa maturidade, é preciso ser capaz de medir o risco.

Em relação ao cálculo dos impactos do risco cibernético, como apontado, não é uma tarefa particularmente difícil quando se trata dos riscos cibernéticos na categoria de *compliance*. De fato, muitas multas são calibradas precisamente para pressionar as organizações a internalizarem os custos das violações de dados ou de fraudes de pagamento. Em outras palavras, enquanto as empresas costumavam evitar a responsabilidade dessas ocorrências, as reguladoras começam a repassar os custos, com a intenção de que as empresas aprendam a lidar com os dados com mais cuidado[28].

Não obstante calcular o impacto, às vezes, possa ser tão simples quanto pesquisar as multas máximas para a falta de *compliance*, essa abordagem pode ser mais sutil, ou eventualmente os custos serem desconhecidos. O primeiro passo, em qualquer situação, é calcular uma rápida estimativa e fazer perguntas sobre dinheiro, tempo e esforço. Por exemplo, quanto custaria se os funcionários da empresa caíssem em um golpe que os fizesse perder dinheiro? Talvez seja impossível prever essa ocorrência, todavia é possível manter o foco nas previsões mínimas e máximas. Por exemplo, o mínimo pode ser zero, visto que é possível entrar em contato com o banco imediatamente após um golpe e bloquear o pagamento. O máximo parece ser impossível de calcular, mas um bom ponto de

28 Este tipo de fenômeno está fortemente documentado na literatura de economia de segurança, como nas obras de Anderson e Moore (2006).

partida é conduzir uma rápida análise do maior valor que já se teve na conta bancária. Continuando com essa abordagem, percebe-se que a probabilidade do risco mínimo (zero) e o pagamento corporativo/bancário máximo não são iguais; dessa forma, determinar a probabilidade de cada um desses valores é um passo importante para a gestão de risco cibernético.

De acordo com Hubbard e Seiersen (2016), a quantificação de risco raramente se trata de chegar a um número exato, mas de reduzir sua incerteza. Quando uma organização tem uma gama de impactos possíveis para determinado risco cibernético e possui uma confiança razoável nesses números, ela pode começar a examinar os quatro pilares da gestão de risco (Quadro 3) como diferentes tratamentos para esses riscos.

QUADRO 3 - OS QUATRO PILARES DA GESTÃO DE RISCO

1: Evitar o risco
Gestores que tendem mais a essa abordagem são conhecidos por terem aversão ao risco, por isso, às vezes, é a maneira adequada de gerenciar certos tipos de empresas e entidades filantrópicas, já que, em outros tipos de organizações ou empresas, essa estratégia pode impedir a inovação ou o sucesso. Em suma, a tolerância ao risco pode e deve ser adaptada à missão central da organização.

2: Aceitar o risco
Essa é a forma mais comum de atuar diante dos riscos cibernéticos. A maioria das pessoas preocupa-se em como fazer a empresa ganhar dinheiro e raramente considera os riscos. Quando os considera, minimiza a possível gravidade de suas consequências e hesita em gastar tempo ou dinheiro para reduzir a incerteza.

3: Reduzir/restaurar o risco
Um bom gerente de risco sabe como pedir ajuda de várias pessoas para reduzir os riscos antes de aceitá-los. Um excelente gestor de risco examinará não apenas como prevenir um risco, mas, também, como reduzir seu impacto, caso aconteça (por exemplo, dados criptografados). Com o risco cibernético, a estratégia de restauração é, muitas vezes, ignorada: dedicam-se quase todos os esforços a programas de antivírus e *firewalls* (redução), mas poucos a planos de continuidade de negócios, planos de resposta a incidentes e criptografias de dados (restauração). Todos esses últimos tratamentos pressupõem a ocorrência de riscos, entretanto procuram reduzir seu impacto ou restaurar a empresa o mais rápido possível[29].

29 Há um amplo panorama das estratégias e da literatura sobre a redução de risco em Gordon, Loeb e Sohail (2003).

4: Transferir/compartilhar o risco
Imagine uma comunidade tão próxima e vibrante, na qual todos são dedicados uns aos outros, e que todas as empresas que apoiam seu negócio depositam algumas moedas em um pote. Esse pote seria aberto apenas em caso de dano: se você tivesse sucesso em se restabelecer, você colocaria um pouco de dinheiro no pote para uma empresa que pode estar em risco no futuro. Isso é uma cooperativa de empresas compartilhando riscos, de forma bastante criativa. Claro, elas também poderiam formar uma cooperativa de seguro em que cada empresa paga uma pequena taxa, mas conseguiriam muito mais do que aquela taxa se sofressem danos. Seguros nem sempre precisam ser fornecidos por corporações gigantes; até pequenas organizações podem formar um clube, compartilhar e transferir o risco.

TRANSFERÊNCIA DO RISCO CIBERNÉTICO

Para ilustrar a transferência do risco cibernético, considere um cenário em que a seguradora contra riscos cibernéticos realiza a inspeção de uma empresa que gostaria de proteger 25% de seu faturamento em caso de uma violação de dados. A seguradora talvez esteja disposta a aceitar esse risco, e pode até cobrar um pequeno prêmio da empresa; contudo, talvez esteja disposta a pagar uma quantia muito maior à empresa se houver uma violação, mais do que a empresa conseguiria manter na conta bancária. Nesse caso, a seguradora provavelmente faça algumas demandas à empresa, como estar em conformidade com o GDPR, o PCI-DSS e a LGPD. Todavia, se a empresa já estiver de acordo com essas legislações e for aprovada em todas as auditorias causais, a seguradora poderá estar disposta a transferir para si alguns dos riscos da empresa por um determinado preço.

Obviamente, uma cooperativa local pode fazer exatamente a mesma coisa **sem** dinheiro. Imagine um pequeno grupo de empresas que trabalham próximas umas das outras e que concordam em armazenar o *backup* de dados umas das outras. Elas podem discutir boas práticas de armazenamento de dados e dedicar um dia de seu próprio tempo para se ajudarem, caso outra empresa sofra um ataque cibernético. Essa também é uma forma de transferência e de compartilhamento de risco, sem que haja troca de dinheiro. De fato, os CERTs são uma maneira de transferir o risco cibernético, pois protegem seus constituintes com seu tempo.

OS RISCOS COMUNS E COMO QUANTIFICÁ-LOS

Existem diferentes tipos de riscos cibernéticos e os mais comuns serão detalhados a seguir. É importante notar que os riscos cibernéticos raros podem ser tratados da mesma forma que os comuns.

PERDA DE DADOS (ACIDENTAL E MALICIOSA)

O primeiro passo e o mais simples na gestão de risco cibernético é ter um método para conseguir ser contatado por terceiros, algo que pode ser tão simples quanto um endereço de *e-mail*, uma exigência sob o ISO/IEC 27002:2013. A seguir, apresentam-se mais detalhes sobre as violações de dados, seus custos e as respostas para ajudar a construir um *framework* robusto de gestão de risco cibernético para empresas.

No extremo inferior do espectro, os custos de violações variam com o volume dos dados perdidos, o que é medido pelo número de registros. Por exemplo, se uma determinada empresa processa 200 cartões de crédito por mês, talvez ela tenha 2,4 mil dados de cartões de crédito no último ano. Como alguns podem ser clientes repetidos, na realidade esse número pode ser em torno de 2 mil. De forma simples, se uma empresa perde 10 mil registros, deve esperar um custo de mil dólares. Isso muda um pouco na escala P8[30], em que a perda de 100 milhões de registros começa a custar cerca de 100 milhões de dólares.

É fácil para uma pequena empresa pensar que tem menos registros do que realmente tem. Um bom ponto de partida são os registros que toda organização provavelmente possui sobre todos os funcionários que já trabalharam nela; ademais, várias pequenas empresas ou organizações possuem muito mais dados do que funcionários. Assim, ao procurar por uma série de registros que poderiam ser perdidos caso **ocorresse uma violação**, é possível usar estimativas dos números de clientes como ponto de partida. No entanto, é importante notar que o número de registros perdidos não é um grande preditor de custo por razões matemáticas (Cyentia Institute, 2020): uma abordagem muito melhor do que o custo fixo por registro seria a média ou média geométrica.

30 Trata-se de uma escala logarítmica de tamanhos de violações, lançada no centro de estudos do risco do qual o autor faz parte, e documentada no livro de Coburn, Leverett e Woo (2018).

37% das perdas evitadas precisam ser gastas com planos de contingência; dessa forma, vale a pena desenvolver dois planos: um para os primeiros três dias após uma notificação de violação, e um para o próximo mês. Os primeiros três dias são cruciais e podem ser a diferença entre perder muito dinheiro e perder apenas um pouco. De fato, a resposta a uma violação pode até resultar no **aumento** no preço de ações durante uma crise, se for tão boa quanto a de Norsk Hydro[31].

No caso de uma violação, é importante ter um plano de investigação de TI e uma resposta para corrigir o que aconteceu. Os planos também devem incluir a gestão de comunicações e o atendimento ao cliente, talvez até mesmo o fornecimento de uma compensação justa por eventuais perdas. Além disso, a resposta à mídia também é crucial neste momento, inclusive no sentido de promover a marca (empresas que lidam honesta e abertamente com seus incidentes geralmente não sofrem tanto na bolsa de valores ou no tribunal da opinião pública). A comunicação com investidores ou um relatório ao conselho de administração também podem ser críticos.

Muitos marcos regulatórios em todo o mundo também exigem uma rápida notificação a uma autoridade regional nas primeiras 48-72 horas. Portanto, é essencial conhecer esses regulamentos, saber quem são os responsáveis por elaborar esse relatório, e dar-lhes todo o orçamento/tempo de que necessitam para essa tarefa.

A longo prazo, deve-se considerar planos mais estratégicos, como planos legais, comunicações corporativas e um aumento do orçamento de TI para reduzir as chances desses eventos ocorrerem novamente. Muitas empresas são especializadas em comunicações de crise e podem ser bem úteis durante uma violação, como o Brasil, que oferece diversas orientações e apoio por meio de seu CERT[32]. Vale notar que há diferenças importantes na forma de lidar com casos acidentais, como deixar dados em um *notebook* no carro que foi roubado, e os casos

31 A Hydro foi alvo de um amplo ciberataque, em 19 de março de 2019, que interrompeu as operações em várias áreas de negócio da empresa. Mais detalhes disponíveis em: https://www.youtube.com/watch?v=C6MDz-AgQuE

32 As publicações do CERT são geralmente recomendadas. Se ocorrer um incidente, eles devem ser contatados diretamente.

maliciosos, como um evento de *hacking* malicioso em que os dados foram roubados de propósito.

No primeiro exemplo, pode ser o caso de abrir um inquérito, com a apresentação de um boletim de ocorrência, e de criar uma nova política de nunca deixar *notebooks* dentro de carros; em ambos, os reguladores são notificados, mas em um roubo malicioso de dados, pode ser necessário ir direto para o CERT[33], talvez muito mais útil do que a polícia se houver o envolvimento de *hackers*, já que as investigações em casos cibernéticos podem levar meses e muitas vezes resultar em respostas não tão claras.

Como calcular o custo da frequência

É extremamente difícil descobrir a probabilidade de ser *hackeado*, pois depende de muitos fatores, como as capacidades dos *hackers*, o setor empresarial ou a chance de ser um alvo devido ao fato daquela tecnologia, por acaso, estar vulnerável. Em suma, é pouco provável que pequenas empresas tenham uma boa noção da probabilidade de serem violadas.

No entanto, a utilização de análises previamente executadas pode ser extremamente útil, o que geralmente envolve o cálculo de uma razão, conhecida como taxa de incidência. Para tanto, é preciso ter uma população conhecida, assim como conhecimento sobre quantos eventos acontecem nessa população, os quais podem ser violações por empresa ou eventos de *ransomware* por pessoa. Normalmente, essas taxas já foram calculadas e os detalhes podem ser bastante complicados. Por exemplo, no caso de *ransomware*, em 2016, existem trabalhos prévios que relatam uma taxa em torno de 3-4% (Simoiu, Bonneau, Gates, & Goel, 2019; Hull, John, & Arief, 2019). Para a gestão de risco cibernético, presume-se que a chance anual de ser atingido por um ataque de *ransomware* é de cerca de 3-4%, a menos que haja dinheiro e tempo disponíveis para se realizar uma pesquisa muito mais aprofundada.

Em caso de violações, a frequência está associada ao tamanho da organização[34]. Se não houver nenhuma informação sobre uma empresa, assume-se uma probabilidade de violação entre 5-7% ao ano; contudo, essa porcentagem é extremamente

33 Recuperado de https://cert.br/csirts/brasil/

34 Mais detalhes disponíveis em Cyentia Institute (2020).

imprecisa para a maioria dos casos, pois o número relatado é a maior frequência de infrações quando se decompõe por setor, sendo que a mais alta está no setor público. Ao observar os outros setores, a maioria apresenta uma frequência de violações abaixo de 1% (entre 0,82% e 0,03%); desse modo, uma simples análise desses dados, por setor, fornece uma boa noção da frequência do risco de violação de dados. Da mesma forma, a receita de uma empresa é um bom preditor, que varia entre 0,07% para empresas que ganham menos de 10 milhões de dólares e 75% para empresas que ganham mais de 100 bilhões de dólares.

COMPROMETIMENTO DE *E-MAIL* COMERCIAL (BEC) & *PHISHING*

Na prática, o comprometimento de *e-mail* comercial (business e-mail compromise – BEC) toma muitas formas diferentes, desde a alteração de faturas até o uso de *sites* falsos, de engenharia social, de *e-mails* ou telefone, entre muitas outras táticas; por isso, é simples mitigar este perigo. É preciso aplicar vários tratamentos de forma que cada um se acrescente aos sucessos do anterior, presumindo também que todos podem falhar[35].

Não há muita literatura sobre a frequência do BEC, além de menções ocasionais do aumento percentual ou do número de incidentes. A taxa de base de empresas que são alvos desses eventos, em alguns países ou até em âmbito global, parece estar subnotificada na literatura que existe até o presente. Presumivelmente, as empresas de seguro para riscos cibernéticos têm esses números, mas é improvável que os compartilhem, pois essa informação está no cerne de sua atividade.

Contudo, uma leitura de relatórios de seguradoras pode ajudar a entender o risco. Por exemplo, um quarto dos 3,3 mil incidentes globais no Beazley 2018 Breach Report ocorreu devido a BEC[36], número que fornece apenas um norte amplo e representa uma proporção significativa dos riscos cibernéticos regulares. Além disso, muitos trabalhos já foram escritos sobre como responder a esse tipo de risco, com soluções que vão desde

35 Uma entrevista de KrebsOnSecurity fornece uma introdução fácil ao ecossistema que apoia o ataque de BEC, disponível em https://krebsonsecurity.com/tag/bec-scams/. Já uma análise mais aprofundada dos detalhes técnicos do BEC está disponível no relatório TrendMicro (2017).

36 Recuperado de https://www.beazley.com/news/2019/beazley_breach_briefing_2019.html

ações que podem ser tomadas por pequenas organizações até abordagens mais globais para lidar com a epidemia[37].

Se os métodos comprovados de prevenção e mitigação forem implementados, como monitorar e medir sua eficácia dentro das organizações, ou até mesmo de modo global? Uma forma simples e mais fácil interna do que globalmente é agendar um teste de *phishing*, que pode ser conduzido por uma empresa especializada para medir cuidadosamente as taxas de detecção[38]. Se um *hacker* enviar mil *e-mails* para funcionários da empresa, tentando conseguir uma brecha de acesso, quantos vão cair em contas inativas? Quantos serão captados por filtros de *spam* e quantos outros serão abertos? Quantos serão relatados pelos funcionários no canal correto? Quantos serão investigados? Quantos *links* serão clicados? Quantos cliques podem levar ao comprometimento de um computador? Quantos podem levar uma engenharia social bem-sucedida? Quantos desse subgrupo final dos mil *e-mails* originais podem levar a um evento oneroso e qual o custo desse evento? Será mais caro se a organização for lenta na detecção da violação? Quantificar cuidadosamente cada um desses passos e compreender cada uma das camadas de defesa – técnica, humana, de detecção e de reação – são objetivos de um bom programa de BEC.

Como calcular o custo da eficácia

Uma vez aplicado o tratamento, como medir sua eficácia? A forma mais simples de testá-lo é tentando burlá-lo. Isso pode ser realizado por alguém de dentro da organização, um *hacker* ético profissional ou um engenheiro social que tente contornar os tratamentos de risco. O número de tentativas iniciais sob o número de tentativas bem-sucedidas é uma boa maneira de analisar a eficácia do controle, o qual não precisa ser 100% efetivo para ser útil, exceto se for muito oneroso. Em vez disso,

37 Apesar de existir há quase cinco anos, um dos melhores recursos para as organizações – pequenas e grandes – é o Plano de Ação de Londres. Recuperado de http://londonactionplan.org/wp-content/uploads/2012/12/Operation-Safety-Net-web-version1.pdf

38 Existem muitas organizações que podem conduzir testes/simulações automatizadas de penetração de *phishing*. Também há organizações que podem conduzir simulações de *phishing* projetadas por humanos e feitas sob medida para outras organizações. Embora a diferença esteja no preço, é preciso priorizar as organizações locais, principalmente por motivos linguísticos e culturais.

simplesmente significa que é preciso aplicar mais tratamento de risco para que sejam realizados mais cedo e mais tarde na linha do tempo de um ataque.

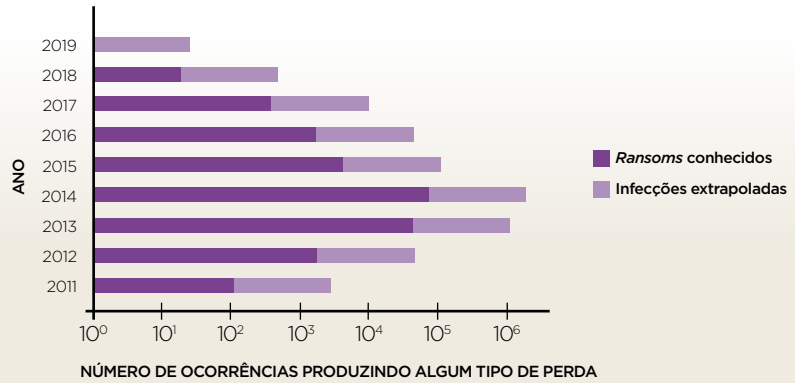
RANSOMWARE

O *ransomware* é a extorsão digital, o que significa que *hackers* negam acesso aos dados ou a computadores do alvo. De forma geral, ocorre por meio da criptografia ou exclusão dos dados; os que apagam dados às vezes são chamados de "varredores". De vez em quando, gangues de *ransomware* ameaçam publicar os dados ou tirar o *site* do ar com um ataque DDoS (negação de serviço), mas todos tentam demandar dinheiro de resgate, geralmente por meio de *bitcoin*, mas também por outras criptomoedas ou vale-presentes em lojas *on-line*. Existem muitas gangues de *ransomware*, cujo impacto nos últimos 10 anos é impressionante, tanto para pequenas como grandes empresas[39].

No contexto das pequenas empresas, o que pode ser feito se isso acontecer? Quantas são afetadas todos os anos? É possível estimar o número total de infecções com base no número de resgates pagos e na razão da disposição de pagamento supracitada: ao aplicar a razão de disposição para pagar e multiplicá-la pelo número de resgates sabidamente pagos, consegue-se uma estimativa bruta do número total de infecções, mesmo quando resgates não foram pagos (Gráfico 1). É preciso reconhecer que há um atraso de amostragem devido à forma como os dados são coletados, de modo a não acreditar que o número de ataques esteja caindo tão drasticamente. Essa é uma aplicação tanto do princípio da razão quanto do princípio do reconhecimento de vieses, em virtude de os dados serem úteis para estabelecer um limite inferior do número de infecções, ainda que não devam ser usados para concluir tendências nos últimos anos em razão do atraso na aquisição de dados.

39 A empresa do próprio autor possui um banco de dados de uma década de resgates registrados para que as seguradoras e empresas de risco possam calcular com mais precisão o risco de *ransomware*. Mais informações disponíveis em: https://billing.concinnity-risks.com/

GRÁFICO 1 - ESTIMATIVA DO LIMITE INFERIOR DE OCORRÊNCIAS DE *RANSOMWARE*



FONTE: ELABORADO PELO AUTOR.

Em suma, o Gráfico 1 ilustra que, para cada resgate pago, pode-se esperar mais 25 infecções que custaram dinheiro para a organização, mesmo sem pagamento de resgate.

Muitas empresas não funcionam sem computadores ou sem seus dados, os quais podem incluir números de telefone, *e-mails*, números de contas bancárias e fabricação digital. Se esses dados forem criptografados ou apagados repentinamente, seria muito difícil continuar operando[40].

Há pessoas que trabalham constantemente em todo o mundo para desenvolver soluções contra essas infecções digitais, conhecidas como decodificadores. Em razão de eles nem sempre existirem ou trabalharem com todas as famílias de *ransomware*, o que uma pequena empresa deve fazer diante desse tipo de incidente? É preciso implementar planos para a redução de riscos e de impacto.

Na categoria de medidas preventivas e de redução de risco, existem métodos bastante tradicionais e bem conhecidos. O antivírus pode impedir os tipos mais antigos e comuns de

40 Se essa situação ocorrer, pode ser útil acessar o *site* https://www.nomoreransom.org/, que permite o *upload* de bilhetes de resgate para tentar identificar a gangue ou o tipo de *ransomware*. O *site* oferece ferramentas que podem ser usadas para descriptografar os dados sem o pagamento de resgate. Há diretrizes em vários idiomas e é um ponto de partida muito útil.

ransomware, mas não os tipos mais novos e recentes. Talvez seja útil para os principais funcionários da empresa configurarem um *notebook* antigo exatamente da mesma forma que um novo, a fim de que ambos sejam capazes de acessar *e-mails*, faturamentos e *timesheets* (folhas de ponto). Para algumas pessoas, é mais fácil fazer isso ao efetuar *login* uma vez por mês nesse computador e verificar se ainda conseguem trabalhar com ele sem muita dificuldade: se não conseguirem, é preciso atualizá-lo. Esse simples exercício é útil tanto para saber o nível de dependência em tecnologias como para indicar o que é mais crucial para planos de *backups* e restauração. A vantagem dessa abordagem é que esse computador faz parte da base de operações a partir da qual se pode dar a reconstrução; todavia, é crucial mantê-lo desligado a maior parte do tempo e, de modo ideal, em um local diferente ao da empresa, porque, quando acontece um ataque de *ransomware*, ele infecta todos os computadores do mesmo tipo na mesma rede. Após um incidente, tanto a comunicação interna como a externa são vitais. Externamente, é preciso transmitir informações para os clientes, a imprensa, o CERT, seguradoras e investidores. A resposta ao incidente de *ransomware* da Norsk Hydro fornece importantes lições, assim como a de Maersk[41]: ambas as organizações não só reconstruíram partes de suas empresas do zero como também conseguiram transmitir uma sensação de resiliência e calma durante uma crise existencial e se tornaram, merecidamente, modelos de gestão de crise durante ciberataques.

Além disso, é possível adquirir produtos de seguros específicos para *ransomware*, muitas vezes acompanhados por um pacote de assistência, no caso desse evento ocorrer. Eles também exigem que as empresas tomem uma série de medidas para se proteger antes de vender o seguro.

Os custos de lidar com as consequências de *ransomware* são muito mais altos do que o resgate pedido, por isso os criminosos conseguem ganhar dinheiro, já que, se fosse possível fazer essa "limpeza" por meio de empresas que não cobrassem caro, os invasores não teriam mais essa vantagem. Logo, as organizações

41 Detalhes sobre as lições aprendidas após o ciberataque sofrido por Maersk e como foram realizadas estão disponíveis em: https://www.youtube.com/watch?v=wQ8HIjkEe9o. Ver também nota de rodapé nº 31.

devem centrar seus esforços em serem capazes de restaurar seus sistemas de computador rapidamente do zero **antes** de um evento cibernético ocorrer. Se for possível restaurar um computador e seus dados para qualquer parte do negócio da organização por menos do que ela fatura por mês, pode diminuir significativamente a vantagem para extorsões.

Outro problema com o pagamento do resgate é não excluir o custo da limpeza. O fato de que houve uma invasão permanece: a organização precisa notificar a infração e, ainda que alguém dê as chaves para obter os dados de volta, é necessário descobrir como conseguiram invadir, a fim de expulsá-los. Às vezes, os decodificadores não funcionam adequadamente e ainda há muito trabalho a fazer, mesmo que o resgate tenha sido pago. Assim, é muito melhor planejar um incidente pelo qual a empresa é impedida de acessar todos os computadores e ensaiar, com sua equipe, possíveis respostas.

OS RISCOS ESPECÍFICOS ENFRENTADOS, DOCUMENTADOS E MUITAS VEZES IMPEDIDOS PELA SOCIEDADE CIVIL

A maioria dos riscos e danos descritos até aqui são um problema principalmente para empresas, porém também podem afetar grupos da sociedade civil, organizações sem fins lucrativos ou organizações de caridade. No entanto, existem alguns riscos específicos não enfrentados pelas empresas, mas por essas outras organizações: desde *stalkerware*, golpes românticos, ataques de *phishing* direcionados, vazamentos politicamente motivados e até mesmo a defesa do consumidor no ambiente tecnológico, a sociedade civil tem lidado, por décadas, com riscos cibernéticos que costumam ser subestimados e subnotificados.

- *Stalkerware* é o nome dado a aplicativos instalados em telefones para espionar pessoas, especialmente em situações de abuso com base no gênero ou violência por parceiro íntimo. Alguns aspectos disso recaem na categoria de controle coercitivo, como às vezes aparece na

literatura acadêmica[42]. Há três aspectos desse fenômeno que merecem mais atenção: quanto dinheiro essas empresas estão ganhando, como aplicar a LGPD para proteger as pessoas afetadas e, para todas as organizações (incluindo empresas), como perceber os impactos que a violência íntima de parceiros e o abuso tecnológico têm em seus funcionários.

- O golpe romântico é uma pequena indústria em desenvolvimento em fóruns da *dark web*, que fornece muitos tutoriais sobre como seduzir pessoas para lhes dar um golpe financeiro, transformá-las em mulas para a lavagem de dinheiro, ou os dois ao mesmo tempo. Os tutoriais apresentam lugares nos quais é possível comprar fotografias íntimas adquiridas ilicitamente, de modo a conseguir se passar por outra pessoa. Esse fenômeno também é conhecido como *e-whoring*[43]*;* os leitores que não o conhecem devem observar como há muitas vítimas no ecossistema, desde as pessoas cujas fotografias íntimas foram roubadas ou obtidas por meio de um golpe, até aquelas que sofreram um golpe financeiro ou ainda o dano emocional de acreditar em um romance falso, além do trabalho extra que uma vítima precisa realizar para se livrar das acusações de lavagem de dinheiro.
- Ataques de *phishing* direcionados buscam enganar as pessoas, convencendo-as a inserirem suas senhas ou credenciais em *sites* que simulam outros *sites* usados regularmente pelas vítimas. Os alvos desses ataques costumam ser pessoas cujo trabalho é politicamente sensível: jornalistas, ativistas ou líderes comunitários. Uma vez conhecidas as credenciais, elas são usadas nos *sites* originais para coletar o máximo de informações possíveis. Às vezes eles também são vazados para públicos mais amplos. Como se já não fosse traumatizante o suficiente para alguém ter seu *e-mail* lido e vazado, uma nova preocupação tem surgido nos últimos anos: os va-

42 Um excelente panorama da questão está documentado no relatório do Citizen Lab, *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* (Parsons et al., 2019). Um programa de pesquisa muito mais amplo ou profundo sobre gênero e a IoT está sendo desenvolvido na UCL, sob a direção do Dr. Leonie Tanczer (Lopez-Neira, 2019). Mais informações em: https://tspace.library.utoronto.ca/handle/1807/96320

43 Este fenômeno foi documentado por Hutchings (2019), em uma análise muito mais aprofundada.

zamentos são estrategicamente alterados e modificados para se adequarem à agenda dos atacantes. Se a maior parte do vazamento for factualmente precisa e apenas uma parte for falsa, os ataques tendem a ser engolidos como um todo pelo público, sem distinção; consequentemente, leva as vítimas desses ataques a se exaurirem na luta contra a desinformação sobre elas e evitarem os perigos associados a isso[44].

- Infelizmente, a censura e as interrupções na Internet também são comuns. Em alguns casos, duram anos[45] e podem até ser direcionadas a grupos linguísticos específicos[46]. Os efeitos nocivos estão documentados de várias maneiras, desde aqueles de saúde mental até a desigualdade educacional. Até mesmo o impacto econômico em uma região pode ser significativo[47], ocasionando muitos outros problemas produzidos pela desigualdade de renda.
- A Internet das Coisas (IoT) apresenta um dilema de política pública muito complicado. Na sua forma mais simples, é uma colisão lenta entre duas filosofias: a primeira é a ideia de que programas de *software* não podem ser responsabilizados; a segunda, que os direitos dos consumidores e a segurança de produtos devem ser embasados na responsabilidade. O problema torna-se cada vez mais exacerbado quanto mais a IoT se integra à existência quotidiana. Os *microchips* compõem cada vez mais objetos, e o custo de consertá-los aumenta, mas também param de funcionar quando a empresa que os fabricou vai à falência. Além disso, são óbvios os danos físicos que podem ser causados por *microchips*. O custo de falhas de qualidade de *software* não é simplesmente virtual, apesar da maioria da sociedade ainda acreditar nisso. Embora pessoas que trabalham com *softwares* que controlam a rede elétrica, por exemplo, tenham conhecimento desde sempre do enorme custo potencial

44 Um exemplo abrangente desse tipo de fenômeno está documentado em *Tainted Leaks: Disinformation and Phishing With a Russian Nexus* (Hulcoop, Scott-Railton, Tanchak, Brooks, & Deibert, 2017). Mais informações em: https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

45 Recuperado de https://en.wikipedia.org/wiki/Block_of_Wikipedia_in_Turkey

46 Recuperado de https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

47 Recuperado de https://www.internetsociety.org/policybriefs/internet-shutdowns

de uma pequena falha, é preciso que bilhões de pessoas tomem consciência de que seus celulares as estão espionando para entenderem como inevitavelmente essa ação levará à responsabilidade de programas de *software*[48]. A responsabilização de empresas de tecnologia pelos danos gerados pelos seus produtos ainda é incipiente, entretanto revela uma grande capacidade de mudar o comportamento de grandes corporações.

- O viés algorítmico, geralmente na forma de racismo ou sexismo, também é um problema. É preciso deixar claro que ele pode estar no próprio algoritmo, mas também pode estar embutido nos dados coletados originariamente. Portanto, mesmo um pesquisador bem-intencionado, ao usar o que considera um algoritmo e uma metodologia de pesquisa neutra, pode, de repente, descobrir que construiu um sistema racista ou sexista. Por exemplo, se uma base de dados foi coletada apenas considerando os salários de homens, então necessariamente não considerará a distribuição dos salários das mulheres; logo, qualquer inferência feita a partir desses dados tem alta chance de exibir um resultado sexista[49].

Nesta seção, não se focalizou tanto na quantificação dos riscos por dois motivos. Primeiro, muitos não são riscos operacionais para grupos da sociedade civil, embora seja o caso para alguns. Em outras palavras, não são uma ameaça à integridade da organização, mas para as pessoas atingidas. Portanto, a quantificação desses riscos seria conduzida de forma muito diferente e de modo mais eficaz se feita pelas próprias organizações. Em segundo lugar, esses estudos ainda são incipientes e os números não estão sendo sistematicamente coletados. É claro que um grupo da sociedade civil poderia começar esse processo agora e alcançar grandes progressos na documentação desses danos – bem como muitos outros – a fim de construir uma política baseada em evidências em torno dessas ocorrências.

---

48 Uma análise mais aprofundada pode ser encontrada em Leverett, Clayton e Anderson (2017). Seria uma boa ideia que grupos de direitos do consumidor se juntassem ao debate e conseguissem um tecnólogo na equipe para ajudar os advogados.

49 Esse tema é documentado meticulosamente pelo Algorithmic Justice League (Liga de Justiça Algorítmica), de Joy Buolamwini, e merece muito mais espaço do que o oferecido neste artigo. Recuperado de https://www.ajlunited.org/library/research

ANÁLISE DOS TRATAMENTOS DE RISCO

Existem vários tratamentos de risco para danos cibernéticos, portanto não há como listá-los integralmente com precisão. No entanto, é importante reconhecer os grandes temas dos diferentes tratamentos, bem como os benefícios, os efeitos colaterais e as armadilhas contraproducentes.

Em primeiro lugar, é útil agrupar os tratamentos em duas categorias: aqueles que ajudam a prevenir danos e aqueles que ajudam a reduzir o impacto caso ocorram. Naturalmente, alguns tratamentos ajudarão em ambos os casos, o que também é um benefício; entretanto, um risco frequente e que apresenta danos menores, ainda que se repita, seria mais bem tratado por meio da prevenção. Riscos menos frequentes, porém profundamente prejudiciais, talvez não possam ser prevenidos, mas há muito que pode ser feito para limitar a gravidade do evento.

Para captar essas informações de forma mais concreta, pode-se pensar em termos de desastres naturais. É possível examiná-los de acordo com três critérios: o desastre pode ser previsto ou evitado? É possível fazer qualquer coisa dentro da janela de previsão? É possível reduzir os impactos?

Terremotos não podem ser previstos com muita antecedência, ou melhor, sabe-se que vão acontecer, mas não há como precisar quando ocorrem. Embora não possam ser prevenidos como evento, seus efeitos em edifícios ou pessoas podem ser mitigados. Existem sistemas de alerta para terremotos iminentes, mas funcionam apenas alguns segundos antes do evento, tempo insuficiente para que salvem, efetivamente, vidas; contudo, o planejamento a longo prazo pode reduzir seu impacto, tal como melhorar os padrões de construção para tornar os edifícios mais seguros. Ao se considerarem as enchentes; embora não possam ser evitadas (mesmo com a descarbonização da sociedade), sistemas de alerta às vezes podem emitir notificações com dias de antecedência, e as evacuações podem salvar vidas. Isso também pode ser combinado com defesas contra enchentes a longo prazo distribuídas em todas as regiões para reduzir impactos. Finalmente, é possível fornecer recursos para ajudar a reconstruir comunidades após uma região ser atingida por uma enchente.

A questão principal é haver uma qualidade intersetorial na maneira que se cria uma resposta a esses problemas, definida *(i)* pela janela de tempo de previsão/alerta, *(ii)* pelo número de medidas que podem ser tomadas antes de um evento, e (iii) pelo

número de medidas que podem ser tomadas após um evento. Não se trata de escolher entre a prevenção e a redução de impacto, mas de fazer ambas as ações na medida correta. Também é importante – nos exemplos de desastres naturais supracitados – perceber como alguns tratamentos são centralizados (sistemas de alerta) e outros, decentralizados (construção de edifícios seguros ou defesas contra enchentes). É possível alcançar os mesmos resultados quando se trata do risco cibernético? Algumas soluções, como VPNs e a autenticação de dois fatores, devem ser centralizadas, mas outras soluções, como treinamento sobre *phishing*, podem ser descentralizadas. A análise dessas variações para cada risco estudado pode ajudar as organizações a definirem suas respostas e a otimizarem o uso dos recursos disponíveis.

EFICÁCIA DA MITIGAÇÃO CONJUNTA

Algumas defesas resolvem mais de um problema, o que é uma abordagem muito mais eficiente e econômica. Priorizá-las pode permitir que as organizações encontrem algumas formas de mitigação, como *backups,* para ajudá-las em caso de um ataque de *ransomware,* ou de um terremoto ou enchente. É preciso centrar-se exatamente nesse efeito, embora possa haver outros tratamentos de risco que se intercalem com cada um desses riscos individualmente.

Seguro cibernético para os riscos remanescentes que não podem ser tratados

Depois de ter tentado todos os tratamentos de risco práticos, eficientes e com um preço adequado, ainda existem alguns riscos residuais. É tentador simplesmente aceitar o risco residual e continuar a vida, porém ainda há a opção de transferência de risco. Quando já se esgotaram todas as opções mais fáceis, os seguros para riscos cibernéticos podem ser usados para cobrir riscos que a organização não sabe como tratar, administrar ou mitigar[50].

Comprar uma apólice de seguro não é a única alternativa. É possível criar cooperativas, assim como grupos de seguros ou

50 Romanosky et al. (2017) publicaram um documento abrangente mostrando a gama de políticas disponíveis e o que elas cobrem. Esse documento também fornece um esboço do custo dessa solução e do quanto as políticas conseguem realizar quando são ativadas. Uma perspectiva atuarial e baseada em pesquisa é apresentada por Marotta, Martinelli, Nanni, Orlando e Yautsiukhin (2017).

seguradoras cativas. Existem muitas formas de autosseguro, por exemplo, um grupo de empresas pode formar uma cooperativa, um fundo mútuo ou um grupo de seguros[51]. Eles podem alocar um dinheiro todo mês ou ano e concordar em usar parte dele caso alguém seja atingido por um ataque cibernético ou acidente tecnológico. Nesse esquema, é possível "agrupar" os recursos a fim de tornar viável o que seria caro demais para algumas empresas individuais, ao dividir o risco entre muitos. Isso também tem a vantagem de que, enquanto uma organização talvez não seja capaz de pagar por um profissional de segurança em tempo integral, um grupo de empresas o conseguiria. Assim, cada empresa receberia um *timeshare* de boas práticas de segurança e privacidade, apesar de serem pequenas empresas que talvez não fossem capazes de pagar por isso.

Outra opção é a criação de uma seguradora cativa[52]. No final do dia, você está se assegurando contra riscos, ou transferindo alguns dos riscos a terceiros. Claro, também é possível misturar as estratégias supracitadas para corresponder ao nível de risco ao qual uma empresa é exposta ou que consegue tolerar. Por exemplo, um plano de resposta a incidentes pode ser implementado, projetando custos para os três primeiros dias e ativando a apólice de seguro, com antecedência, se exceder o limite planejado pelo conselho administrativo. Dessa forma, o risco cibernético será medido de forma reproduzível e útil. Também indica sobrepor tratamentos de risco um sobre o outro, melhorando sua eficácia por meio de um conjunto de políticas, respostas e mecanismos de prevenção interligados. Esse conjunto de ações, em sua essência, é a gestão de riscos.

CONCLUSÃO

Este artigo discutiu o que seria uma boa métrica de risco cibernético e apresentou uma longa discussão sobre a razão da necessidade de tomar medidas. Princípios úteis para a construção de métricas de risco cibernético também foram apresentados, rumo à quantificação da grande variedade de riscos cibernéticos.

Apesar da ampla gama de riscos cibernéticos existente, uma organização deve nomear os ciber-riscos conhecidos e elencar

51 Recuperado de https://www.insuranceopedia.com/definition/1383/cooperative-insurance
52 Recuperado de https://www.captive.com/news/2018/08/08/what-is-captive-insurance

aqueles que enfrenta. Uma vez nomeados e elencados, os riscos devem, então, ser medidos de forma adequada. Da mesma forma, é importante melhorar os métodos de coleta de dados usados para gerenciar esses riscos: ao coletá-los, deve-se estar atento aos números sempre crescentes e decrescentes e as médias aplicadas. Além disso, embora seja importante medir o trabalho realizado, não se deve confundi-lo com a redução do risco, visto que só é possível medir algum elemento de risco quando sua frequência é reduzida ou sua gravidade mitigada. Logo, o esforço realizado para alcançar essa redução de riscos é o que precisa ser melhorado.

Em termos de medição do risco, há aspectos importantes a serem considerados. O primeiro relaciona-se com o fato de que, quando se reúnem métricas para representar uma economia, elas se tornam um jogo para as pessoas, não mais uma métrica (Lei de Goodhart). Por exemplo, se recompensar as pessoas que respondem a incidentes pelo número de incidentes tratados, elas, justificadamente, começarão a dividir os incidentes em pedaços menores e registrá-los como incidentes diferentes. Embora não seja errado, pois estão simplesmente fazendo o mesmo trabalho com uma estratégia diferente de registro, isso muda tudo quando se trata de analisar o que está sendo refletido pelas métricas de risco.

A segunda preocupação é outro desafio de *design* de incentivos, cujo objetivo é incentivar a **redução** do risco, mas uma métrica mal escolhida incentiva o trabalho de **registro**. Por exemplo, muitas equipes de risco lentamente migram para documentar práticas de *compliance* e o trabalho que isso exige, em vez de trabalharem para inovar o risco cibernético. Não há nada de errado em documentar o trabalho por si só se a equipe de risco permanecer centrada na redução de risco e em inovações para alcançar ou medir essa redução. Entretanto, se esforços cada vez maiores forem recompensados sem que a redução do risco seja documentada, haverá incentivo à ação errada. Isso é uma falha clássica de departamentos de risco de *compliance* em toda parte[53].

É aceitável errar os números e as métricas e melhorá-los ao longo do tempo ao construir e coletar as métricas de risco. Seria

53 Tema amplamente documentado no excelente livro *The Failure of Risk Management: Why It's Broken and How to Fix It* (Hubbard, 2009).

ainda mais interessante começar com uma estimativa e aprimorá-la a tomar decisões sobre assuntos arriscados sem o apoio de evidências. Mesmo que boas equipes de gestão de risco consigam lidar tanto com a incerteza como com dados enviesados, é importante dar-lhes o máximo de informações possíveis.

Ao se aperfeiçoarem as informações que servem de base para decisões sobre riscos, as métricas melhoram a prática de gestão de riscos; porém, ainda há muito trabalho a ser feito para elevar também as atitudes organizacionais sobre riscos, em razão de prevenirem a ocorrência de mais eventos negativos e lidarem melhor com elas quando acontecem. Outro elemento crucial é reconhecer e discutir uma diversidade de níveis de tolerância ao risco. Uma empresa talvez precise se arriscar mais do que outra para alcançar seus objetivos estratégicos. Por exemplo, uma padaria pode ter uma tolerância ao risco muito menor do que uma equipe de busca e resgate. A equipe de busca e resgate precisa **necessariamente** assumir riscos à saúde e à segurança da equipe em seu trabalho rotineiro de ajudar os outros. Contudo, talvez os padeiros achem interessante saber que, historicamente, sua profissão já foi de grande risco e que foi aprimorada, ao longo do tempo[54], por meio da gestão de risco.

Melhorias na eficiência e na eficácia dos tratamentos de risco são a força vital de qualquer gestão de riscos; portanto, medi-los e melhorá-los ao longo do tempo é essencial. Se uma organização nunca aprender com seu próprio passado, particularmente, quando já esteve em risco, terá uma gestão de risco de baixa qualidade. Se houver uma equipe de gestão de risco vibrante, diversificada e inovadora, que sempre descobre novas características do risco cibernético, a organização terá esperança de sobreviver aos desafios das próximas décadas.

A redução de riscos não é alcançada isoladamente: muitas organizações melhoram a sua gestão de riscos ao discuti-la ou compartilhá-la. Há inúmeras organizações em todo o mundo dedicadas a ensinar seu conhecimento sobre riscos ou a partilhá-los entre grupos mais amplos. É válido escolher uma delas, pois a questão principal é simplesmente nunca caminhar sozinho.

A frase mais prejudicial na linguagem é: "sempre foi feito dessa maneira".

GRACE BREWSTER MURRAY HOPPER (1976)

54 Recuperado de https://hughesenv.com/history-of-combustible-dust-explosions/

REFERÊNCIAS

Anderson, R., & Moore, (2006, 27 de outubro). The economics of information security. *Science, 314*(5799), 610-613. doi 10.1126/science.1130992

Anderson, R., Leverett, E., & Clayton, R. (2017). *Standardisation and certification of safety, security and privacy in the 'Internet of Things'*. Luxembourg: European Union. Recuperado de https://doi.org/10.17863/CAM.35286

Coburn, A., Leverett, E., & Woo, G. *Solving Cyber Risk: Protecting Your Company and Society* (pp. 34-40). Hoboken, NJ: John Wiley & Sons.

Cyentia Institute (2020). *Information Risk Insights Study (IRIS 20/20). A Clearer Vision for Assessing the Risk os Cyber Incidents*. Recuperado de: https://www.cyentia.com/iris

Gordon, L. A., & Loeb, M. P. (2002, novembro). The Economics of Information Security Investment. *ACM Transactions on Information and System Security,* 438-457. Recuperado de https://dl.acm.org/doi/abs/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM 46*, 3, 81-85.

Hubbard, D. W. (2009). *The failure of risk management: Why it's broken and how to fix it*. Hoboken, NJ: John Wiley & Sons.

Hubbard, D. W., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk*. Hoboken, NJ: John Wiley & Sons. Recuperado de https://www.wiley.com/en-us/How+to+Measure+Anything+in+Cybersecurity+Risk-p-9781119085294

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science, 8*(2). Recuperado de https://www.researchgate.net/publication/331046766_Ransomware_deployment_methods_and_analysis_views_from_a_predictive_model_and_human_responses/fulltext/5c6300f2299bf1d14cc1e663/Ransomware-deployment-methods-and-analysis-views-from-a-predictive-model-and-human-responses.pdf

Jardine, E. (2018). Mind the denominator: towards a more effective measurement system for cybersecurity. *Journal of Cyber Policy, 3*(1), 116–139.

Lipson, H. F., & Fisher, D. A. (1999). *Survivability — A New Technical and Business Perspective on Security.* Recuperado de https://www.researchgate.net/publication/2454026_Survivability__A_New_Technical_and_Business_Perspective_on_Security#read

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review, 24*, 35-61.

Payment Card Industry Data Security Standard (PCI-DSS). (n. d.) A*pproved Scanning Vendors*. Recuperado de https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

Payment Card Industry Data Security Standard (PCI-DSS). (n. d.) *Attestation of Compliance*. Recuperado de https://www.pcisecuritystandards.org/document_library?category=saqs#results

Payment Card Industry Data Security Standard (PCI-DSS). (n. d.) *Completing Self-Assessment*. Recuperado de https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). *Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk?* Washington D.C., VA: Rand, 38. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929137

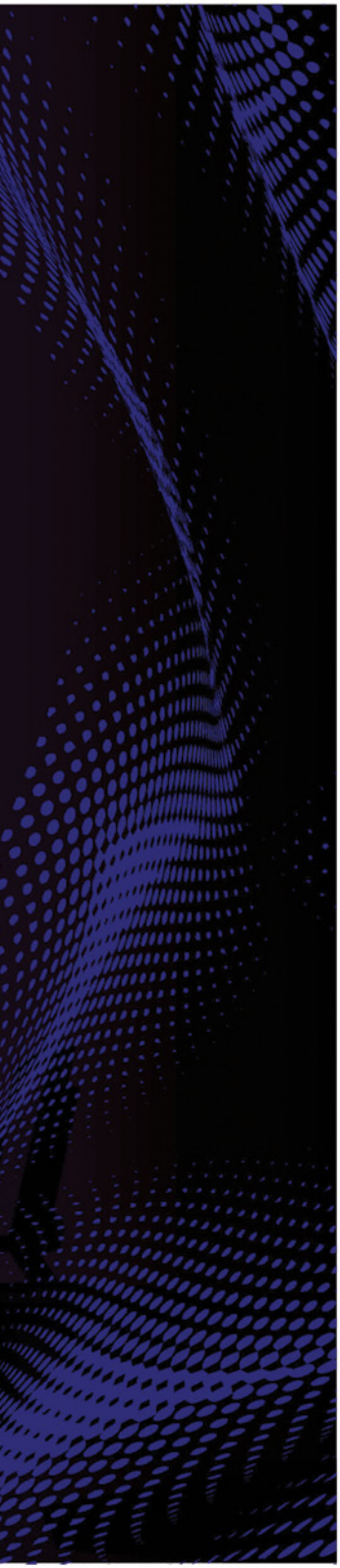
Simoiu, C., Bonneau, J., Gates, C., & Goel, S. (2019). I was told to buy a *software* or lose my computer. I ignored it: A study of ransomware. *Fifteenth Symposium on Usable Privacy and Security (SOUPS)*. https://www.usenix.org/conference/soups2019/presentation/simoiu

CAPÍTULO 3

Onde investir para reduzir o risco: um retrato a partir dos incidentes de segurança reportados e dos dados de sensores e fontes externas agregados pelo CERT.br

Cristine Hoepers[1]

1 Gerente Geral do CERT.br|NIC.br, Bacharel em Ciências da Computação pela Universidade Federal de Santa Catarina (UFSC) e Doutora em Computação Aplicada pelo Instituto Nacional de Pesquisas Espaciais (INPE).



INTRODUÇÃO

Em praticamente todas as áreas do conhecimento, de economia a saúde, passando por engenharia e desenvolvimento de *software*, um conceito essencial é o princípio de Pareto[2]. De maneira simplificada, esse princípio preconiza que 80% dos resultados são devido a 20% das ações. Aplicando esse princípio a problemas, significa que provavelmente 80% dos problemas poderiam ser resolvidos consertando 20% dos erros que levam a esses problemas.

Este é um olhar muito importante, pois a tendência é sempre de tentarmos focar os esforços naquilo que é novo ou que nos parece o mais "grave", por isso tememos muito mais um acidente de avião que um acidente de trânsito, embora o segundo tenha um risco estatisticamente muito mais alto de ocorrer.

Com relação a ataques a sistemas conectados à Internet, há, tanto por parte da mídia quanto por gestores, um grande foco em ataques que sejam novos, que explorem vulnerabilidades complexas ou que tenham motivações políticas, como espionagem ou guerra cibernética. Entretanto, no dia-a-dia das organizações, são problemas muito mais simples e com soluções já bem estabelecidas que causam a maioria dos ataques que alcançam sucesso, como poderemos observar nas análises que serão feitas neste artigo, com base nos dados de ataques e incidentes observados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br).

Considerando esse cenário, pode-se argumentar que existem três medidas que poderiam reduzir pelo menos 80% dos incidentes de segurança reportados ao grupo:

1. **Manter todos os *softwares* (sistemas operacionais e aplicativos) atualizados.** Ou seja, mantê-los sempre em sua última versão e com todas as correções de segurança instaladas. Isso vale para computadores, celulares, *tablets* e Internet das coisas (IoT).
2. **Fazer o *hardening* de todos os sistemas e dispositivos.** Ou seja, desabilitar serviços desnecessários para a função dos dispositivos, mudar todas as senhas padrão, configurar

2 Recuperado de https://pt.wikipedia.org/wiki/Princípio_de_Pareto

todos os serviços expostos na Internet de forma segura e constantemente rever as configurações, incluindo periodicamente checar se a medida 1 está sendo feita.

3. **Melhorar os processos de identificação e autenticação em serviços e sistemas.** Isso implica educação para gestão de senhas, com foco em não reutilização de senhas, e adequação de todos os sistemas e contas para não utilizar apenas senhas para autenticação. Ou seja, implementar e utilizar múltiplos fatores de autenticação em todos os serviços (sejam corporativos, em redes sociais, bancos ou quaisquer outros).

Mas, se o princípio de Pareto se aplica também na redução dos ataques na Internet, por que ainda estamos em um cenário com tantas vulnerabilidades e ataques bem-sucedidos? Por que os vazamentos de dados só crescem? Por que é tão difícil melhorarmos o cenário e atingirmos o almejado ecossistema saudável?

Esta análise abordará o cenário nacional a partir dos dados coletados pelo CERT.br, que incluem incidentes reportados voluntariamente por usuários e administradores de sistemas, dados coletados em sensores próprios e dados coletados por organizações internacionais e repassados ao CERT.br. Ao final, serão feitas algumas reflexões sobre a complexidade para implementar esses 3 passos em um cenário em que o uso da Internet das Coisas só cresce, como indicam os dados da pesquisa TIC Domicílios[3], e a cultura de que todos precisam fazer parte da construção de uma Internet mais saudável não está permeada na sociedade.

FONTES DOS DADOS UTILIZADOS PARA ANÁLISE

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), é um grupo de tratamento de incidentes com responsabilidade nacional, que atua como um ponto focal para notificações de incidentes de segurança no Brasil. O público-alvo (*constituency*) atendido pelo CERT.br inclui todas as redes que utilizam recursos aloca-

3 A cada ano, cresce o número de pessoas que utilizam TVs para se conectar, bem como celular; esse último, do ponto de vista de segurança, é muito mais próximo das características de dispositivos IoT do que de um computador. TIC Domicílios – 2019, Indivíduos, Usuários de Internet, por dispositivo utilizado, https://cetic.br/pt/tics/domicilios/2019/individuos/C16/

dos pelo NIC.br, ou seja, todas as redes que possuam endereços IP ou Sistemas Autônomos (ASNs) alocados ao Brasil ou que possuam domínios registrados sob o ccTLD .br.

As atividades desenvolvidas pelo CERT.br têm o objetivo estratégico de aumentar os níveis de segurança e de capacidade de tratamento de incidentes de usuários e redes conectadas à Internet no Brasil, contribuindo para sua crescente e adequada utilização pela sociedade. Para atingir esses objetivos, o grupo desenvolve diversas atividades, dentre as quais duas em especial contribuem para a produção de dados sobre o estado das ameaças no espaço Internet nacional: o tratamento de incidentes de segurança envolvendo quaisquer redes nacionais, de modo a prover a coordenação e o apoio no processo de resposta a incidentes, e suas atividades de análise de tendências de ataques.

Para permitir essa análise, além dos dados sobre as características dos incidentes de segurança reportados, o CERT.br também trabalha com outros dois tipos de dados: ataques observados na rede nacional de sensores (*honeypots*) que mantém[4]; e dados sobre ameaças no espaço Internet brasileiro observadas por projetos globais de medição de ameaças que compartilham esses dados com o CERT.br. Segue uma discussão sobre os tipos de dados, suas características e limitações.

NOTIFICAÇÕES DE INCIDENTES DE SEGURANÇA RECEBIDAS PELO CERT.br

Um Grupo de Tratamento de Incidentes de Segurança, ou CSIRT (do inglês *Computer Security Incident Response Team*), é uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. Um CSIRT normalmente presta serviços para uma comunidade bem definida, que pode ser a entidade que o mantém, como uma empresa, um órgão governamental ou uma organização acadêmica. Um CSIRT também pode prestar serviços para uma comunidade maior, como um país, uma rede de pesquisa ou clientes que pagam por seus serviços[5].

4 Projeto *Honeypots* Distribuídos. Recuperado de https://cert.br/projetos/
5 CSIRT FAQ. Recuperado de https://cert.br/certcc/csirts/csirt_faq-br.html

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. Alguns exemplos de incidentes de segurança são: tentativa de uso ou acesso não autorizado a sistemas ou dados, tentativa de tornar serviços indisponíveis, modificação em sistemas (sem o conhecimento ou consentimento prévio dos donos) e o desrespeito à política de segurança ou à política de uso aceitável de uma instituição.

O CERT.br é um CSIRT de responsabilidade nacional que atua como um CSIRT de último recurso (*CSIRT of last resort*), sendo um ponto de contato dentro do país que facilita a cooperação de forma coordenada entre as organizações que estejam envolvidas em um incidente, seja como origem ou como destino dos ataques. Ou seja, é um CSIRT ao qual qualquer um pode recorrer em caso de incidentes que envolvam redes alocadas ao Brasil.

Neste contexto, o CERT.br é bastante flexível na definição do que é um incidente de segurança que será tratado pelo grupo, de modo que recebe notificações sobre atividades diversas nos dispositivos ou na rede que possam ameaçar a segurança dos sistemas computacionais do seu público-alvo. Uma vez recebidas essas notificações, o CERT.br segue um processo conhecido como Gestão de Incidentes.

A Gestão de Incidentes de Segurança da Informação consiste em um conjunto de serviços que são vitais para ajudar o público-alvo de um CSIRT durante um ataque ou incidente. Esses serviços incluem não somente a coleta e avaliação das informações presentes em notificações de incidentes, mas também a análise de outros dados relevantes, como detalhes técnicos e artefatos relacionados. De forma específica, o CERT.br possui os seguintes serviços que fazem parte do processo de Gestão de Incidentes[6]:

- Dar suporte ao processo de recuperação e análise de ataques e de sistemas comprometidos;
- Estabelecer um trabalho colaborativo com outras entidades, como outros CSIRTs, empresas, universidades, provedores de acesso e serviços Internet e *backbones*;
- Manter estatísticas públicas dos incidentes tratados e das reclamações de *spam* recebidas.

6 Sobre o CERT.br, https://cert.br/sobre/

Essas estatísticas públicas dos incidentes tratados pelo grupo são mantidas desde 1999 no seguinte endereço: https://cert.br/stats/incidentes/. Como apontado anteriormente, o CERT.br recebe notificações voluntárias de um público-alvo bastante variado, que vai de usuários finais a administradores de sistemas e redes, de uma gama muito ampla de setores e de porte. Desta forma, para permitir uma categorização por tipo de ataque, mas ainda assim manter comparabilidade entre os dados coletados ao longo dos 21 anos de estatísticas disponíveis, o grupo optou por ter poucas categorias de ataques catalogadas, mas que pudessem agrupar esses ataques pelos tipos mais significativos. Os tipos de ataque em que os incidentes são categorizados são:

- ***worm*:** notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede;
- **dos** (DoS - *Denial of Service*)**:** notificações de ataques de negação de serviço, onde o atacante utiliza um dispositivo ou um conjunto de dispositivos para tirar de operação um serviço, computador ou rede;
- **invasão:** um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede;
- ***web*:** um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet;
- ***scan*:** notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Varreduras são amplamente utilizadas por atacantes para identificar potenciais alvos, pois permitem associar possíveis vulnerabilidades aos serviços habilitados em um dispositivo;
- **fraude:** segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Essa categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem;
- **outros:** notificações de incidentes que não se enquadram nas categorias anteriores.

Também são apresentados, para cada ano da série, detalhamentos sobre quais tipos de varreduras são mais frequentes. As

varreduras, embora não sejam um ataque com sucesso, são um indicativo de quais serviços são mais buscados por atacantes e evidenciam onde estão as vulnerabilidades mais exploradas.

REDE DE *HONEYPOTS* DISTRIBUÍDOS MANTIDA PELO CERT.br

O CERT.br mantém o Projeto *Honeypots* Distribuídos, uma rede distribuída de *honeypots* de baixa interatividade em endereços IP da Internet no Brasil. Este projeto tem o objetivo de aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no Brasil[7].

Um *honeypot* é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido. Em um *honeypot* de baixa interatividade, são instaladas ferramentas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir. Desta forma, o sistema operacional real deste tipo de *honeypot* deve ser instalado e configurado de modo seguro para minimizar o risco de comprometimento[8].

Um *honeypot* traz como grande vantagem o fato de ser implementado de forma que todo o tráfego destinado a ele é, por definição, anômalo ou malicioso. Portanto é, em teoria, uma ferramenta de segurança isenta de falsos-positivos, que fornece informações de alto valor e em um volume bem menor do que outras ferramentas de segurança, como um Sistema de Detecção de Intrusão (IDS). Vale ressaltar que um *honeypot* só é capaz de observar o tráfego destinado a ele, não sendo uma ferramenta que utilize inspeção de tráfego.

O valor dos *honeypot*s baseia-se no fato de que tudo o que é observado é suspeito e potencialmente malicioso, e sua aplicação depende do tipo de resultado que se quer alcançar. Normalmente, o uso de *honeypot*s de baixa interatividade está associado aos seguintes objetivos:

- detectar ataques internos;
- identificar varreduras e ataques automatizados;
- identificar tendências;
- coletar assinaturas de ataques;

---

7 Idem ao *footnote* 2: Projeto *Honeypots* Distribuídos. Recuperado de https://cert.br/projetos/

8 *Honeypots* e *Honeynets*: Definições e Aplicações, CERT.br. Recuperado de https://cert.br/docs/whitepapers/honeypots-honeynets/

- detectar máquinas comprometidas ou com problemas de configuração;
- coletar código malicioso (*malware*).

No Projeto *Honeypots* Distribuídos, o CERT.br utiliza *honeypots* de baixa interatividade para detectar varreduras, ataques automatizados, códigos maliciosos e máquinas comprometidas ou com problemas de configuração. Para atingir esses objetivos, as seguintes atividades são desenvolvidas:

- É mantida uma rede distribuída de *honeypots* de baixa interatividade, cobrindo uma quantidade razoável do espaço de endereços IPv4 da Internet no Brasil;
- Foi desenvolvido um sistema que notifica, diariamente, os grupos de tratamento de incidentes (CSIRTs) das redes responsáveis por originar ataques aos *honeypots*;
- São mantidas estatísticas públicas:
    - gráficos diários dos fluxos de rede do tráfego direcionado a todos os *honeypots*[9];
    - estatísticas e análises anuais dos ataques mais frequentes contra os *honeypots* mantidos pelo CERT.br[10].

INDICADORES RECEBIDOS A PARTIR DE FONTES DE DADOS EXTERNAS

O CERT.br, por ser um CSIRT nacional de último recurso, conforme discutido anteriormente, qualifica-se para receber informações de entidades internacionais que trabalham para mapear atividades maliciosas e sistemas vulneráveis na Internet. As informações recebidas são relativas somente ao espaço de endereçamento IP alocado ao Brasil e são parte de fontes de informação utilizadas por CSIRTs do mundo todo para a detecção proativa de incidentes de segurança de redes.

O CERT.br recebe dados de diversas organizações, porém os mais relevantes para essa análise são os dados recebidos da Fundação Shadowserver[11] e do Shodan[12]. Os dados da Fundação Shadowserver incluem dados sobre dispositivos

9 Recuperado de https://honeytarg.cert.br/honeypots/stats/flows/current/
10 Recuperado de https://cert.br/stats/honeypots/
11 Recuperado de https://www.shadowserver.org
12 Recuperado de https://www.shodan.io

vulneráveis ou infectados, coletados por sensores passivos e dados advindos de varreduras realizadas em todo o espaço de endereçamento IPv4. O Shodan é um motor de buscas que indexa dispositivos de Internet das Coisas (IoT, do inglês *Internet of Things*), com foco em buscas por dispositivos vulneráveis expostos na Internet.

CENÁRIO DE ATAQUES OBSERVADOS NO ESPAÇO INTERNET BRASILEIRO

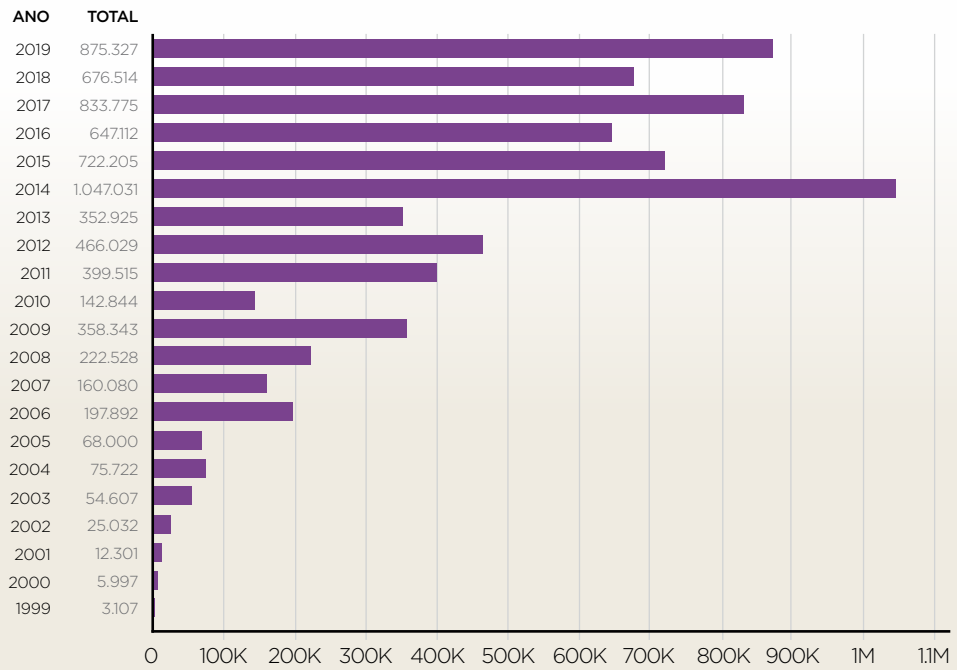
Nesta seção, vamos nos debruçar sobre os dados que podem ser observados nas fontes às quais o CERT.br tem acesso, iniciando pelos incidentes notificados ao grupo, passando para os dados dos *honeypots* e finalizando com os dados das fontes externas.

PERFIL DOS INCIDENTES DE SEGURANÇA NOTIFICADOS AO CERT.br

O CERT.br mantém, desde 1999, estatísticas sobre incidentes reportados voluntariamente para o grupo. Como é possível observar no Gráfico 1, há uma tendência de aumento nas notificações ao longo dos anos. Existem múltiplos fatores que contribuem para esse aumento, incluindo o próprio crescimento da Internet, pois, com mais dispositivos conectados, aumentam as vulnerabilidades expostas e também aumenta o interesse por parte dos atacantes.

É possível, também, observar que, em 2014, houve um aumento repentino nas notificações, e a partir dali os números sobem para um novo patamar, sempre acima de 600 mil notificações anuais. Além disso, as categorias de ataques mais notificadas naquele ano permanecem sendo as mais notificadas nos anos seguintes, motivo pelo qual segue uma análise mais detalhada sobre quais são esses ataques, qual a distribuição em 2014 e como isso evoluiu até 2019.

GRÁFICO 1 - TOTAL DE INCIDENTES REPORTADOS AO CERT.br POR ANO



FONTE: CERT.br

Esse grande número de incidentes em 2014 foi devido a três categorias de ataques: tentativas de fraude, varreduras (*scan*) e ataques de negação de serviço[13][14]. As notificações de tentativas de fraude, nesse ano, totalizaram 467.621, número cinco vezes maior que o de 2013, representando 44% de todos os relatos recebidos pelo CERT.br em 2014. Os casos de páginas falsas de bancos e sítios de comércio eletrônico (*phishing* clássico) cresceram 80%, e os casos de páginas falsas não relacionadas com fraudes financeiras, como as de serviços de *webmail* e redes sociais, tiveram um aumento de 73% em naquele ano. É importante ressaltar que o maior objetivo desse tipo de ataque é a

13 Recuperado de https://cert.br/stats/incidentes/2014-jan-dec/analise.html
14 Recuperado de https://www.nic.br/noticia/releases/cert-br-registra-aumento-de-ataques-de-negacao-de-servico-em-2014/

captura de credenciais de acesso a *sites*, sistemas corporativos e contas de *e-mail*, entre outros.

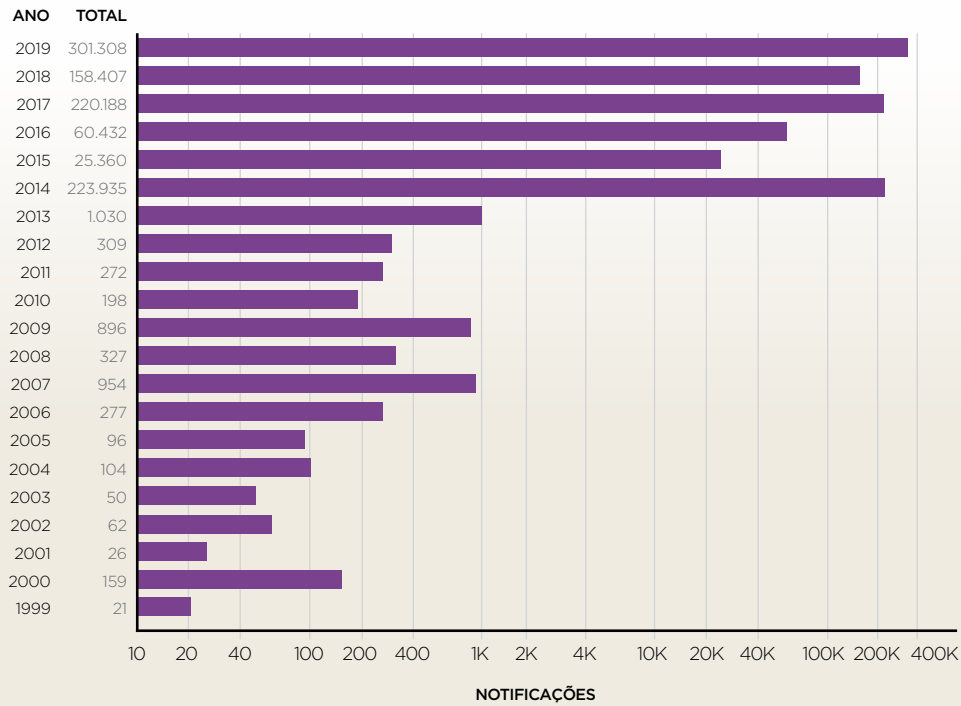
As varreduras, que são ações com intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles, totalizaram 263.659 notificações em 2014, representando um aumento de 59%. Os serviços que podem sofrer ataques de força bruta, ou seja, ataques cujo objetivo é testar repetidamente contas e senhas até adivinhar as credenciais de acesso, foram os mais procurados: SSH (22/TCP) correspondeu a 21% das notificações de varreduras de 2014, FTP (21/TCP) a 12% e TELNET (23/TCP) a 10%.

Com relação a ataques de negação de serviço (DoS), em 2014, foram recebidas 223.935 notificações sobre IPs alocados ao Brasil que participaram de ataques de DoS, número 217 vezes maior que o número de notificações recebidas em 2013 para a mesma categoria. A maior parte das notificações foram relativas a dispositivos mal configurados, localizados no Brasil, sendo abusados para amplificar ataques de negação de serviço. Ou seja, esses dispositivos possuíam serviços habilitados que expunham na Internet protocolos de rede que podem ser utilizados como amplificadores[15], tais como: CHARGEN (19/UDP), DNS (53/UDP), NTP (123/UDP), SNMP (161/UDP) e SSDP (1900/UDP). Juntos, esses cinco protocolos corresponderam a mais de 90% das notificações de DoS em 2014. Os outros 10% das notificações foram sobre dispositivos infectados com *bots*, que são códigos maliciosos que dispõem de mecanismos de comunicação com o invasor e permitem que ele seja controlado remotamente, de modo a disparar ataques contra terceiros, incluindo ataques de negação de serviços. Redes controladas por um atacante e que são formadas por centenas ou milhares de *bots* são denominadas de *botnets*.

Somados, esses 3 tipos de ataques representaram 91,23% de todas as notificações de 2014. Varreduras e tentativas de fraude já eram duas categorias que costumavam representar uma parte significativa das notificações, mas DoS foi uma categoria que subiu substancialmente a partir desse ano, como pode ser visto no Gráfico 2. Essa categoria era responsável por menos de 1% das notificações em anos anteriores e passou a representar uma quantidade substancial das notificações desde 2014.

15 Alert (TA14-017A) UDP-Based Amplification Attacks, Cybersecurity and Infrastructure Security Agency (CISA). Recuperado de https://www.us-cert.gov/ncas/alerts/TA14-017A

GRÁFICO 2 - NOTIFICAÇÕES SOBRE DISPOSITIVOS: PARTICIPANDO EM ATAQUES DoS
Escala logarítmica



FONTE: CERT.br

No período entre 2015 e 2018, a maior parte dos ataques de negação de serviço notificados ao CERT.br era relativa a dispositivos gerando amplificação, mas um ponto já chamava atenção, que era o aumento ano a ano das notificações de ataques de DoS originados a partir de *botnets*, formadas por dispositivos infectados que poderiam ser caracterizados de maneira ampla como Internet das Coisas, por exemplo: câmeras de segurança, DVRs (*Digital Video Recorders*), *smart* TVs, discos externos e roteadores WiFi e de banda larga.

Em 2019, o CERT.br recebeu 875.327 notificações de incidentes de segurança; destas, 301.308 foram notificações sobre dispositivos que participaram de ataques de negação de serviço, sendo que esse número foi o maior da série histórica. A maior parcela dessas notificações foi de ataques do tipo UDP *flood*

gerados por *botnets* IoT. *Botnets*, como Mirai e Bashlite, que infectam tanto dispositivos como DVRs quanto roteadores de banda larga, foram responsáveis pela maior parte dos ataques notificados. Esses ataques já estavam sendo reportados desde 2015, mas os números se intensificaram em 2019.

Essa mudança de padrão, de amplificação para *botnets* IoT, está, provavelmente, relacionada a dois fatores concomitantes: a redução de amplificadores no país e o aumento no número de dispositivos IoT na Internet. Mais detalhes sobre estes fatores serão discutidos nas seções a seguir, quando exploraremos os dados de *honeypots* e de fontes externas.

Com relação às estatísticas de incidentes mais frequentes em 2019, cabe ainda ressaltar que as notificações de varreduras continuaram sendo majoritariamente por serviços que permitem ataques de força bruta de senhas, divididas nas seguintes categorias, de acordo com as portas TCP varridas:

- Força bruta de credenciais de servidores de rede, de roteadores e de dispositivos IoT (portas 22, 23 e busca conjunta pelas portas 23 e 2323);
- Força bruta de senhas de *e-mail* (portas 25 e 143);
- Força bruta de credenciais em conjunto com vulnerabilidades de Winbox MikroTik (busca conjunta pelas portas 23 e 8291).

Notadamente, se compararmos as portas mais atacadas de 2014 com as de 2019, vemos que o número de portas aumentou, bem como ganharam destaque ataques contra serviços de *e-mail*. Esse foco dos atacantes em credenciais também é corroborado por alguns estudos externos de empresas de segurança que acompanham o mercado negro. O relatório de 2020 da TrendMicro, intitulado "*Shifts in Underground Markets Past, Present, and Future*"[16], mostra, na análise da página 5, que, dentre as ofertas no mercado negro, credenciais e contas furtadas são a "mercadoria" mais ofertada. Essas são credenciais variadas, incluindo contas bancárias, de *e-mail*, mídias sociais, serviços de entretenimento, entre outras. Esse estudo também inclui, dentre as "mercadorias", vulnerabilidades de IoT, *botnets* e ataques de negação de serviço, evidenciando que

16 Recuperado de https://documents.trendmicro.com/assets/white_papers/wp-shifts-in-the-underground.pdf

os incidentes mais notificados ao CERT.br são consistentes com as mercadorias e serviços mais negociados pelos atacantes.

ATAQUES MAIS FREQUENTES CONTRA OS *HONEYPOTS* DISTRIBUÍDOS MANTIDOS PELO CERT.br

Conforme comentado anteriormente, o CERT.br mantém uma rede distribuída de *honeypots*, que são sensores 100% passivos e que, numa Internet ideal em que não ocorressem ataques, não receberiam nenhum tráfego, pois não há nenhum tipo de serviço sendo provido por esses sensores. Esse tipo de sensor nos permite detectar o ruído de fundo da Internet, ou seja, o constante tráfego gerado por códigos maliciosos tentando se propagar e por atacantes varrendo o endereçamento IPv4 em busca de sistemas vulneráveis ou mal configurados. O que segue é uma análise de todos os ataques recebidos por esses sensores em 2019[17] e a comparação com 2018[18], além de um olhar sobre como esses dados complementam os dados de incidentes reportados ao CERT.br.

Com relação a varreduras nas portas TCP, os seguintes ataques foram os mais significativos:

- As varreduras pelas portas TCP 23, 22, 81, 5555, 8000 e 8080 estão todas relacionadas com atividade de propagação de *botnets* IoT, como a Mirai e suas variantes e a Bashlite e suas variantes. Os ataques nessas portas são tentativas de força bruta de credenciais ou tentativas de explorar vulnerabilidades nas interfaces de gerência de roteadores de banda larga ou de WiFi.
- Houve um aumento de varreduras contra serviços de *e-mail*, mais notadamente às portas POP3 (110/TCP), SMTPS (465/TCP), IMAPS (993/TCP) e POPS (995/TCP). Esse aumento pode estar relacionado com o aumento de força bruta contra outros serviços de *e-mail*, como visto nos incidentes de segurança reportados ao CERT.br.
- De 2018 para 2019 houve um aumento de 546% no número de pacotes contra a porta RDP (Remote Desktop Protocol), sendo que esse aumento coincidiu com a divulgação da vulnerabilidade chamada BlueKeep (CVE-

17 Recuperado de https://cert.br/stats/honeypots/
18 Recuperado de https://cert.br/stats/honeypots/2018/

2019-0708[19]), que passou a ser explorada por diversos códigos maliciosos.

Já com relação ao tráfego com destino a portas UDP, esses são os pontos de destaque:

- A porta UDP com mais varreduras continua sendo a 5060/UDP, que teve aumento de 32% de 2018 para 2019. Essa atividade está relacionada com o abuso de servidores SIP, através da força bruta das credenciais dos ramais para realização de ligações de longa distância.
- Outro ponto que chama a atenção é a continuidade das varreduras à procura de serviços passíveis de serem abusados para amplificação de tráfego. São eles: SNMP (161/UDP), NTP (123/UDP), DNS (53/UDP), SSDP (1900/UDP), Netbios (137/UDP), Chargen (19/UDP), Portmap (111/UDP), mDNS (5353/UDP), TFTP (69/UDP) e qotd (17/UDP). Essas varreduras, provavelmente, são as atividades de atacantes tentando mapear amplificadores para, posteriormente, abusá-los em ataques de negação de serviço.

É interessante destacar que, dentre as atividades maliciosas mais observadas pelos *honeypots*, estão várias varreduras que estão relacionadas com a propagação de *botnets* IoT, com a busca por amplificadores e com o mapeamento de serviços que permitam força bruta de credenciais. Todas essas atividades também estão entre as mais frequentes nos incidentes reportados ao CERT.br.

O PROBLEMA DOS AMPLIFICADORES QUE PERMITEM ABUSO PARA NEGAÇÃO DE SERVIÇO

Conforme discutido na análise dos incidentes notificados para o CERT.br, o ano de 2014 foi marcado pelo aumento dos ataques de DoS com uso de amplificação de protocolos UDP mal configurados e expostos na Internet. Para entendermos melhor o impacto desses ataques e a dificuldade para reduzi-lo, segue uma descrição de como foi a evolução desde meados dos anos 2000.

Os primeiros ataques de amplificação ocorreram em 2007, abusando especificamente o protocolo DNS, e eram casos em

19 Recuperado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

que servidores recursivos eram mal configurados e respondiam a perguntas a partir de qualquer ponto da Internet. Este ataque foi tão efetivo que chegou a ser utilizado para tirar do ar os servidores raiz de DNS. Já naquela época, o CERT.br escreveu um documento[20] que explica o problema e como corrigi-lo, e iniciou um processo de notificar redes brasileiras que permitissem amplificação de DNS para que corrigissem o problema.

Os ataques de amplificação abusavam basicamente o protocolo DNS. Até que, em 2013, o pesquisador Christian Rossow, enquanto escrevia um artigo sobre protocolos que permitem amplificação, que foi publicado na Conferência NDSS, trabalhou em conjunto com o US-CERT para o desenvolvimento do Alerta TA14-017A[21], lançado em janeiro de 2014, trazendo novamente o assunto à tona para comunidade técnica, dessa vez descrevendo outros 11 protocolos UDP que permitem amplificação. Esse alerta e o artigo não só trouxeram o assunto à tona, como levaram ao desenvolvimento de novas ferramentas de ataque de negação de serviço, que se popularizaram em 2014, levando ao aumento visto não só nos incidentes notificados para o CERT.br, como no tamanho dos ataques de negação de serviço.

Em reação a esse novo cenário, em março de 2014, a Fundação Shadowserver iniciou um projeto com o objetivo de varrer todo o espaço de endereçamento IPv4 em busca dos serviços listados no alerta do US-CERT e que permitem amplificação[22]. Este se tornou um projeto contínuo, que tem sido constantemente atualizado para adicionar mais protocolos à testagem e que gera dois tipos de dados: estatísticas públicas dos países que mais possuem amplificadores e dados separados por país de alocação dos IPs, e que são compartilhados com os CERTs nacionais desses países. Estes dados do Shadowserver são também compartilhados com o CyberGreen[23], que mantém estatísticas públicas dos dados, incluindo um painel que mostra o potencial de negação de

---

20 Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos; Cristine Hoepers, Klaus Steding-Jessen, Nelson Murilo, Rafael R. Obelheiro. Recuperado de https://cert.br/docs/whitepapers/dns-recursivo-aberto/

21 Alert (TA14-017A) UDP-Based Amplification Attacks; Original release date: January 17, 2014; Last revised: December 18, 2019. Recuperado de https://www.us-cert.gov/ncas/alerts/TA14-017A

22 The scannings will continue until the Internet improves. Recuperado de https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/

23 O Instituto CyberGreen é uma organização colaborativa, sem fins lucrativos, que desenvolve atividades para uma Internet mais saudável e resiliente. Recuperado de https://www.cybergreen.net/who-we-are/

serviço global e uma tabela que lista os países de acordo com os que possuem mais dispositivos que permitem amplificação[24] [25].

O CERT.br começou, já em 2015, a compilar os dados do Shadowserver relativos a amplificadores DNS e NTP em IPs alocados ao Brasil, realizando notificações periódicas para os responsáveis pelos Sistemas Autônomos destes IPs, incluindo nessas notificações instruções detalhadas sobre como resolver o problema. Mas, com o passar dos anos, o número de dispositivos permitindo amplificação foi mudando o seu perfil de servidores de rede com os serviços mal configurados para um cenário em que boa parte desses amplificadores eram roteadores de banda larga e dispositivos de rede. Estes são dispositivos que não precisam nem utilizam a maior parte dos serviços que permitem amplificação, mas são dispositivos que vêm de fábrica com esses serviços abertos, por conta de más políticas de desenvolvimento, integração de *software* e configuração padrão. Essas más práticas dos fabricantes de roteadores domésticos foram muito bem caracterizadas no relatório "*Home Router Security Report 2020*", que levantou diversos problemas graves, principalmente a falta consistente de atualizações e a utilização de sistemas operacionais antigos e desatualizados por esses fabricantes.

No período de 2014 a 2017, diversas organizações começaram a fazer manifestos pela adoção de boas práticas de rede, principalmente para evitar *spoofing* (falsificação do endereço IP de origem de um pacote TCP/IP), que é um problema de má configuração de redes imprescindível para que um atacante possa iniciar um ataque de amplificação[26]. Um dos primeiros foi o "*Routing Resilience Manifesto – Draft 1*", que foi colocado em discussão pela Internet Society (ISOC) entre junho e julho de 2014 e foi oficialmente publicado em 31 de agosto de 2014 com o título "*Mutually Agreed Norms for Routing Security (MANRS)*"[27]. Esse documento não tem um foco tão grande em redução de amplificação, mas tem entre um de seus quatro pilares a implementação de *antispoofing*.

---

24 CyberGreen Country Overview. Recuperado de https://stats.cybergreen.net/country

25 Em 2017, quando o CyberGreen começou a divulgar estatísticas, o Brasil era o país número 1 em termos de "poder de fogo" de negação de serviço.

26 *Antispoofing*. Recuperado de https://bcp.nic.br/antispoofing

27 MANRS History. Recuperado de https://www.manrs.org/about/history/

Outro grupo que estava discutindo intensamente o problema à época era o *Latin American and Caribbean Anti-Abuse Working Group* (LAC-AAWG), grupo que faz parte do LACNOG, fórum de operadores de redes da região atendida pelo LACNIC (Registro Regional de Recursos Internet para Região da América Latina e Caribe). Esse fórum, que é composto por operadores de rede da região, estava discutindo o impacto das vulnerabilidades em roteadores de banda larga para a resiliência dos PSIs e decidiu, em sua reunião de outubro de 2017, desenvolver um documento com um conjunto de requisitos mínimos de segurança que deveriam ser levados em conta no momento da aquisição de CPEs[28] (*Consumer Premises Equipment*) por PSIs. Essa boa prática foi construída em conjunto pelo LAC-AAWG e pelo M3AAWG (Messaging, Malware and Mobile Anti-abuse Working Group), tendo sido revisada por diversos especialistas externos e publicada em 06 de maio de 2019.

O ponto principal dessa boa prática é que os CPEs precisam sair de fábrica com configurações mais seguras, precisam permitir atualizações de *firmware* e que não devem vir de fábrica com serviços desnecessários, como os que permitem amplificação, ligados por padrão. Este foi um consenso, e os problemas foram apontados como os maiores responsáveis pela quantidade de roteadores de banda larga infectados e permitindo amplificação.

Diante desse cenário, o CGI.br e NIC.br lançaram, no final de 2017, no IX Fórum 11, o Programa por uma Internet mais segura (Programa i+seg), com o apoio da SindiTelebrasil, associação das operadoras de telecomunicações, da ABRANET e da ABRINT, associações de provedores de acesso à Internet, e em parceria com a Internet Society[29]. O Programa tem como objetivo atuar em apoio à comunidade técnica da Internet para a redução de ataques de negação de serviço (DDoS) originados nas redes do Brasil, reduzir o sequestro de prefixos, o vazamento de rotas e a falsificação de endereços IP de origem, além de reduzir as vulnerabilidades e as falhas de configuração presentes nos elementos da rede, e aproximar as diferentes equipes

28 CPE (do inglês *Customer Premise Equipment*) é o equipamento utilizado para conectar assinantes à rede de um Provedor de Serviços de Internet (ISP). Exemplos de CPE incluem *modems* (cabo, xDSL, fibra) e roteadores WiFi, entre outros.

29 Recuperado de https://bcp.nic.br/i+seg/sobre/

responsáveis pela segurança e estabilidade da rede para criar uma cultura de segurança entre os operadores da rede. As boas práticas divulgadas são basicamente o MANRS, o *hardening* de dispositivos e a redução no número de amplificadores.

As métricas sobre a situação dos amplificadores no Brasil são derivadas do trabalho do CERT.br em cima dos dados recebidos do Shadowserver e do Shodan[30]. O CERT.br identifica nesses dados todos os endereços IP que são apontados como tendo um serviço permitindo amplificação; neste momento, para cada categoria de amplificador, o CERT.br faz os seus próprios testes e armazena a informação sobre o *timestamp* do teste e os detalhes do resultado. Esses dados são agrupados por ASN, e uma notificação com os detalhes do teste e como resolver o problema é enviada para cada responsável dos Sistemas Autônomos.

De julho de 2018 até dezembro de 2019, o número de IPs permitindo amplificação alocados ao Brasil e presentes nos dados do Shadowserver e do Shodan reduziu cerca de 60%, principalmente na categoria SNMP[31]. Essa diminuição está ligada às notificações do CERT.br somadas às reuniões com operadoras e provedores de Internet, parte do Programa i+seg, que tem contribuído de forma significativa para conscientizá-los sobre as boas práticas de infraestrutura de rede. Essa diminuição, como vimos anteriormente, refletiu-se também na redução das notificações de ataques de DoS envolvendo amplificadores para o CERT.br e na posição do Brasil no *ranking* do CyberGreen, que agora figura como oitavo país com mais "poder de fogo", posição compatível com o tamanho da nossa rede, tanto em número de domínios quanto em número de endereços IP alocados, quando comparado com outros países do mundo.

COMO CHEGAR AO PARETO PARA REDUÇÃO DE INCIDENTES

Na introdução deste artigo, foi feita a provocação de que três medidas de segurança poderiam reduzir pelo menos 80% dos incidentes de segurança observados pelo CERT.br, sendo que, a seguir,

30 Estatísticas de Notificações de IPs e ASNs Permitindo Amplificação. Recuperado de https://cert.br/stats/amplificadores/

31 Recuperado de https://www.nic.br/noticia/releases/estatisticas-do-cert-br-apontam-aumento-de-ataques-de-negacao-de-servico-em-2019/

foram discutidos os ataques mais frequentes, sua prevalência e causas. São revisitadas aqui as três medidas, desta vez apontando em quais dos problemas observados estas medidas atuariam:

1. **Manter todos os *softwares* (sistemas operacionais e aplicativos) atualizados.** Como vimos, boa parte dos ataques utiliza *botnets* e depende da infecção de dispositivos, o que significa comprometer o dispositivo de alguma maneira, seja acertando as credenciais (tópico do item 3 a seguir) ou explorando vulnerabilidades. O US-CERT apresentou uma estatística muito preocupante, mas não surpreendente, de que as 10 vulnerabilidades mais exploradas para o comprometimento de sistemas de redes governamentais são todas conhecidas, e existem correções disponíveis, em alguns casos há mais de 5 anos[32]. O mesmo ocorre no caso de vulnerabilidades exploradas por *botnets* como Mirai e Bashlite, discutidas neste artigo.
2. **Fazer o *hardening* de todos os sistemas e dispositivos.** Como visto, mesmo sistemas que estejam atualizados, se estiverem com as configurações de fábrica, senhas padrão, entre outros, serão abusados para diversos ataques. Os ataques de amplificação ocorrem basicamente porque não é feito o *hardening* de sistemas, principalmente de roteadores domésticos e dispositivos de rede, mas isso também ocorre com serviços que estejam expostos na Internet.
3. **Melhorar os processos de identificação e autenticação em serviços e sistemas.** Os atacantes sempre vão escolher o caminho mais fácil e, hoje em dia, sistemas que utilizam apenas senhas são a norma, e este é o caminho que leva à maior parte dos golpes, comprometimentos de IoT, entre outros. Muitos sistemas não possuem múltiplos fatores de autenticação, o que requer educação redobrada dos usuários sobre como escolher e gerenciar senhas adequadas e como proteger suas credenciais.

Essas três medidas, que parecem simples, são as medidas essenciais para atingirmos um ecossistema saudável, que muitos têm chamado inclusive de higiene digital, mas que não dependem apenas de um ator da cadeia. Elas dependem de

32 Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities; May 12, 2020. Recuperado de https://us-cert.cisa.gov/ncas/alerts/aa20-133a

toda a cadeia de fornecedores, dos profissionais de TI e de segurança e dos usuários.

Essas ações não resolverão todos os problemas, mas, se implementadas por todos, implicarão a redução do volume de incidentes para patamares mais facilmente gerenciáveis, permitindo um foco das organizações em gerenciar os outros 20% dos riscos, sem ter que se preocupar com os 80% dos ataques que ocorrem por causas conhecidas e para as quais já há solução bem estabelecida.

REFLEXÕES SOBRE COMO ATINGIR UM ECOSSISTEMA SAUDÁVEL

Com podemos ver, atingir um ecossistema saudável e reduzir os riscos depende de diversos fatores. Depende do *software* utilizado, depende da capacitação dos profissionais e depende do empenho de cada um de nós em fazer a nossa parte. Por exemplo, no caso de ataques de negação de serviço, para reduzir o volume de ataques, é necessário que se reduza o "poder de fogo" dos atacantes, como discutido. Mas, quem pode fazer isso não são as redes sendo atacadas, mas sim redes que, a princípio, não estão sofrendo com o problema[33]. Este é um caso clássico de falta de incentivo para implementação e no qual é necessário que todas as redes conectadas à Internet implementem medidas que servirão para o bem comum, mas não necessariamente trarão um benefício imediato para quem implementa as ações.

Seguem algumas considerações sobre processos cruciais que precisam ser implantados em todas as organizações e que podem fazer uma grande diferença para reduzir os incidentes de segurança em larga escala.

- **Tudo começa com a escolha certa.** Ao escolher fornecedores de *software* e *hardware* (incluindo coisas como câmeras, impressoras, lâmpadas, sistemas de controle de crachás ou qualquer outra coisa "inteligente"), é necessário verificar as políticas de atualização (também conhecidas como políticas de *patches*, *fixes* e *updates*). Ou seja, o produto precisa oferecer um programa constante de atualizações *on-line* e precisa deixar claro como se faz para entrar em contato com o fabricante para reportar

33 Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS); CERT.br. Recuperado de https://cert.br/docs/whitepapers/ddos/

problemas e para obter informações sobre atualizações.

- **Não depender somente de senhas para segurança de acesso.** Deve-se implantar autenticação com múltiplos fatores (MFA, também chamado de 2FA) nos equipamentos e escolher serviços *on-line* que permitam o uso de MFA/2FA. Como visto, grande parte dos ataques reportados ao CERT.br nos últimos 5 anos envolviam ou furto de senhas ou adivinhação de senhas. Esses ataques incluíam, entre outros, senhas de acesso a: serviços de nuvem, *back-end* de lojas virtuais, contas de *e-mail*, servidores locais nas empresas, *desktops*, dispositivos como câmeras e discos externos, credenciais de serviços *on-line* e contas de redes sociais.
- **Aplicar correções sempre, não deixar para depois.** É essencial que todos os sistemas operacionais, serviços e aplicativos usados pelas empresas estejam sempre na última versão, com todas as correções de segurança aplicadas. Isso previne que a empresa seja comprometida por códigos maliciosos que exploram vulnerabilidades nesses sistemas. E, muito importante, não se deve esquecer das "coisas": câmeras, impressoras, *modems* de banda larga, roteador WiFi, lâmpadas, *smart* TVs, entre outros dispositivos conectados. Eles também são infectados e lançam ataques.
- **Ter acompanhamento periódico de profissionais qualificados em segurança.** Grandes empresas conseguem implantar mecanismos mais robustos através da manutenção de equipes dedicadas a gestão de risco, segurança e tratamento de incidentes. As pequenas e médias empresas operam em um cenário diferente, sem profissionais dedicados na área de TIC. É essencial que essas empresas encontrem alguma maneira de periodicamente revisar suas configurações, rever as medidas de segurança e implantar melhorias, seja com pessoal próprio ou com auxílio externo.
- **Educar os funcionários.** Na maior parte das empresas invadidas ou que tem dados vazados, tudo começou com um *phishing* contra um funcionário. Pode ser um *e-mail* se fazendo passar pelo chefe, uma mensagem "urgente" via outros serviços de mensagem, ou até mesmo uma visita a um *site* legítimo, mas que estava infectado. A partir disso, a invasão vai se permeando em toda a rede e o efeito

pode ser vazamento de dados, sequestro de dados via um *ransomware*, fraudes financeiras ou até mesmo uso da rede da empresa para cometer crimes e atacar terceiros. É necessário educar as pessoas para que elas também tenham algumas medidas de higiene básicas: ter sempre os sistemas na sua última versão, aplicar todas as correções de segurança imediatamente, não seguir *links* ou acreditar em promessas ou negócios bons demais para serem verdade e utilizar ferramentas básicas de segurança.

As três medidas discutidas neste artigo são simples do ponto de vista que não requerem ferramentas especializadas ou o desenvolvimento de novas tecnologias, mas sua implementação depende da implantação de processos e do investimento em pessoal, passos que requerem a sua priorização por parte de gestores e compreensão de que não existe uma solução pronta ou ferramenta que possa resolver o problema.

REFERÊNCIAS

Ceron, J. M., Steding-Jessen, K., & Hoepers, C. (2012). Anatomy of SIP Attacks. *Usenix; login magazine, 37*(6), 25-32. Recuperado de https://www.usenix.org/publications/login/december-2012-volume-37-number-6/anatomy-sip-attacks

Ceron, J. M., Steding-Jessen, K., Hoepers, C., Granville, L., & Margi, C. (2019). Improving IoT Botnet Investigation Using an Adaptive Network Layer. *Sensors, 19*(3), 727. Recuperado de https://doi.org/10.3390/s19030727

CGI.br (2012). Mecanismos de Segurança. In *Cartilha de Segurança para Internet* (Capítulo 7, pp. 47-58). São Paulo: CGI.br. Recuperado de https://cartilha.cert.br/livro/

CGI.br (2020). Cuidado com o que sai da sua rede. *Revista .br* (17ª ed.). Recuperado de https://cgi.br/publicacao/revista-br-ano-11-2020-edicao-17/

Desiderá, L., Steding-Jessen C., & Hoepers, C. Requisitos Mínimos de Segurança para CPEs: a Experiência de Construir uma Recomendação Global. *V Workshop de Regulação, Avaliação da Conformidade e Certificação de Segurança (WRAC+)*, São Paulo, SP. Recuperado de https://cert.br/docs/papers/bcop-cpe-wrac2019.pdf

ENISA (2011). *Proactive detection of network security incidents, report.* Recuperado de https://www.enisa.europa.eu/publications/proactive-detection-report

FIRST (2019). *FIRST Computer Security Incident Response Team (CSIRT) Services Framework*, Version 2.1. Recuperado de: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

FKIE (2020). *Home Router Security Report 2020.* Recuperado de https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

Hoepers, C., Steding-Jessen, K., Cordeiro, L. E. R., Chaves, M. H. P. C. (2005). A National Early Warning Capability Based on a Network of Distributed Honeypots. *17th Annual FIRST Conference on Computer Security Incident Handling*, Singapore, SG. Recuperado de https://cert.br/docs/papers/early-warning-first2005.pdf

Internet Governance Forum (IGF). (2014). *Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security*. Recuperado de https://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency--response-teams-certs-for--internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file

Marzano, A., Alexander, D., Fazzion, E., Fonseca, O., Cunha, Í., Hoepers, C., ... Meira Jr, W. (2018). Monitoramento e Caracterização de Botnets Bashlite em Dispositivos IoT. *XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, Campos do Jordão, SP. Recuperado de https://honeytarg.cert.br/honeypots/docs/papers/honeypots-sbrc18.pdf

Marzano, A., Alexander, D., Fonseca, O., Fazzion, E., Hoepers, C., Steding-Jessen, K., ... Meira Jr, W. (2018). The Evolution of Bashlite and Mirai IoT Botnets. *IEEE Symposium on Computers and Communications*, Natal, RN. Recuperado de https://honeytarg.cert.br/honeypots/docs/papers/honeypots-iscc18.pdf

Rossow, C. (2013). Amplification Hell: Revisiting Network Protocols for DDoS Abuse. *NDSS Symposium 2014*, San Diego, CA. Recuperado de https://www.ndss-symposium.org/ndss2014/programme/amplification-hell-revisiting-network-protocols-ddos-abuse/

CAPÍTULO 4

Segurança digital e gestão de riscos: uma análise de empresas brasileiras[1]

Stefania L. Cantoni[2], Leonardo M. Lins[3] e Tatiana Jereissati[4]

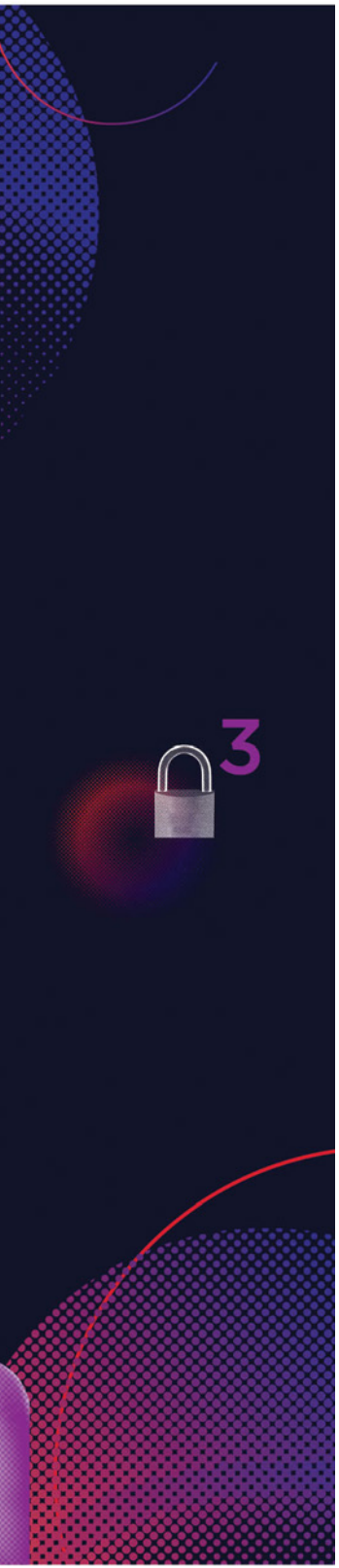
1 Agradecemos a Fábio Senne (Cetic.br|NIC.br) a leitura atenta e as sugestões realizadas neste capítulo.

2 Mestre em Ciência Política pela Universidade de São Paulo (USP), é pesquisadora na Coordenação de Métodos Qualitativos e Estudos Setoriais no Cetic.br|NIC.br.

3 Doutor e mestre em Sociologia pela USP, é pesquisador na Coordenação de Projetos de Pesquisa do Cetic.br|NIC.br, onde coordena as pesquisas TIC Empresas e TIC Provedores.

4 Pós-graduada em Ciências Sociais com menção de Gênero e Políticas Públicas pela Facultad Latinoamericana de Ciencias Sociales (FLACSO-Argentina), é coordenadora de Métodos Qualitativos e Estudos Setoriais no Cetic.br|NIC.br.

2
1



INTRODUÇÃO

Na última década, as tecnologias de informação e comunicação (TIC) consolidaram-se como um importante vetor de desenvolvimento nos diferentes setores da sociedade. Isso é resultado de um contexto em que o ambiente digital torna-se cada vez mais expressivo para as atividades do governo, das empresas e dos indivíduos (OECD, 2015), enquanto a economia baseada em dados adquire a cada dia mais relevância.

Dada a importância das TIC para impulsionar a competitividade dos países, muito tem sido debatido sobre os avanços da economia digital e os efeitos positivos e negativos de uma ampla digitalização dos processos produtivos. De um lado, há um intenso debate sobre os benefícios dos avanços tecnológicos da era digital e os consequentes ganhos de eficiência de uma economia altamente conectada, estabelecendo um novo paradigma de produção com efeitos em diversos setores (Schwab, 2016; Brynjolfsson & Mcafee, 2014). De outro lado, há visões mais cautelosas quanto ao avanço da economia digital, destacando-se as mudanças nas relações de trabalho, o aumento da concentração de renda, a destruição de postos de trabalho, bem como novas ameaças que surgem do aproveitamento das vulnerabilidades criadas pela intensificação de interconexão de indivíduos e organizações (Srnicek, 2016; Frey & Osborne, 2017). Nessa nova conjuntura, os diferentes setores são desafiados a se adequarem com vistas a reduzirem suas desvantagens e a ampliarem os ganhos derivados de uma economia altamente conectada (OECD, 2017; UNCTAD, 2019). Contudo, as diferentes organizações que compõem o cenário econômico apresentam capacidades desiguais de adaptação ao contexto da transformação digital; caso esses hiatos não sejam endereçados, as desigualdades regionais e econômicas poderão se aprofundar (OECD, 2015).

Nesse contexto de transformação impulsionada pelos avanços em Inteligência Artificial (IA), análise de *Big Data* e *cloud computing*, somada ao crescente aumento do número total de indivíduos e dispositivos conectados à Internet, ganha especial importância a discussão sobre as consequências advindas da crescente digitalização das empresas no Brasil e suas implica-

ções para a gestão dessas organizações. Em virtude de o setor produtivo estar entre os mais afetados pela transformação digital em curso, compreender como diferentes empresas têm lidado com a adaptação das suas rotinas a novas tecnologias permitirá o desenho de um panorama dos efeitos de uma economia mais conectada. Dentre os temas ligados à digitalização e à adaptação dos processos empresariais, destaca-se aquele associado aos incidentes de segurança digital e seus efeitos, decorrente de uma crescente exposição ao ambiente digital e de uma dependência, cada vez maior, da interconexão de processos digitalizados e da presença em redes. Assim, o presente capítulo visa discutir o modo como um conjunto de empresas brasileiras conduz sua gestão de riscos de segurança digital. A partir de uma abordagem qualitativa, busca-se analisar a visão que pequenas, médias e grandes empresas brasileiras de diferentes segmentos de atividade econômica têm sobre os riscos de segurança digital, assim como averiguar se possuem processos de gestão desses riscos e como os implementam, incluindo sua avaliação das potenciais consequências, seu tratamento e as limitações enfrentadas por essas empresas para desenvolver uma gestão de risco de segurança digital madura.

ORGANIZAÇÕES, INCERTEZAS E GESTÃO DE RISCO

De maneira geral, em processos de tomada de decisão, o risco relaciona-se à quantidade e à qualidade de informação existente sobre determinada situação; desse modo, entende-se que os riscos variam conforme a incerteza acerca da probabilidade de um evento ocorrer (March, 1994). Apesar de organizações tenderem a evitar a incerteza, para a qual mobiliza, como principais recursos, a criação de padrões de coleta e processamento de informações e o estabelecimento de rotinas internas, diversos fatores podem perturbar essas formas de antecipação e de controle de eventos, trazendo situações adversas (March, 2010).

A gestão de risco é, portanto, o ato de mitigar os resultados não antecipados derivados da variação de informações sobre o ambiente em que se atua (March & Shapira, 1987; OECD, 2015). Os riscos não são apenas resultados da escassez de informações, mas decorrem também dos limites cognitivos individuais que restringem a capacidade de processar e interpretar informações em todo seu conjunto, aumentando as chances

de cursos de ações saírem do previsto e gerarem eventos não esperados (March, 1994). Aliada a isso, a interconexão dos processos entre as mais diversas organizações significa que estas não estão isoladas de problemas que possam ocorrer com as demais, gerando reações imprevistas em cadeias que exigem ações imediatas, as quais nem sempre constam no repertório de rotinas (Perrow, 1999).

Embora riscos não possam ser evitados completamente, é importante que as organizações empreendam esforços para sua adequada gestão. Assumir riscos está na base da atividade de uma empresa: o desenvolvimento de um novo produto, a mudança no modelo de negócios ou a procura por novos mercados são ações envoltas em incertezas que, se evitadas a todo custo, constrangem a capacidade da empresa de explorar novidades que possam trazer retornos positivos. Dessa forma, é importante que as empresas direcionem recursos para a constante criação e o acúmulo de conhecimento sobre os ambientes em que atuam, a fim de reduzirem incertezas e mitigarem riscos, buscando ampliar e melhorar seu escopo de atuação e de desempenho (Pisano, 2017).

GESTÃO DE RISCOS DE SEGURANÇA DIGITAL

As organizações também estão expostas a riscos resultantes da adoção das TIC e da interconexão de sistemas e dispositivos em rede. De natureza dinâmica, o risco relacionado à segurança digital pode se originar de ameaças e vulnerabilidades decorrentes do ambiente digital, e afetar o alcance de objetivos econômicos e sociais, visto que prejudica a "tríade CID", isto é, a confidencialidade, a integridade e também a disponibilidade de atividades.

Vale ressaltar, no entanto, que o risco digital não tem relação apenas com a incerteza relativa ao uso do ambiente digital. A dependência do ambiente digital requer não somente *software* e *hardware*, mas também intervenção humana – direta ou indiretamente –; todos esses aspectos estão sujeitos a ameaças, vulnerabilidades e incidentes.

Os efeitos dessas incertezas sobre os ativos tangíveis e intangíveis das organizações são de natureza econômica e social, de modo que o risco de segurança digital deve ser formulado em termos econômicos e sociais e não puramente técnicos (OECD, 2015).

Nesse contexto, ganha destaque a Gestão de Risco de Segurança Digital (GRSD), definida pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) como o "conjunto de ações coordenadas, tomadas dentro de uma organização e/ou entre organizações, para lidar com os riscos à segurança digital e maximizar as oportunidades"[5] (OECD, 2015, p. 8, tradução nossa). A GRSD compreende a tomada de decisão e uma estrutura mais geral para gerenciar os riscos inerentes às atividades econômicas e sociais, orientada por um conjunto holístico, sistemático e flexível de processos cíclicos os quais ajudam a garantir que as medidas de GRSD sejam "apropriadas e proporcionais aos riscos e aos objetivos econômicos e sociais em jogo"[6] (OECD, 2015, p. 8, tradução nossa).

A seguir são apresentadas quatro possíveis estratégias de tratamento do risco digital pelas organizações.

GESTÃO DE RISCO DIGITAL: QUATRO ESTRATÉGIAS

- **Aceitar o risco:** "assumir o risco" e aceitar o efeito da incerteza sobre os objetivos, incluindo o fracasso parcial ou total. Se a atividade for realizada, o risco não pode ser totalmente eliminado; portanto, algum risco "residual" deve ser aceito. Em geral, a gestão de risco é economicamente eficiente quando os benefícios obtidos com a realização da atividade superam o risco residual.
- **Reduzir o risco:** reduzi-lo ao nível aceitável *(i)* selecionando e aplicando medidas de segurança para proteger as atividades contra certas ameaças potenciais que exploram vulnerabilidades identificadas na avaliação de risco; *(ii)* mudando a atividade, por exemplo: redesenhando-a ou operando-a de maneira diferente, o que pode levar à inovação; e *(iii)* definindo e, conforme necessário, operando medidas de preparação para lidar com a ocorrência de incidentes.
- **Transferir o risco:** transferir os efeitos indesejados da incerteza sobre os objetivos da atividade para terceiros, por exemplo: por contrato ou por meio de seguro.
- **Evitar o risco:** eliminá-lo ao não realizar a atividade, ou eliminar seu elemento digital.

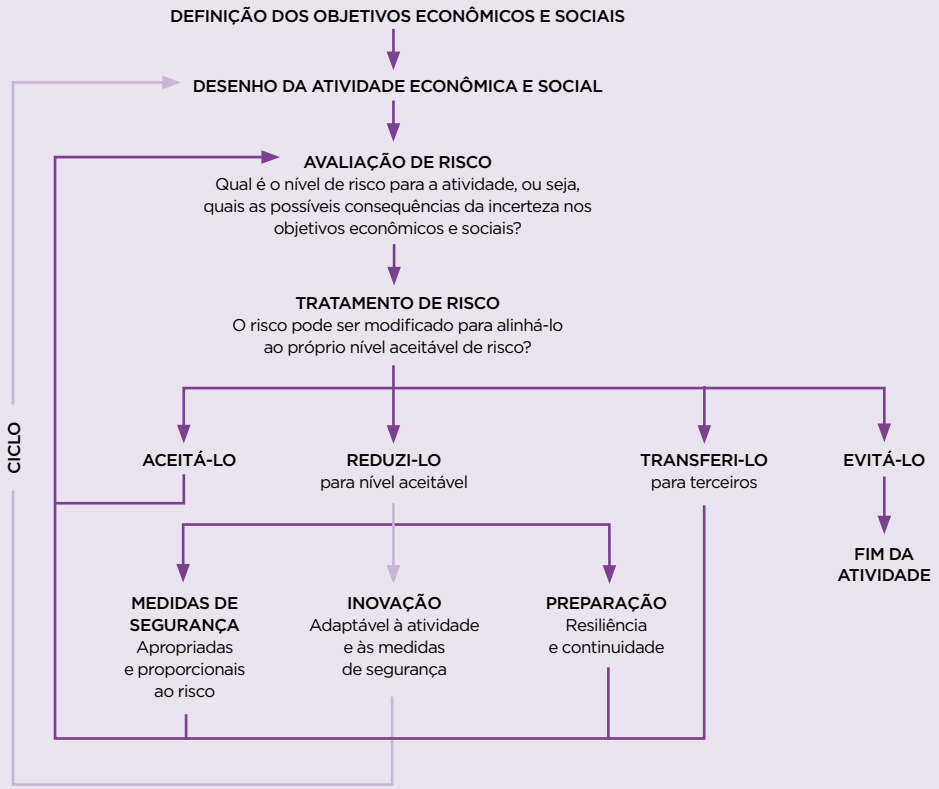
FONTE: ADAPTADO DE OECD (2015).

5 "Digital security risk management is the set of coordinated actions taken within an organisation and/or among organisations, to address digital security risk while maximising opportunities".

6 "appropriate to and commensurate with the risk and economic and social objectives at stake".

Em virtude de os riscos serem inerentes às operações das organizações, a OCDE destaca também a importância do ciclo de gestão de risco para as atividades das empresas, sobretudo como insumo para os processos de tomada de decisão (OECD, 2015). A Figura 1 representa o ciclo da gestão de risco baseado nos princípios operacionais das Recomendações do Conselho da OCDE em Gestão de Risco de Segurança Digital para a Prosperidade Econômica e Social.

FIGURA 1 - UMA VISÃO DO CICLO DA GESTÃO DE RISCO POR ORGANIZAÇÕES



FONTE: OECD (2015).

De acordo com o fluxo proposto pelo modelo, deve-se partir das definições, dos objetivos e do desenho da atividade organizacional. Em seguida, os riscos específicos podem ser avaliados e tratados segundo a abordagem eleita como mais adequada, a fim de que os objetivos iniciais sejam preservados e apoiados (OECD, 2015). Para melhor compreender como ocorre o processo de gestão de riscos pelas organizações, é de fundamental importância que sejam produzidos indicadores que retratem essa realidade.

MEDIÇÃO DE RISCOS DIGITAIS NAS EMPRESAS

Segundo a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (United Nations Conference on Trade and Development – UNCTAD), apenas 4% dos países em desenvolvimento produzem dados sobre o uso das TIC nas empresas, enquanto essa proporção é de 85% entre os países desenvolvidos (UNCTAD, 2019). Esse hiato significa que os países menos desenvolvidos dispõem também de menos informações para formularem políticas que promovam o desenvolvimento da economia digital.

As capacidades e os recursos dos países para a medição de tais fenômenos não têm acompanhado o ritmo acelerado da transformação digital. Além da falta de recursos humanos e financeiros para essa tarefa, há uma série de desafios metodológicos que contribuem para esse cenário de baixa produção de dados, que se agrava no âmbito da segurança digital. Entre os motivos para isso, está a falta de definições padronizadas relativas a conceitos, tipologia e taxonomia, o que dificulta o processo de produção de dados comparáveis. Soma-se também a escassez histórica de dados sobre temas especificamente ligados a vulnerabilidades, ameaças e incidentes digitais (OECD, 2019b). A ausência de um padrão metodológico orientador da produção de dados é um desafio para a formulação de políticas públicas que enderecem o tema (OECD, 2019b).

A fim de atender a essa lacuna de informação e contribuir para a criação de repositórios de dados sobre esse tema, após a Reunião Ministerial de Cancún de 2016 sobre a Economia Digital[7], a OCDE iniciou um projeto para mapear pesquisas com dados sobre risco de segurança digital. A análise de pes-

7 A Declaração Ministerial sobre Economia Digital, ou "Declaração de Cancún" está disponível em: https://www.oecd.org/internet/Digital-Economy-Ministerial-Declaration-2016.pdf

quisas existentes revelou que poucas incluíam perguntas sobre práticas de gestão de riscos de segurança digital; quando havia, os indicadores eram restritos a medidas técnicas (OECD, 2019b). Nesse cenário, tem início a iniciativa da OCDE nomeada *Measuring Digital Security Risk Management Practices in Business* (Medição de Práticas de Gestão de Risco de Segurança Digital entre Empresas), detalhada a seguir.

A INICIATIVA DA OCDE: MEDIÇÃO DE PRÁTICAS DE GESTÃO DE RISCO DE SEGURANÇA DIGITAL ENTRE EMPRESAS

Com o objetivo de oferecer parâmetros para as empresas avaliarem as próprias práticas de GRSD, assim como informar as políticas públicas destinadas a aumentar o nível de maturidade das empresas no que diz respeito à GRSD, a OCDE (2019a) elaborou o projeto "Medição de Práticas de Gestão de Risco de Segurança Digital entre Empresas", cujo principal objetivo é fomentar a medição de práticas de GRSD, principalmente nas pequenas e médias empresas (PME), em diferentes setores econômicos. De acordo com a OECD (2017), as PME compõem a maioria da população empresarial e contribuem muito para a criação de emprego e valor; além disso, existe uma escassez de evidências relevantes, confiáveis e rigorosas sobre as práticas de GRSD nas PME.

Alinhado aos princípios das Recomendações do Conselho da OCDE em Gestão de Risco de Segurança Digital para a Prosperidade Econômica e Social, a organização desenvolveu um *framework* para medição de práticas de gestão de risco de segurança digital em empresas (ver p. 138). Estruturado em três fases[8] conduzidas entre fevereiro de 2017 e novembro de 2018, o projeto integrou o projeto Going Digital, que visa fornecer, especialmente aos formuladores de políticas públicas, ferramentas necessárias para ajudar a economia e a sociedade a prosperar em um mundo cada vez mais digital e orientado por dados[9].

---

8 O relatório da OCDE referente às três fases do projeto pode ser acessado em https://www.oecd-ilibrary.org/science-and-technology/measuring-digital-security-risk-management-practices-in-businesses_7b93c1f1-en

9 O projeto Going Digital da OCDE está atualmente na segunda fase, de 2019 a 2020, marcada pelo lançamento do Going Digital Toolkit (https://goingdigital.oecd.org/en/). A primeira fase, de 2017 a 2018, foi encerrada com a realização do Going Digital Summit e o lançamento dos documentos "Going Digital: Shaping Policies, Improving Lives" e "Measuring the Digital Transformation: A Roadmap for the Future". Mais informações em: http://www.oecd.org/going-digital/project/

MÓDULOS PARA MEDIÇÃO DE PRÁTICAS DE GESTÃO DE RISCO SEGUNDO FRAMEWORK *DA OCDE*

Adotando uma estrutura modular, o *framework* proposto pela OCDE permite a medição de conceitos-chave[10] de maneira comparável no âmbito internacional, além de possibilitar que os países o adaptem para atender às necessidades específicas de cada contexto nacional. As seis dimensões cobertas pelo *framework* são detalhadas a seguir.

- **Módulo A –** Informações básicas sobre a empresa: porte, setor de atividade e receita anual. Mede a intensidade digital da empresa a partir da composição de indicadores selecionados sobre uso das TIC.
- **Módulo B –** Governança de Risco em Segurança Digital: avalia se existe uma estrutura de governança de GRSD adequada na empresa respondente.
- **Módulo C –** Práticas de avaliação de risco digital: mapeia o processo de três etapas da avaliação de riscos (identificação, análise e avaliação de informações); verifica se o processo de avaliação de riscos leva em consideração as consequências da incerteza sobre outras partes interessadas; e o resultado do processo de avaliação de risco.
- **Módulo D –** Práticas de redução de risco digital: mede quais práticas de redução de risco foram selecionadas e operadas e quais os riscos que essas práticas pretendiam reduzir, e compreende o motivo das decisões de redução de risco (ou seja, se foram a consequência de um processo de avaliação de risco).
- **Módulo E –** Práticas de transferência de risco digital: mede ações ou processos usados para transferir para outra parte os efeitos indesejados da incerteza nas atividades da empresa. Tem foco no uso de seguros (por exemplo, apólices e suas respectivas coberturas), mede quais riscos são transferidos e compreende o motivo das decisões de transferência de riscos (isto é, se foram a consequência de um processo de avaliação de riscos).
- **Módulo F –** Sensibilização sobre riscos de segurança digital e treinamento: mede a conscientização do respondente em relação aos efeitos que o risco de segurança digital pode trazer para a consecução dos objetivos econômicos e sociais de uma empresa, como o gerenciamento de risco de segurança digital pode afetar outras pessoas, se o respondente possui as habilidades necessárias para entender o risco de segurança digital, os meios para aquisição de habilidades e se e onde existe um hiato em relação às habilidades.

---

10 A elaboração do questionário-piloto considerou os conceitos-chave e as definições, os desafios de medição e os indicadores propostos no documento "Proposed draft indicators on digital security risk management practice in businesses" (OECD, 2017), principal referência metodológica que norteou o projeto da OCDE. Um adendo a esse trabalho, intitulado "Revision of Indicators for Measuring Digital Security Management Practices in Businesses", ofereceu contribuições ao *framework* analítico original e indicadores com base no *feedback* dos grupos de trabalho da OCDE WP-SPDE e WP-MADE. Além disso, três questionários de pesquisa foram utilizados como referências metodológicas para seu desenho: o Community Survey on ICT Usage and E-Commerce in Enterprises (EUROSTAT, 2017), o United Kingdom Cyber Security Breaches Survey 2018 (Klahr et al., 2018) e o Canadian Survey of Cyber Security and Cybercrime (Statistics Canada, 2017).

CONSTRUÇÃO DE QUESTIONÁRIO PARA A MEDIÇÃO DE PRÁTICAS DE GESTÃO DE RISCO

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), departamentos do NIC.br, estabeleceram um protocolo de cooperação com a OCDE, com o objetivo de construir um instrumento de coleta de dados, conforme atividades específicas detalhadas a seguir:

- Revisão de questionários e relatórios sobre segurança e riscos digitais, visando integrar indicadores, perguntas e categorias de respostas já existentes;
- Desenvolvimento de uma versão preliminar do questionário-piloto para ser compartilhada com os grupos de trabalho da OCDE Working Party on Security and Privacy in the Digital Economy (WP-SPDE)[11] e Working Party on Measurement and Analysis of the Digital Economy (WP-MADE)[12];
- Recebimento de *feedback* dos grupos de trabalho sobre os módulos do questionário propostos, incluindo: conceitos, definições, categorias de perguntas e respostas, estrutura e fluxo de tópicos, sequência de perguntas, filtros e redação;
- Realização de entrevistas cognitivas e elaboração do relatório final com a análise e as recomendações para aprimoramento do questionário;
- Atualização da versão preliminar com base nas entrevistas cognitivas e desenvolvimento da versão final do questionário para discussão entre os grupos de trabalho para validação.

O instrumento de coleta foi elaborado e aprimorado entre março e abril de 2018 pelo grupo composto por representantes

11 O Grupo de Trabalho da OCDE sobre Segurança e Privacidade na Economia Digital (SPDE) desenvolve análises de políticas públicas e recomendações de alto nível para ajudar governos e outras partes interessadas a garantir que a segurança digital e a proteção da privacidade promovam o desenvolvimento da economia digital. Mais informações em: https://www.oecd.org/sti/ieconomy/workingpartyonsecurityandprivacyinthedigitaleconomyspde.htm

12 O mandato do Grupo de Trabalho da OCDE sobre Medição e Análise da Economia Digital (MADE) é conduzir a medição da economia digital e analisar a contribuição das políticas da economia digital para o desempenho econômico e os resultados sociais. Mais informações em: https://oecdgroups.oecd.org/Bodies/ShowBodyView.aspx?BodyID=5291&Lang=en&Book=True

do Cetic.br|NIC.br, CERT.br|NIC.br e da OCDE. Em seguida, esse questionário foi submetido a um processo de testes cognitivos, revisado e testado pela Federation of European of Risk Management Associations (FERMA), no período de julho a setembro de 2018, o qual reuniu 80 entrevistas, principalmente de gestores de riscos de grandes empresas de quinze países. Como resultado dos pilotos, recomendou-se que determinados aspectos do instrumento de pesquisa fossem aprimorados, como a duração do questionário e ajustes pontuais às formulações de perguntas e respostas (OECD, 2019b).

ABORDAGEM QUALITATIVA NO BRASIL: ENTREVISTAS COGNITIVAS COM EMPRESAS BRASILEIRAS

No âmbito do processo de elaboração do instrumento de coleta do projeto "Medição de Práticas de Gestão de Risco de Segurança Digital entre Empresas", da OCDE, o Cetic.br|NIC.br realizou um conjunto de entrevistas cognitivas[13] com empresas brasileiras com o objetivo de avaliar a adequação do questionário ao contexto nacional e sua aplicabilidade entre pequenas, médias e grandes empresas. Além disso, buscou identificar qualquer sensibilidade possível relacionada às perguntas, bem como garantir que as perguntas eram adequadas ao público-alvo (OECD, 2019b). Além de fornecer informações para a revisão do questionário da OCDE, os resultados dessa etapa foram utilizados pelo Cetic.br|NIC.br como insumo para a realização de uma análise qualitativa sobre o tema gestão de risco de segurança digital de 16 empresas brasileiras.

METODOLOGIA QUALITATIVA: RESPONDENTES E TRATAMENTO DOS DADOS

Entre 26 de março e 11 de abril de 2018, o Cetic.br|NIC.br conduziu 16 entrevistas cognitivas presenciais[14] com pessoas

13 A entrevista cognitiva avalia perguntas da pesquisa, usando várias técnicas para averiguar como os entrevistados entendem as questões e como chegam, por meio de seu próprio raciocínio cognitivo, às suas respostas (Groves et al., 2009). É particularmente útil para avaliar novas perguntas e identificar possíveis fontes de erro antes de administrar questionários de pesquisa em campo, assim como avaliar questões de tradução e adaptação de questionários internacionais, identificando possíveis sensibilidades a questões específicas e garantindo que as perguntas sejam apropriadas para cada população-alvo.

14 Nos casos em que não era possível realizar entrevistas em salas de entrevistas preparadas, os respondentes foram contatados no local de trabalho. Todas as entrevistas – seja na sala de entrevistas ou no local – foram integralmente gravadas e recomendações éticas internacionalmente aceitas foram aplicadas.

empregadas em empresas de diferentes portes[15], atividades econômicas e localizações geográficas, em três municípios do Brasil: São Paulo, Recife e Porto Alegre (Tabela 1)[16]. Essas localidades foram selecionadas para a garantia de uma diversidade regional entre os respondentes. O tipo de atividade econômica das empresas entrevistadas foi classificado de acordo com a Classificação Nacional de Atividades Econômicas (CNAE 2.0) e refere-se apenas a empresas legalmente constituídas no Brasil, categorizadas e registradas em registros oficiais. Além disso, embora o questionário fosse destinado a pequenas e médias empresas (PME), foram entrevistadas cinco empresas de porte grande, a fim de compreender a influência do tamanho e da complexidade dessas organizações na compreensão geral do questionário.

TABELA 1 – CARACTERÍSTICAS DAS EMPRESAS SELECIONADAS PARA A REALIZAÇÃO DE ENTREVISTAS COGNITIVAS

CIDADE	SETOR ECONÔMICO	PORTE	CARGO DO/A ENTREVISTADO/A
São Paulo	Transporte, armazenagem e correio	Grande	Diretor/a de Riscos
São Paulo	Atividades imobiliárias	Grande	Diretor/a de TI
São Paulo	Alojamento e alimentação	Grande	Supervisor/a de TI
São Paulo	Construção	Grande	Gerente de TI
Recife	Comércio	Grande	Gerente de TI
São Paulo	Artes, cultura, esportes e recreação	Médio	Coordenador/a de TI
São Paulo	Atividades imobiliárias	Médio	Coordenador/a de TI e de Infraestrutura
São Paulo	Transporte, armazenagem e correio	Médio	Gerente Administrativo/a
São Paulo	Informação e comunicação	Médio	Gerente Financeiro/a
Porto Alegre	Construção	Médio	Gerente de TI e Administrativo/a
São Paulo	Informação e comunicação	Pequeno	Gerente de Infraestrutura
São Paulo	Artes, cultura, esportes e recreação	Pequeno	Gerente de Operações
São Paulo	Artes, cultura, esportes e recreação	Pequeno	Gerente de Projetos
São Paulo	Comércio	Pequeno	Proprietário/a
Recife	Atividades imobiliárias	Pequeno	Proprietário/a
Porto Alegre	Alojamento e alimentação	Pequeno	Proprietário/a

FONTE: ELABORAÇÃO PRÓPRIA.

15 O conceito de tamanho das empresas considera pequenas (10 a 49 pessoas empregadas), médias (50 a 249 pessoas empregadas) e grandes empresas (250 ou mais pessoas empregadas). As microempresas, aquelas com 1 a 9 pessoas empregadas, não foram incluídas no escopo dos testes cognitivos.

16 O Cetic.br|NIC.br contou com o apoio do IBOPE Inteligência para a prospecção e o contato com os respondentes e a logística das entrevistas presenciais e não-presenciais.

As pessoas selecionadas para as entrevistas eram formalmente empregadas pelas empresas[17]. Inicialmente, foram buscados profissionais que tivessem atuação na gestão de riscos econômicos e sociais enfrentados pela organização, como gestores de risco. Caso não houvesse uma pessoa empregada a quem tivesse sido explicitamente atribuída a responsabilidade pelo gerenciamento de riscos na empresa, a entrevista era realizada com proprietários, CEOs, gestores ou outras pessoas com uma visão geral do lado econômico ou comercial da empresa[18].

A análise do material empírico foi realizada a partir de um procedimento de codificação das transcrições das entrevistas cognitivas, o que permitiu classificar e organizar os conteúdos coletados, comparar respostas e conteúdos discursivos de diferentes respondentes, bem como mensurar remissões a determinados temas e cruzá-las com atributos específicos do universo dos entrevistados. É importante destacar que, apesar de o *framework* da OCDE ter norteado a construção do questionário e auxiliado na análise dos resultados, o material resultante das entrevistas cognitivas foi analisado considerando características do contexto brasileiro[19] e incluindo novas categorizações e agrupamentos das dimensões de análise.

GESTÃO DE RISCOS DE SEGURANÇA DIGITAL ENTRE EMPRESAS BRASILEIRAS

A seguir, será apresentado um breve cenário de indicadores estatísticos de GRSD entre empresas brasileiras a partir dos dados inéditos coletadas pela pesquisa TIC Empresas 2019

17 O conceito de pessoas empregadas refere-se àquelas remuneradas diretamente pela empresa, com ou sem contrato de trabalho. O número de pessoas ocupadas incluiu empregados assalariados, *freelancers* pagos diretamente pela empresa, funcionários e associados, familiares e trabalhadores temporários. Terceiros e consultores não foram inclusos.

18 No caso do Brasil, vale notar que vários entrevistados consideraram os riscos de segurança digital principalmente como uma questão técnica e indicaram que pessoas da equipe técnica (como gerentes de TI) eram os melhores respondentes em suas empresas para responder a perguntas sobre decisões de gerenciamento de riscos de segurança digital.

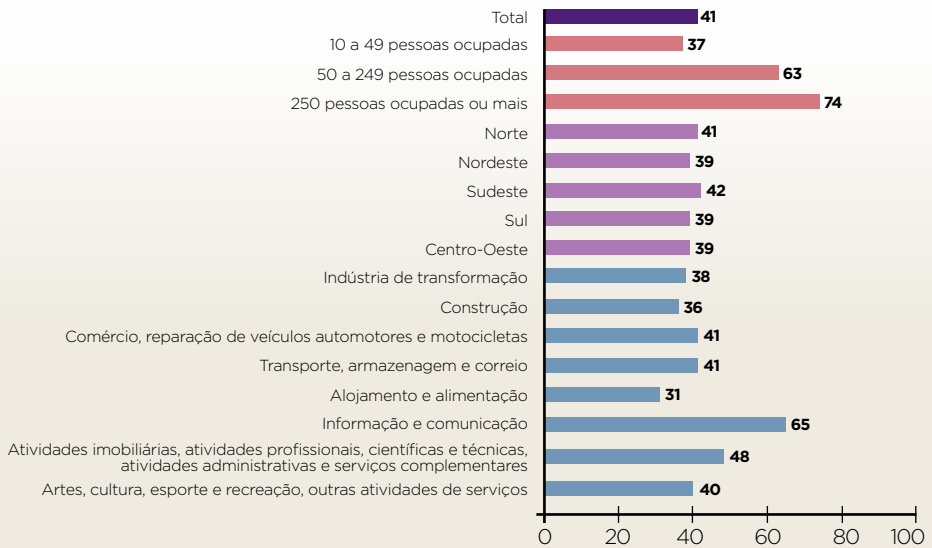
19 Perfil das empresas: além do recorte realizado a partir do *framework* da OCDE, o contexto específico de cada empresa foi considerado relevante para a compreensão da gestão de riscos de segurança digital. Assim, as cinco dimensões selecionadas para a realização da análise, bem como as categorias para a codificação correspondente, foram adaptadas de modo a fazerem sentido à realidade das empresas brasileiras, contemplando, por exemplo, as barreiras enfrentadas para a gestão do risco de segurança digital.

(NIC.br, 2019), com o objetivo de oferecer um contexto geral sobre esse tema no país[20].

BREVE CONTEXTO DE GRSD NO BRASIL: DADOS DA TIC EMPRESAS

Segundo dados da pesquisa TIC Empresas 2019 (NIC.br, 2019), 41% das empresas possuem algum tipo de política de segurança digital, percentual de maior preponderância entre as médias (63%) e grandes empresas (74%). Conforme mostra o Gráfico 1, embora não haja diferenças por região do país, o setor de atividade com mais empresas que possuem algum tipo de política de segurança digital é o de Informação e Comunicação (65%), caracterizado pelo uso intensivo das TIC e pela entrega de produtos ou serviços digitais.

GRÁFICO 1 – EMPRESAS QUE POSSUEM UMA POLÍTICA DE SEGURANÇA DIGITAL
Total de empresas com acesso à Internet (%)

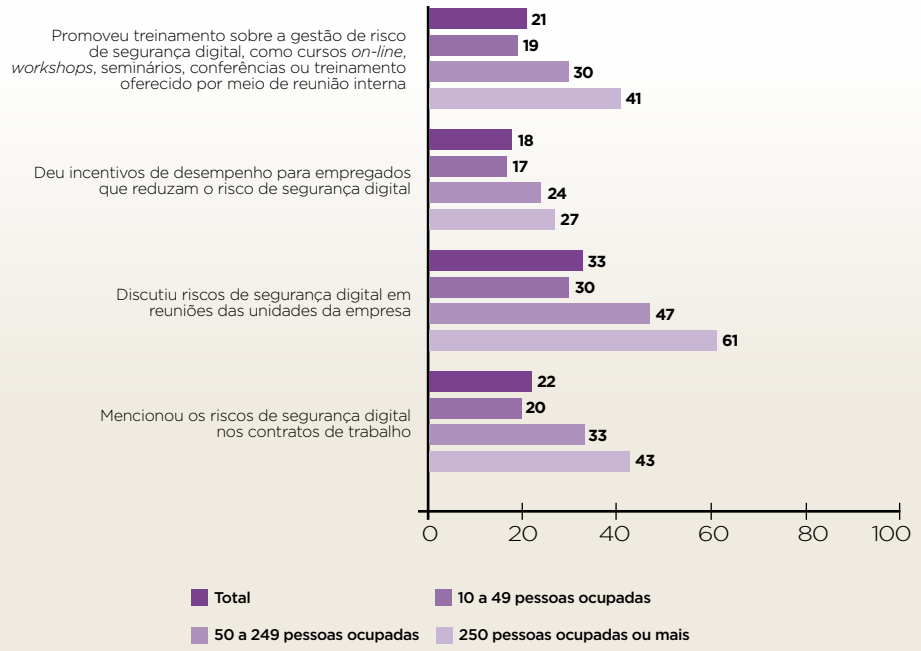


FONTE: NIC.BR (2019).

20 A pesquisa TIC Empresas, conduzida a cada dois anos pelo Cetic.br|NIC.br, tem como objetivo principal medir a posse e o uso das tecnologias de informação e comunicação (TIC) entre as empresas brasileiras com 10 ou mais pessoas ocupadas. Para mais informações sobre a pesquisa, acesse https://cetic.br/pt/pesquisa/empresas/

A pesquisa TIC Empresas 2019 (NIC.br, 2019) também buscou compreender como as políticas de gestão de riscos das empresas se traduzem em práticas voltadas à mitigação dos riscos de segurança digital. Nesse quesito, os dados retratam que poucas empresas implementam ações para informar os funcionários sobre os riscos digitais, tais como treinamentos (21%) ou discussão sobre esse tema em suas reuniões (33%); além disso, é reduzido o percentual de empresas que indicaram, por exemplo, ter contratos de trabalho que mencionem segurança digital (22%) ou incentivos de desempenho para redução de risco de digital (18%). De maneira geral, as ações voltadas para segurança digital estão mais presentes nas grandes empresas, com a discussão em reuniões das unidades das empresas sendo a mais citada, visto ser adotada em 61% das grandes empresas.

GRÁFICO 2 – EMPRESAS, POR PRÁTICAS DE SEGURANÇA DIGITAL
Total de empresas com acesso à Internet (%)



FONTE: NIC.BR (2019).

Os dados levantados pela pesquisa TIC Empresas 2019 (NIC.br, 2019) revelam a presença incipiente de políticas ou práticas de segurança digital entre as empresas brasileiras de todos os portes, sobretudo nas pequenas empresas. A seguir, esses temas serão explorados a partir da abordagem qualitativa conduzida com empresas brasileiras selecionadas.

PRINCIPAIS DESTAQUES DA ANÁLISE DAS ENTREVISTAS QUALITATIVAS COM EMPRESAS BRASILEIRAS

Baseadas no *framework* da OCDE, cinco dimensões foram estabelecidas para nortear a análise das entrevistas cognitivas realizadas com as 16 empresas brasileiras. Os principais destaques serão apresentados para cada uma das dimensões analíticas a seguir: *(i)* Visão sobre (a gestão do) risco digital e exposição ao risco; *(ii)* Processos de análise e avaliação de risco digital; *(iii)* Nível aceitável do risco digital e consequências dos incidentes; *(iv)* Práticas de redução e transferência de risco digital; e *(v)* Estrutura da empresa e dificuldades para a gestão de risco de segurança digital.

Visão sobre (a gestão do) risco digital e exposição ao risco

O *framework* da OCDE busca averiguar **se** e **como** se integra a gestão de risco de segurança digital (GRSD) na prática de gestão de riscos das empresas. A partir dessa perspectiva, o risco digital não é essencialmente distinto de outros tipos de riscos, de modo que deveria ser objeto de uma tomada de decisão proativa no nível gerencial (Jalali, 2018), ao mesmo tempo em que a GRSD deveria ser integrada à estrutura mais ampla de gestão de riscos (OECD, 2015). No contexto brasileiro, porém, as PME nem sempre contam com um departamento, uma área ou uma pessoa responsável pela gestão de risco da empresa como um todo, além de a segurança digital também não ser considerada propriamente uma área de gestão.

Assim, quando os respondentes das empresas brasileiras entrevistadas foram consultados sobre gestão de riscos especificamente no contexto digital, os riscos citados muitas vezes diziam respeito a outros tipos de riscos, tais como financeiros, operacionais e de contratação. Essa visão da gestão de risco digital – junto

com outros elementos abordados a seguir – evidencia o fato de os assuntos relativos à segurança digital, tanto em pequenas, médias e até em algumas grandes empresas entrevistadas, ficarem circunscritos à área técnica ou relacionada à gestão de incidentes.

> "Olha, eu entendo gestão de risco como uma linguagem muito de informática, uma coisa muito relacionada a uma coisa da informação. [...] Eu entenderia como algo ligado a uma governança corporativa, à questão de auditoria de riscos, coisas de uma empresa maior de um negócio maior de área compliance [...] uma série de normas que tem que ser atendidas; se não forem atendidas pode gerar uma multa."
>
> (PROPRIETÁRIO, EMPRESA DE PEQUENO PORTE)

Essa visão da segurança digital como uma questão técnica implica que o foco da atenção está no risco de segurança para sistemas e redes, visão reforçada pelos exemplos fornecidos pelos entrevistados – como violação de dados e casos recentes de ataques de *ransomware*. Já as consequências econômicas e sociais dos incidentes – perdas financeiras e de reputação, de oportunidades de negócio e de competitividade, de confiança e o impacto na privacidade –, não ocupam um lugar central na agenda das lideranças das empresas entrevistadas.

A GRSD pressupõe a existência de ações coordenadas para lidar com os riscos de segurança digital e maximizar as oportunidades, assim como sua integração numa estrutura mais geral para gerenciar riscos às atividades da organização (OECD, 2015). Além disso, ela seria baseada em um conjunto sistemático e flexível de processos cíclicos, a fim de garantir que as medidas de GRSD sejam apropriadas e proporcionais aos riscos e aos objetivos econômicos e sociais em jogo (OECD, 2015). Se as visões sobre gestão de risco das empresas variam pouco segundo o setor econômico e/ou seu grau de digitalização, o porte e a internacionalização de uma empresa aparecem como variáveis relevantes para a compreensão do tema, em razão de as únicas empresas que informaram contar com processos estabelecidos de gestão de riscos de segurança digital, ou pelo menos contar com um processo reflexivo de avaliação de risco, terem sido as de maior porte e multinacionais.

Constatou-se que, além de a GRSD não fazer parte da rotina de pequenas e médias empresas, para muitos respondentes não há clareza quanto ao próprio conceito de risco digital. A dificuldade de nomear e perceber os riscos digitais independe da maturidade digital e do setor econômico da empresa em ques-

tão. Nas entrevistas, o risco é principalmente associado com o vazamento de informações da empresa[21]. De forma transversal a todos os perfis das empresas entrevistadas, há uma grande preocupação que funcionários e/ou terceiros tenham acesso – indevido –, a *e-mails,* à Internet, a situações envolvendo a perda e o vazamento de informações da empresa, o sequestro de dados e a invasão dos computadores e servidores.

Em relação a essas preocupações, sobretudo no que diz respeito ao sequestro de dados, é importante observar que o *ransomware*[22] é um dos ataques à segurança digital mais disseminados e representa uma séria ameaça às empresas de qualquer porte, mas principalmente às PME (Stuart, 2016). Contudo, as melhores práticas de mitigação se aplicam a todos e, se realizadas corretamente, têm efeitos positivos muito além do *ransomware*. Nas entrevistas, os exemplos de riscos citados vinham acompanhados do que se acredita ser uma das medidas mais efetivas para reduzi-los: fazer *backup* dos dados, seja em servidores próprios, na nuvem ou contratando um serviço para tal. Isso se verifica também nas duas empresas mais maduras em termos de segurança digital, uma das quais teria, segundo o entrevistado, "duplicata" e até "triplicata" das informações, junto com um plano de continuidade de negócios sólido na área de tecnologia da informação.

> "[...] a gente coloca dados criptografados [...] é mais difícil a gente sofrer uma invasão, ter os dados vazados, dos clientes, funcionários mesmo [...] A disponibilidade, a perda das informações, que a gente costuma trabalhar com *backup*, [...] principalmente em serviços essenciais para empresa telefone IP, por exemplo, nosso é telefone IP, caixa de servidor de *e-mail* é super importante, parte de servidor de arquivos."
>
> (GERENTE DE OPERAÇÕES, EMPRESA DE PEQUENO PORTE)

Embora pequenas empresas apliquem práticas de tratamento do risco digital – no caso, para reduzi-lo –, os relatos indicam seu isolamento em relação a decisões tecnológicas, circunscrita ao "pessoal da TI". Dado que as medidas para reduzir o risco de segurança digital podem ter efeitos negativos sobre as ati-

21 É importante ressaltar que as entrevistas foram realizadas em 2018, após o ataque WannaCry, a maior infecção de *ransomware* da história, que afetou mais de 200 mil sistemas em 150 países.

22 Depois de ser infectado por *malware*, ao clicar em um *link* ou baixar e abrir um arquivo, o usuário desavisado descobre que não consegue inicializar seus programas ou acessar seus arquivos. Uma nota de resgate informa que seus arquivos agora estão criptografados e um pagamento é necessário para liberá-los. Enquanto isso, o *ransomware* já se espalhou por toda a rede corporativa, criptografando conforme avança (Stuart, 2016).

vidades econômicas e sociais que devem proteger – afetando processos de inovação, desempenho etc. –, é necessária a existência de processos de gestão de risco que busquem reduzi-lo até um nível aceitável sem comprometer o funcionamento da empresa. Essa ponderação, adotada no nível da liderança das empresas, foi pouco relatada nas entrevistas realizadas.

A única empresa entrevistada a mencionar as opções de tratamento de riscos, isto é, analisar e reduzir o risco, e mitigar as consequências do incidente – era uma multinacional de grande porte. Para o respondente dessa empresa, inclusive, os riscos não são considerados algo estritamente negativo, em razão de poderem trazer também ganhos para a companhia. Nesse quesito, um ponto a destacar é que a própria noção de risco pressupõe explorar a incerteza: inovar implica assumir riscos (e a segurança digital visa aumentar a probabilidade do sucesso de atividades econômicas e sociais) (OECD, 2015). Ou seja, apesar de o "risco" geralmente capturar apenas os efeitos prejudiciais da incerteza, esta também pode ter efeitos positivos e beneficiar uma atividade. Dessa forma, o efeito benéfico da incerteza é frequentemente chamado "oportunidade" em vez de risco. A relação entre risco e oportunidade é importante, pois a GRSD também pode ser usada para criar valor, detectando sistematicamente e aproveitando as incertezas para impulsionar a inovação (OECD, 2015). Porém, se é verdade que algumas organizações ressurgem mais fortes, e se as organizações mais resilientes em termos de segurança digital podem responder a um incidente, consertar as vulnerabilidades e aplicar as lições às estratégias para o futuro, um elemento-chave de sua resiliência é a governança, tarefa que cabe à liderança da organização e não recai apenas na área técnica (EIU, 2018).

"Na gestão de riscos, você tem os riscos positivos e os riscos negativos né, de repente surge uma oportunidade de um risco positivo que eu posso trazer para a organização e a gente rever alguma situação que pode ter um ganho para a companhia. [...]. Gestão de risco não é só perda de negócio."

(DIRETOR DE RISCOS, EMPRESA DE GRANDE PORTE)

Apesar de existir grande preocupação com o acesso a informações sigilosas, o principal ponto de atenção está relacionado ao aproveitamento dessa informação por parte dos concorrentes ou dos próprios funcionários. Ainda que alguns responden-

tes tenham mencionado a importância das ações de *compliance*, a preocupação com a proteção de dados pessoais de parceiros comerciais não foi mencionada nas entrevistas[23]. Em última instância, os respondentes reconhecem riscos que geram danos financeiros de forma mais imediata. Cabe notar que o roubo de segredos comerciais[24] pode levar a custos significativos de oportunidade, impactos negativos na inovação, aumento de gastos em segurança e danos à reputação (PwC, 2019), especialmente quando se trata de PME que são, ao mesmo tempo, alvos mais vulneráveis a esse tipo de ataque.

> "Invadiram o *site* da empresa, colocaram com um monte de propaganda [...]. É o risco de perder venda, é o risco de perder a parceria com o meu distribuidor com o meu fabricante. [...]. É questão de informação [...]. São concorrentes estão no mesmo mercado então a gente tem que manter um sigilo."
>
> (GERENTE FINANCEIRO E INFRAESTRUTURA, EMPRESA DE PORTE MÉDIO)

Observada em empresas de perfis diversos, há uma associação do risco com algo que vem da própria empresa, ou seja, um risco interno: a segurança digital, nesse sentido, é considerada o estabelecimento de regras do que os empregados podem ou não podem fazer. Isso torna o controle dos empregados uma questão chave para se gerir esses riscos – por exemplo, uma questão muito presente nos relatos é o potencial uso indevido de *pendrives* por parte dos funcionários, com o intuito de se apropriar de informações que os beneficiassem. Essa visão do "risco interno", muitas vezes ligada a comportamentos dos funcionários, resulta em práticas de gestão caracterizadas pelo controle, a qual contrasta com uma gestão que estimule a responsabilidade dos colaboradores e fomente a sensibilização e o treinamento. Para manter o ecossistema da segurança digital saudável, os funcionários precisam ser treinados para que entendam o que são comportamentos seguros em termos de segurança digital e como evitar riscos desnecessários (Worthy, 2017).

---

23 Também à época das entrevistas, o General Data Protection Regulation (GDPR) da União Europeia e a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira ainda não faziam parte dos debates na mídia.

24 São valiosos segredos comerciais os conhecimentos e as informações que as empresas tratam como confidenciais, considerando-os um ativo fundamental para sua vantagem competitiva no mercado. Um número significativo de intrusões cibernéticas tem como alvo conhecimento e informações valiosas, como detalhes sobre o negócio, *know-how* e tecnologia que as empresas tratam como confidenciais.

"[...] é o controle de tudo que trafega na minha rede, tudo que entra e sai, então eu tenho que ter esse controle. Eu tenho uma ferramenta hoje que me ajuda nesse controle, [...] principalmente informação de clientes. [...] hoje, se um funcionário meu espetar um *pendrive* [...] minha parte de risco digital é isso, controlar as informações que entram e saem da minha rede."

(COORDENADOR DE TI E INFRAESTRUTURA, EMPRESA DE PORTE MÉDIO)

Ainda em relação a esse tema, para respondentes de empresas de pequeno porte, existe uma visão de risco como algo interno e de acesso "físico". Nesse sentido, vale salientar que a segurança digital pode ser comprometida com qualquer incidente que afete a tríade CID de *hardware, software*, redes e/ou dados dos quais dependem as atividades econômicas e sociais de uma empresa. Eventos potenciais podem ser ameaças intencionais ou não intencionais (como erros humanos ou eventos naturais) que se aproveitam de vulnerabilidades – por exemplo, erros (*bugs*) em *hardware, software* ou redes; falta de treinamento; proteção insuficiente, seja ela digital (*firewalls*) ou física (câmaras e fechaduras no *data center*); assim como procedimentos inapropriados (processos de *backup* ou planos de recuperação de desastres).

Processos de análise e avaliação de risco digital

A gestão de risco digital pressupõe que os riscos sejam identificados (riscos possíveis, lembrando a natureza dinâmica e cambiante dos riscos digitais), analisados (a probabilidade de afetarem a própria empresa e os potenciais impactos) e avaliados (a partir do qual ações são tomadas, considerando o apetite de risco da organização) (OECD, 2015).

Contudo, nos relatos obtidos, não houve menção a processos estabelecidos para identificar os riscos, analisar as potenciais consequências – em relação às vulnerabilidades da própria empresa – nem para decidir cursos de ação a partir de uma avaliação. Sobre este último, verificou-se que apenas a empresa mais madura em termos de GRSD – multinacional e de porte grande – possui processos contínuos e com frequência pré-definida para decidir o quanto de risco deve ser assumido, reduzido, transferido e evitado (ver p. 134), associando essa situação, inclusive, ao apetite de risco da organização. Com exceção dessa empresa, as quatro estratégias de tratamento do risco não foram identificadas pelos respondentes.

> "A gente não tem um processo, porque isso a gente decide em reuniões de diretoria. Mas não está escrito, fulano traz, ciclano aprova. Não, a gente tem um processo que ele está, chamar de 50% maduro, mas não está formal. As pessoas sabem o que acontece, mas não está escrito isso."
>
> (DIRETOR DE TI, EMPRESA DE GRANDE PORTE)

Cabe salientar que a tomada de decisão referente às estratégias de tratamento de risco decorre de seu processo de avaliação. A medida de quanto risco a organização está disposta a aceitar para realizar uma atividade é conhecida como seu "apetite de risco", que depende de muitos fatores, tais como o tipo de atividade e seus objetivos, a cultura da organização, as condições de mercado, etc. A menos que o risco seja totalmente aceito ou evitado, uma decisão deve ser tomada sobre como reduzi-lo ao nível aceitável ou transferi-lo (OECD, 2015); por isso, o processo de avaliação é imprescindível para se ter propriamente uma gestão de risco.

A percepção dos riscos digitais como uma questão exclusivamente técnica parece levar a níveis descoordenados de práticas de GRSD. De fato, nas entrevistas, não houve evidências de empresas com processos estruturados que considerem os resultados da avaliação de risco digital em suas ações gerenciais. Ao contrário, foi verificado que as ações implementadas costumam ser reativas, isto é, após a organização ter sofrido algum incidente. Ou seja, as práticas de redução de risco, assim como o compartilhamento de informações e as ações de conscientização interna relatadas, estiveram diretamente associadas à ocorrência de incidentes de segurança concretos e não a uma gestão prévia de risco. Inclusive, mesmo quando foram mencionadas atividades desenvolvidas pelas empresas em termos de avaliação de risco digital, indicaram que acontecem habitualmente em assembleias gerais e não de forma regular.

Esse trabalho reativo vai de encontro à natureza dinâmica do risco, o qual deve ser avaliado e tratado de forma contínua, como parte de um ciclo de gestão de risco permanente, para garantir que os riscos existentes sejam gerenciados de maneira adequada e quaisquer novos riscos identificados e mitigados com sucesso. Os riscos digitais exigem que as empresas sejam proativas no desenvolvimento de recursos de segurança digital: se uma organização tiver fortes proteções e protocolos de segurança digital antes de uma violação, poderá se recuperar mais

rapidamente e incorrer em menos custos com ataques digitais (Jalali, 2018). Da mesma forma, políticas claras de segurança digital precisam ser definidas e revisadas regularmente para garantir que os riscos sejam tratados e as ameaças minimizadas (Worthy, 2017).

> "Isso é conforme acompanha o mercado. Vamos supor, você sabe que está tendo um ataque cibernético e aí você meio que acompanha, vai, três em três meses. Porque tem ataque cibernético você não sabe quando acontece. [...]. É por demanda. [...] o ataque cibernético, geralmente, acontece de sexta a domingo. São períodos que não tem uma pessoa física ali analisando. Então, teoricamente são os dias que você fica mais atento pode acontecer."
>
> (COORDENADOR DE TI E INFRAESTRUTURA, EMPRESA DE PORTE MÉDIO)

A citação anterior também reflete a baixa maturidade das empresas – verificada nas entrevistas – em termos da existência de políticas estruturadas de GRSD. Nesse sentido, constatou-se que apenas as duas maiores empresas entrevistadas, ambas multinacionais, contam com uma política formal por escrito que pode ser considerada GRSD.

Vale ressaltar que, apesar de vários respondentes terem afirmado existir uma política de gestão de riscos em suas organizações, ao explicarem sobre o que tratava, citaram atas de reuniões e, principalmente, "manuais", orientações de comportamento e/ou códigos de ética para os próprios funcionários (com detalhes sobre o monitoramento em relação aos acessos à rede, o uso de *e-mail* pessoal, o uso de *pendrive* e o acesso aos contatos da própria empresa). Algumas empresas mencionaram, ainda, a divulgação de um guia prático sobre o uso de dispositivos eletrônicos por funcionários da organização. A assimilação da política sobre GRSD com as regras de comportamento interno – inclusive considerada como "coisa de RH" –, é um reflexo do entendimento que os respondentes têm sobre o que constitui um risco de segurança digital, o qual, em muitos casos, é concebido como um risco interno, sujeito a ações indevidas dos próprios funcionários que prejudicam a empresa.

Destaca-se o fato de alguns respondentes considerarem ter meios informais de disseminar as melhores práticas, refletindo que a GRSD segue as regras gerais de comportamento da organização: nesses casos, trata-se de um conjunto de práticas recomendadas e não uma política formal da empresa. Mesmo quando o objetivo das "melhores práticas" é orientar o comportamen-

to dos funcionários para evitar incidentes digitais – entendido como a política de GRSD da empresa –, os entrevistados consideram a política algo abrangente para toda a organização e não apenas seu ambiente digital. Ou seja, a política é entendida como um conjunto de procedimentos para cobrir todas as situações da empresa, desde o relacionamento entre os funcionários até a forma correta de usar a Internet, como garantir a proteção de dados e como reportar e tratar incidentes de segurança. Essa política geral inclui não apenas a GRSD, mas também outros aspectos importantes para o bom funcionamento da organização.

"Isso está escrito no manual, em uma folha exclusiva da política de segurança."
"*Isso é a política de segurança digital? [...] O que ela traz?*"
"O que é permitido nos acessos, o que é permitido em relação ao uso dos recursos, as impressões de não fazer trabalhos em horário de trabalho, exatamente como se fosse um manual de comportamento de uso de TI com os mesmos itens que a gente criou nessa base [...] só que lá eles estão descritos de forma aberta que não pode. A gente descreveu os principais assuntos: estão contidos os acessos à Internet, a utilização dos recursos, não fornecer suas senhas pra ninguém, não copiar conteúdo da empresa, que todos os conteúdos de trabalho estejam nas pastas do departamento."

(GERENTE DE TECNOLOGIA E ADMINISTRATIVO, EMPRESA DE PORTE MÉDIO)

Alguns respondentes justificaram a falta de política disponível devido ao porte da empresa, ou seja, não é necessária por não existirem problemas relacionados à segurança digital em organizações de pequeno porte. Outros justificaram a ausência pela natureza dinâmica dos riscos digitais, o que tornaria necessário realizar mudanças em suas políticas conforme o surgimento de novas questões.

As duas empresas que demonstravam maior maturidade em termos de gestão de riscos de segurança digital foram as de maior porte e de caráter multinacional, conforme mencionado. Logo, é relevante destacar que a política de GRSD disponível em ambos os casos é uma política "importada" que passou por um processo de adaptação ao contexto brasileiro.

"Sim, você tem coisas simples como senha de acesso, você não pode deixar em uma gaveta. Tem treinamentos internos que a gente faz para lembrar o óbvio. [...] Vem de fora, é uma empresa Alemã, então, lógico, existe uma certa adequação. [...] tem inclusive um treinamento muito forte especificamente para todos os funcionários e é mandatório, chamado [nome de programa de treinamento]. [...] Você tem uma customização local sempre, mas não pode fugir muito do que vem de fora. [...] Toda a política está acessível aqui na nossa pasta pública."

(DIRETOR DE RISCOS, EMPRESA DE GRANDE PORTE)

Nível aceitável de risco digital e consequências dos incidentes

Os dados coletados nas entrevistas com as empresas mostram que na ausência de processos estruturados sobre o tema, quem define o quanto de risco é tolerável são os próprios gestores de TI, gestores de projetos e/ou gerentes de segurança da informação, ou seja, esta é uma decisão técnica e não necessariamente estratégica – com exceção das duas empresas de maior porte e multinacionais, em que o responsável por estabelecer o "apetite de risco" da empresa é o presidente ou diretor.

Ainda que os especialistas técnicos entendam as possíveis ameaças, vulnerabilidades, incidentes e opções de redução de risco digital, os gestores das empresas estão mais bem posicionados para estabelecerem o "apetite de risco" da organização, avaliarem as possíveis consequências do risco segundo os objetivos econômicos e sociais e assegurarem que medidas de segurança não prejudiquem essas atividades nem reduzam o potencial das TIC para inovar e contribuir para a competitividade. Portanto, idealmente, ambos devem trabalhar juntos, ao passo que as decisões e a responsabilidade de gestão de riscos precisam, em última instância, ser assumidas pelos tomadores de decisão da empresa e não delegadas a especialistas técnicos (OECD, 2015; Jalali, 2018). Aqui vale fazer uma consideração: nas entrevistas, evidenciou-se que o nível aceitável de risco não é um conceito facilmente compreendido pelos respondentes e parece não haver um processo consciente sobre o quanto se deve arriscar.

Nas empresas entrevistadas, não havia uma instância de avaliação para estabelecer o nível aceitável de risco, o qual poderia ser determinado a partir de processos estruturados de avaliação de risco. A ausência dessas instâncias reflete a precariedade de governança de risco de segurança digital, dado que a avaliação dos riscos, como um processo contínuo, deve estabelecer quanto se aceita e quanto se reduz e se transfere – discussão ausente nas práticas das empresas brasileiras entrevistadas. O processo de avaliação de riscos é importante porque, por meio dele, se ponderam as potenciais consequências das ameaças, combinadas com as vulnerabilidades nas atividades econômicas e sociais em jogo, e se informa também o processo de tomada de decisão para o tratamento do risco (OECD, 2015). Ou seja, a decisão sobre o tratamento do

risco deve reduzir o risco a um nível aceitável em relação aos benefícios econômicos e sociais – isto é, inovar e capitalizar o uso das tecnologias nos negócios.

Por mais que não haja processos estruturados para lidar com o tratamento de risco, quando indagados sobre o tema, muitos dos respondentes indicaram que o nível de risco de segurança digital é aceitável caso não comprometa o funcionamento dos negócios. Nesse sentido, a paralisação total ou parcial da empresa, seja por horas ou dias, é uma das principais consequências que respondentes de pequenas e grandes empresas relataram e a que define, também, o quanto de risco aceitar.

"Ficar com sistema parado [...]. Está perdendo negócio, está perdendo faturamento, estou deixando de enviar alguma coisa para o governo que pode gerar uma multa. Todas consequências do risco digital."

(DIRETOR DE TI, EMPRESA DE GRANDE PORTE)

Cabe aos gestores decidirem o quanto de risco aceitar e considerarem as possíveis consequências de eventuais incidentes de segurança digital. Na prática, essas questões são delegadas, propositalmente ou por omissão, à área de TI, possivelmente, de acordo com Jalali (2018), porque as lideranças não observam a complexidade e a importância da segurança digital. Segundo o autor, é difícil que gerentes e/ou lideranças invistam tempo e recursos a fim de defender ou recuperar algo que, aos olhos deles, parece improvável de sofrer um ataque, avaliação geralmente baseada em características perceptivas. Nesse sentido, um tomador de decisão racional investe em segurança da informação se o investimento render um retorno positivo ou se o custo do investimento for menor do que o risco que ele elimina. As dificuldades em medir os custos – e compreender aqueles indiretos – de potenciais incidentes digitais, bem como os benefícios desses investimentos, obscurecem a visão do tomador de decisão: além de haver um alto nível de complexidade, pois muitas vezes envolvem fatores intangíveis, como confiança e boa vontade, também há uma falta de dados históricos[25], métricas eficazes

25 É necessário salientar o importante papel desempenhado pelos Grupos de Resposta a Incidentes de Segurança (CSIRTs), como o CERT.br. Entretanto, como apresentado na página 158, o compartilhamento de informações sobre incidentes de segurança digital não é uma prática verificada nas empresas entrevistadas, já que que apenas uma pessoa entrevistada mencionou conhecer o CERT.br.

relacionadas a ataques digitais e conhecimento sobre o tipo e o leque de incertezas envolvidas (Jalali, 2018; Richmond, 2013).

De modo semelhante à dificuldade de compreensão do nível aceitável de risco por parte dos respondentes, os entrevistados tiveram dificuldade em reconhecer as potenciais consequências que a empresa poderia sofrer em decorrência de incidentes digitais. Mesmo nos casos em que foi mencionado o acesso a informações sigilosas dos clientes, e inclusive seu vazamento, as potenciais consequências desse risco foram associadas às perdas econômicas para a empresa – decorrente do aproveitamento por parte da concorrência ou dos próprios funcionários –, não havendo menção às implicações mais duradouras em termos da violação da privacidade dessas informações de terceiros ou da reputação da empresa.

Práticas de redução e transferência de risco digital

Embora a maioria das empresas entrevistadas não tenha ciclos de gestão de risco contínuos e sistemáticos nem processos para determinar a exposição e o apetite de risco da empresa, do qual resultem decisões sobre as medidas de redução de risco a serem implementadas (OECD, 2019a), é possível identificar práticas isoladas de redução de risco que, muitas vezes, dependem de iniciativas individuais dos responsáveis pela área de TI.

"Olha, eu só fiz isso depois de ter sido roubado viu?
É? Tá. Tem alguma frequência definida, é por evento?
(Risos) não deveria ser, mas eu considero que agora eu tô mais preocupado em estar fazendo a manutenção pelo menos dos computadores com mais frequência pelo menos a cada dois meses.
E isso é o que, ver se tá funcionando, se o antivírus tá funcionando?
Se o antivírus, se tem histórico, se tem quarentena, se tem, enfim, alguns programinhas que eles fazem uma varredura."

(PROPRIETÁRIO, EMPRESA DE PEQUENO PORTE)

Ter *backup* é a principal prática citada pelos respondentes, tanto de PME quanto de grandes empresas. De forma semelhante, a atualização de antivírus e de servidores é considerada uma medida fundamental para se proteger dos riscos digitais. Também há menção ao cuidado a ser tomado com as senhas e o acesso a *sites*, que passam a fazer parte das regras de comportamento disseminadas – geralmente em instâncias informais – entre os funcionários da organização, principalmente de nível operativo e técnico.

É interessante retomar aqui o próprio conceito de vulnerabilidade, que diz respeito às fraquezas exploradas por um ator e compreendem, por exemplo, erros (*bugs*) em *hardware, software* ou redes; falta de treinamento; proteção insuficiente, seja ela digital (*firewalls*) ou física (câmaras e fechaduras no *data center*); assim como procedimentos inapropriados (processos de *backup* ou planos de recuperação de desastres). Todavia, evidências apontam que a maioria das violações de segurança digital é resultado de vulnerabilidades humanas[26], mais do que falhas de tecnologia ou processos, tais como *phishing*, *ransomware* e outros *malwares*, comprometimento de *e-mail* comercial (Business Email Compromise – BEC) e fraude de transferência eletrônica (EIU, 2019). Assim, apesar de as práticas relatadas serem de extrema importância para reduzir o risco de sofrer ataques, nota-se que a desconexão dessas práticas de uma política e/ou processo estabelecido se reflete, por exemplo, na falta de instâncias formais de qualificação dos funcionários que incluam a todos os membros da organização.

A propósito, a maioria das empresas, tanto pequenas quanto grandes, deu ênfase às medidas e às precauções tomadas para controlar o comportamento dos funcionários, mas não tanto por potenciais erros humanos e sim por atos mal-intencionados. Essa preocupação é refletida na "*proibição de uso de pendrives para controlar a informação que entra e que sai",* de acordo tanto com o coordenador de TI de uma empresa de porte médio quanto com o supervisor de TI de uma grande empresa.

Essa situação cria um paradoxo: ainda que as principais medidas de redução de risco implementadas visem mitigar vulnerabilidades humanas, a conscientização e a qualificação sobre segurança digital dos membros da empresa são limitadas e não estão incorporadas à rotina da organização. Nesse sentido, embora as empresas possam introduzir melhores medidas de segurança, como autenticação de dois fatores – à qual nenhum respondente fez menção –, restrições à navegação na Web e *e-mail* pessoal

26 Um estudo realizado pelo The Economist Intelligence Unit (2019) encontrou que, embora as configurações incorretas do sistema e as exposições acidentais sejam a segunda vulnerabilidade mais citada, além de vulnerabilidades humanas, são todas motivadas por erro humano: dispositivos perdidos, roubados ou *hackeados*; vulnerabilidades de *software* não corrigidas; atividade em uma rede ou local não seguro, como aeroporto ou cafeteria; e nomes de usuário e/ou senhas perdidos ou roubados.

etc., elas devem, em última instância, depender das pessoas para seguir as práticas recomendadas e compartilhar informações sobre incidentes, o que pode ajudar com que eles antecipem e previnam eventos semelhantes (EIU, 2019).

Dada a interconexão dos processos entre as mais diversas organizações proporcionar que nenhuma esteja isolada de incidentes que possam acontecer com as demais, o hábito de compartilhar informação sobre ameaças, vulnerabilidades, incidentes e práticas de gestão de risco ou medidas de segurança é importante para se operacionalizar a cooperação entre as partes interessadas (OECD, 2019a) e se atingir um ecossistema saudável. Contudo, essa prática não é realizada de forma sistemática por nenhuma das empresas entrevistadas; há, inclusive, uma reação de surpresa ou desconfiança, por parte dos/as respondentes, os quais questionam por que isso seria benéfico para a própria empresa. Um respondente até argumentou que, ao não se tratar de uma empresa pública nem possuir capital aberto, não existiria a obrigação de compartilhar informações sobre eventuais incidentes ou problemas de segurança.

"[...] a gente não tem obrigação de divulgar, a gente não está na Bovespa [...]. Entendo que pode impactar negativamente a empresa se eu falar que houve uma falha, um *ransomware*, qualquer coisa. [...] No terceirizado, ele tem um contrato que ele tem que ter o sigilo das informações aqui."

(SUPERVISOR DE TI, EMPRESA DE GRANDE PORTE)

Nos casos em que os respondentes afirmaram compartilhar com terceiros informação sobre riscos digitais, trata-se de compartilhamento com parceiros de negócios. Nesse sentido, o compartilhamento de informações é voltado para a resolução de um problema com um parceiro ou um cliente com o qual é necessário interagir, ou seja, está diretamente associado à ocorrência de incidentes de segurança concretos e não a uma gestão de riscos.

"[...] o cliente franqueado, eu tive que falar pra eles tomarem as medidas básicas de segurança pra eles não serem atacados [...]. E com os fornecedores de TI, sim, porque eu precisava deles, né? Então eles que me passaram, então fiz todas as medidas baseadas no que eles me falaram e com os parceiros de negócio também, no caso com o meu parceiro do sistema que eu tenho com o *data center* e com a rede. Eu tive que falar pra ele ver se ele estava fazendo tudo certinho e o outro eu descobri que não estava porque ele foi atacado."

(GERENTE DE PROJETOS, EMPRESA DE PEQUENO PORTE)

Já no que diz respeito à transferência de riscos, considerando a ausência de processos para avaliar o quanto de risco será aceito com relação às potenciais consequências e o quanto será reduzido, verifica-se que há um desconhecimento generalizado sobre seu significado. Existe, inclusive, uma visão sobre a impossibilidade de transferir riscos, pois, mesmo terceirizando um serviço, sempre se correria certo risco.

> "Eu não consigo transferir esse risco digital, eu tenho que, eu tenho que lidar com ele, tratar da melhor forma. Mesmo que eu contrate um parceiro, o risco ainda é todo meu. [...] mesmo que eu transfira, qualquer invasão, qualquer perda de dado ainda é meu. Mesmo que tenha um parceiro na frente, o máximo ele vai me devolver uma multa contratual. Só seguro, você tem um seguro, você vai transferir o seu risco para um terceiro."
>
> (DIRETOR DE TI, EMPRESA DE GRANDE PORTE)

Ter *backup* na nuvem ou com outra empresa, segundo os respondentes, seria um modo de transferência de riscos, considerado uma *"forma com o qual se garante de ter os dados armazenados num local seguro"*, como *"uma garantia que está num terceiro, que lhe garante que vai armazenar estes dados"*. Por outro lado, para uma empresa de grande porte, *"fazer tudo internamente"* e não *"contar com terceiros"* são situações tidas como um diferencial positivo da organização. Neste sentido, vale salientar que a lógica que rege a transferência de risco, como uma das quatro opções de tratamento do risco, é transferir os efeitos indesejados da incerteza sobre os objetivos da atividade para outra pessoa, por exemplo, por contrato, como por meio de seguro (OECD, 2015).

Diante de uma GRSD madura, os seguros para riscos digitais podem ser usados para cobrir riscos que a organização não sabe como tratar ou reduzir. Contudo, as PME informaram não conhecer um seguro contra riscos digitais, ou ainda algumas se mostraram incrédulas sobre a possibilidade de existir um seguro que cubra as consequências de incidentes digitais. O respondente de uma empresa de grande porte disse ter considerado a contratação de seguro, porém este é visto com desconfiança por não cobrir a perda de dados, item considerado pela empresa o mais importante – para além da questão financeira. A falta de seguro, em certas ocasiões, é atribuída a seu alto custo, o que demonstra a não priorização da contratação.

"Se você pensar financeiramente, não [é insuficiente a cobertura do seguro], dependendo do seguro que você faz, mas o que você perde não é só dinheiro. Então, tem coisas que o seguro não compensa. [...] o básico é caro, e ele acaba não abrangendo tudo que a gente pede. [...] Então, a gente entrou em contato poucas vezes, e na época a cobertura era só financeira. Eu não tinha, para mim o mais importante são os dados. O financeiro também é, mas os dados, se não tem cobertura, acho ninguém faz esse tipo de cobertura. [...] recuperar os dados."

(DIRETOR DE TI, EMPRESA DE GRANDE PORTE)

Estrutura da empresa e dificuldades para a gestão de risco de segurança digital

Ao considerar a estrutura das empresas entrevistadas, não foram relatados departamentos específicos para a GRSD, principalmente devido ao tamanho da empresa, segundo os respondentes, fator que também justificaria o fato de questões de segurança digital "não se aplicarem" a ela, tornando a GRSD um assunto de organizações maiores.

"Eu sou muito pequeno pra essas coisas, eu mesmo vou lá e no dia que eu não tiver fazendo nada vou e vou olhar os computadores e vou ver como que tá. [...] [esse item] não se aplica pra mim. [...] Eu e o meu pai. [...] É empresa familiar, empresa pequena, e você tem que fazer tudo. [...] dois, três computadores; duas, três pessoas não tem tanto receio assim, a gente não lida com banco de dados, informação sigilosa, a gente não lida com balanços de empresas [...] eu não tenho que me preocupar tanto com isso, por isso eu não estruturei uma que eu não tenho porte pra estruturar uma política de segurança digital."

(PROPRIETÁRIO, EMPRESA DE PEQUENO PORTE)

Soma-se a isso o fato de a maioria das empresas não ter políticas escritas a respeito do tema, especialmente as PME[27]. Quando as práticas relacionadas à GRSD existem, elas são fundidas em processos mais rotinizados e não são reconhecidas como originadas na avaliação de risco, conforme verificado particularmente nas empresas de pequeno porte ou naquelas em que os negócios têm menor dependência tecnológica. Vale trazer novamente à discussão os dados da pesquisa TIC Empresas 2019 (NIC.br, 2019), pois, ainda que haja universalização da Internet entre as empresas brasileiras de todos os portes e setores econômicos, aumento de sua exposição *on-line* e intensificação do comércio eletrônico, chama a atenção que não haja igual crescimento da preocupação com os riscos de segurança digital inerentes.

27 Como apresentado na página 152, na maioria dos casos, as empresas relataram práticas informais, como avisos ou regras gerais sobre comportamento dos funcionários.

Empresas que processam cartões de crédito *on-line* devem ser compatíveis com o PCI-DSS (Padrão de Segurança de Dados da Indústria de Pagamento com Cartão de Crédito)[28], ainda que sejam pequenas, visto que dados do cartão de crédito das pessoas são manuseados, armazenados e/ou transferidos. Isso reflete o papel desempenhado pela legislação para estimular a adoção de medidas de segurança digital nas organizações, conforme demonstrado na citação a seguir, de uma empresa com baixa maturidade em termos de GRSD:

> "(...) é a segunda empresa que mais faz transação de cartão de crédito no Nordeste e a gente é obrigado a ter PCI-DSS, é uma norma de segurança das empresas de cartão de crédito."
>
> (GERENTE DE TI, EMPRESA DE GRANDE PORTE)

É interessante notar que a maioria dos respondentes – gestores ou gerentes de TI ou projetos – considera a GSRD como área importante a ser desenvolvida – ou, pelo menos, certas práticas de redução de risco. Nesse sentido, muitas vezes a GRSD depende do voluntarismo da pessoa encarregada por cuidar da área de TI, ou seja, de uma pessoa que esteja "no lugar certo, no momento certo", conforme apontado anteriormente. Em alguns casos, esse gestor encontra adesão por parte da diretoria, o que torna possível a realização ou o estabelecimento de certos processos ou ações de segurança digital, como refletido no relato do supervisor de TI de uma empresa de grande porte:

> "De 2014 pra cá que a TI começou a ficar grande aqui, ela era uma TI de [setor de alimentação] a que normalmente não tem muita atenção em tecnologia, então de 2014, com a minha vinda, muitas coisas que eu tive de experiência em outras empresas grandes eu trouxe pra cá [...] e também com o meu contato com o vice-presidente de TI como estreitou esse contato, muita coisa de lá começou a ser aplicada aqui. [...] Hoje não é oficial, eu não faço essa medida oficial, registro, é tudo por minha vontade, não tem nada no papel escrito que eu teria que fazer essa análise."
>
> (SUPERVISOR DE TI, EMPRESA DE GRANDE PORTE)

Em outros casos, as decisões tomadas pela diretoria não contemplam a análise ou as solicitações feitas pela área de TI e, dada essa "falta de interesse" ou priorização por parte da liderança, os respondentes muitas vezes precisam fazer um tra-

28 O capítulo 2 desta publicação traz a questão do *compliance* das empresas em relação à segurança digital e apresenta algumas das principais leis sobre o tema.

balho de convencimento sobre a necessidade de realizar certa ação, contratar um serviço ou comprar um produto para fins de segurança digital.

Neste sentido, é importante considerar as dificuldades em medir os custos e benefícios dos investimentos em segurança da informação, os quais obscurecem a visão do tomador de decisão (Jalali, 2018; Richmond, 2013). Muitas empresas ainda não estão cientes dos riscos em que estão incorrendo e a liderança tende a considerar as despesas de segurança digital um custo, em vez de um investimento desejável (PwC, 2019).

A falta de priorização do tema reflete-se também nos recursos destinados a ele: segundo as entrevistas, nota-se que o desenvolvimento da gestão de segurança digital vai até onde o custo é percebido como baixo. Quando começa a se tornar caro na visão dos responsáveis, a decisão é assumir o risco – de forma consciente ou inconsciente.

"[...] TI é tido como um departamento extremamente caro. Então, para mim poder justificar uma nova contratação, para justificar uma solução nova, preciso ter um número [...]. Ó, está vendo? Tiveram tantas ameaças [...]. Se eu não tiver um gráfico que realmente traz uma solução, que eu preciso de uma pessoa melhor, se eu não tiver isso em papel, uma análise feita, eu não consigo."

(COORDENADOR DE TI E INFRAESTRUTURA, EMPRESA DE PORTE MÉDIO)

Para além da questão financeira, percebe-se que a segurança digital não é considerada tema transversal, pois o próprio treinamento, quando existente, é algo necessário apenas para os funcionários técnicos e/ou aqueles da área de TI. Nesse sentido, as empresas precisam conscientizar sua própria força de trabalho sobre o tema e enfatizar a importância do treinamento para toda a equipe (PwC, 2019).

"[...] para os 80 funcionários que utilizam a rede, nós nunca fizemos, mas na área de informática, os 7 funcionários, nós temos sim, sentado, conversamos muito sobre questão de segurança, mesmo porque somos comprados pelo controle, que é o diretor da empresa, pela confidencialidade desses arquivos. São diversos documentos, isso entre a gente, nós fazemos, só que não é repassado pros demais da empresa, justamente porque eles não têm acesso a esses arquivos, somente a área de informática. Então se um arquivo desse vazar, foi alguém da informática que vazou, mas é um erro porque todos devem saber."

(COORDENADOR DE TI, EMPRESA DE PORTE MÉDIO)

O nível precário de capacitação nas empresas não diz respeito apenas à gestão de risco digital, mas também à gestão de risco de modo geral. Verificou-se nas entrevistas que as instâncias de treinamento têm caráter reativo: quando ocorre um incidente, mesmo que sem consequências significativas, acontece uma conversa ou reunião informal em que são abordadas questões de segurança digital.

Reflexo da concepção de risco de segurança digital dos respondentes, o treinamento em GRSD muitas vezes é associado ao manual de comportamento ou código de ética que os funcionários assinam ao ingressarem na empresa – os mesmos que alguns respondentes, também, consideraram como a política de GRSD disponível na empresa. Ou seja, o risco digital é associado a algo que pode decorrer do comportamento dos funcionários, e inclusive o escasso treinamento é direcionado a eles – e não a diretivos e/ou lideranças –, porém se trata de conversas informais e imposição de restrições. De fato, os funcionários precisam entender como sua atividade pode apresentar riscos digitais e as implicações desse comportamento, além de políticas claras de segurança digital serem definidas e revisadas regularmente para garantir que os riscos sejam tratados e as ameaças minimizadas (Worthy, 2017).

"[...] a cada dois meses, nós reunimos a equipe, e faz aí o que nós chamamos de '*brainstorm*', aconteceu isto, e você acaba colocando para eles estarem situados, e as sugestões [...] Exatamente para entender, porque eu cortei o acesso [...] Como nós somos menores, e não é o tamanho que define isto, eu digo que é a gestão participativa. Se todos estão imbuídos com a informação, eu acho que fica muito mais fácil. [...] treinamento para diretores ou gestores [...] não [...] é um erro, porque os diretores também são falíveis."

(GERENTE DE INFRAESTRUTURA, EMPRESA DE PEQUENO PORTE)

O papel das lideranças das empresas no processo de transformação digital é cada vez mais importante nas escolhas de rumos e na definição de metas associadas não apenas ao modelo de negócio na economia digital, mas sobretudo à gestão dos riscos digitais. A qualificação do corpo técnico e gerencial é importante para que as empresas participem de instâncias de discussão sobre os problemas da transformação digital, caracterizado pela abertura para novas ideias, formas de trabalho e colaboração com outros atores. Nesse sentido, há consenso de que é necessário um maior esforço de

capacitação sobre resiliência digital, tanto dentro da força de trabalho quanto no nível estratégico. Uma consciência mais ampla da complexidade da segurança digital e programas de treinamento como modelos de simulação são cada vez mais necessários para que os gerentes se preparem à realidade de lidar com ameaças digitais (Jalali, 2018).

CONSIDERAÇÕES FINAIS

A crescente digitalização da economia acarreta transformações relevantes na vida das empresas e, junto com elas, uma série de desafios a serem enfrentados de forma a usufruir das vantagens trazidas pelos avanços tecnológicos. A segurança digital configura-se uma questão que apresenta um duplo desafio: se, por um lado, ainda é uma área pouco priorizada pelas empresas brasileiras, por outro lado, a escassez de dados sobre o tema contribui para a invisibilidade e a falta de percepção das potenciais consequências que os incidentes de segurança digital podem causar nas empresas, mesmo sendo grandes, médias ou pequenas.

Em relação à baixa disponibilidade de dados, é preciso considerar as diversas dificuldades metodológicas relativas à medição da gestão de riscos de segurança digital apresentada, visto que se trata de um tema emergente, dinâmico – pela própria natureza dos riscos –, e complexo, tornando indispensável o estabelecimento de *frameworks* de medição que orientem a coleta de dados. No entanto, verifica-se também a falta de priorização do tema na agenda de medição, relacionada com a baixa conscientização sobre o tema.

Sobre esse último ponto, os dados coletados nas entrevistas cognitivas realizadas com empresas brasileiras selecionadas mostraram que, na avaliação dos respondentes, à segurança digital não é dada a devida atenção pelas lideranças das empresas, que muitas vezes a consideram uma área custosa, não condizente com a realidade da empresa, ou de pouca importância. Portanto, assuntos relativos à segurança digital – e própria gestão dos riscos – ficam circunscritos à área técnica, não sendo incorporados ao *core business* da empresa.

Disso decorre que, na rotina das empresas entrevistadas, a abordagem dada à segurança digital geralmente é reativa após acontecerem incidentes, em vez de existirem processos

estabelecidos para gerir propriamente os riscos, de modo a avaliá-los e decidir as estratégias de tratamento que melhor se ajustem à empresa, assim como políticas formais e instâncias de conscientização e treinamento de todos os membros da organização.

Considerando a incipiência do tema, ainda pouco conhecido não apenas pelo público geral, mas especialmente pelas próprias empresas entrevistadas, é indispensável continuar coletando dados – quantitativos e qualitativos – para tornar visível não apenas os potenciais ganhos da digitalização da economia, mas também das problemáticas inerentes a ela.

REFERÊNCIAS

Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York, NY: W. W. Norton & Company.

Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerization? *Technological Forecasting and Social Change, 114*(C), 254-280.

Groves, R., Fowler, F., Couper, M., Lepkowski, J., Singer, E., & Tourangeau, R. (2009). *Survey Methodology*. New York, NY: John Wiley and Sons.

Jalali, M. S. (2018). *The Trouble with Cybersecurity Management*. Recuperado de https://sloanreview.mit.edu/article/the-trouble-with-cybersecurity-management/?gclid=CjwKCAjwkJj6BRA-EiwA0ZVPVjF2ECyG4-fODvwkcrXZFTFnd34M9ZiYvubJwNzk1UBbcDEbehuZVBoCQl4QAvD_BwE

March, J. (1994). *A primer on decision making: how decisions happen.* New York, NY: The Free Press.

March, J. (2010). *The ambiguities of experience*. Ithaca, NY; London, UK: Cornell University Press.

March, J., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science, 33*(11), 1404-1418.

Núcleo de Informação e Coordenação do Ponto BR (NIC.br). (2019). *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nas Empresas Brasileiras - TIC Empresas 2019*. Recuperado de https://cetic.br/pt/pesquisa/empresas/indicadores/

Organisation for Economic Co-operation and Development (OECD). (2015). *Digital Security Risk Management for Economic and Social Prosperity*. Recuperado de https://www.oecd-ilibrary.org/docserver/9789264245471-en.pdf?expires=1598901438&id=id&accname=guest&checksum=50D91465F99DCCD1665A917270B5C2EF

Organisation for Economic Co-operation and Development (OECD). (2017, 20 de outubro). Proposed draft indicators on digital security risk management practices in businesses. *Working Party on Security and Privacy in the Digital Economy* (for Official Use). Paris, FR: DSTI/CDEP/SPDE.

Organisation for Economic Co-operation and Development (OECD). (2019a). Measuring Digital Security Risk Management Practices in Businesses. *OECD Digital Economy Papers, 283*, Paris, FR: OECD. Recuperado de https://www.oecd-ilibrary.org/science--and-technology/measuring-digital-security-risk-management-practices-in-businesses_7b93c1f1-en

Organisation for Economic Co-operation and Development (OECD). (2019b). *Measuring the Digital Transformation: A roadmap for the future*. Recuperado de https://www.oecd.org/publications/measuring--the-digital-transformation--9789264311992-en.htm

Perrow, C. (1999). *Normal accidents: living with high risk technologies*. Princeton, NJ: Princeton University Press.

Pisano, G. (2017). Toward a prescriptive theory of dynamic capabilities: Connecting strategic choice, learning and competition. *Industrial and Corporate Change, 26*(5), 747-762.

PricewaterhouseCoopers (PwC). (2019). *Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber*. Recuperado de https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and--Impact.pdf

Richmond, R. (2013). *Measuring the soft costs of cybercrime: a hard problem in need of a solution*. Recuperado de https://perspectives.eiu.com/technology-innovation/measuring-cost-cybercrime/article/measuring-soft-costs-cybercrime-hard-problem--need-solution

Schwab, K. (2016). *The Fourth Industrial Revolution: what it means, how to respond*. Recuperado de https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Srnicek, N. (2016). *Platform capitalism*. New York City, NY: Polity Books.

Stuart, A. (2016). *The rise and rise of ransomware*. Recuperado de https://eiuperspectives.economist.com/technology-innovation/rise-and-rise-ransomware

The Economist Intelligence Unit (EIU). (2018). Decode resiliency. *How boards can lead the cyber-resilient organisation*. Recuperado de https://eiuperspectives.economist.com/technology-innovation/how-boards-can-lead-cyber-resilient-organisation

The Economist Intelligence Unit (EIU). (2019). *Cyber insecurity: Managing threats from within*. Recuperado de https://eiuperspectives.economist.com/technology-innovation/cyber-insecurity-managing-threats-within

United Nations Conference on Trade and Development (UNCTAD). (2019). *Value creation and capture: implications for developing countries digital economy report 2019*. Recuperado de https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

Worthy, B. (2017). *What will it take for cyber safety to be recognised in the workplace?* Recuperado de https://perspectives.eiu.com/technology-innovation/what-will-it-take-cyber-safety-be-recognised-workplace

CONCLUSÕES

Contexto regional da segurança cibernética

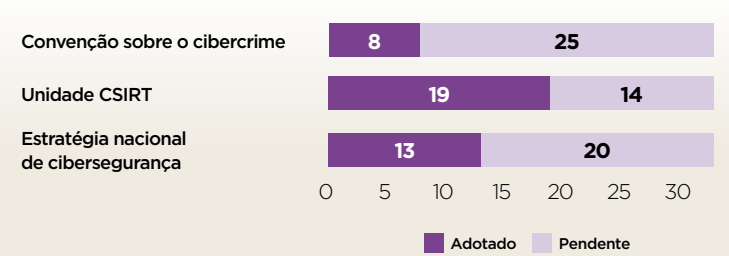
Jorge Alejandro Patiño[1] e Georgina Núñez[2]

1 Jorge Alejandro Patiño é especialista no setor de TIC da Comissão Econômica para a América Latina e o Caribe (CEPAL), com mais de 15 anos de experiência na área. É co-autor de várias publicações sobre tecnologias digitais. Foi Diretor Executivo da Agencia para el Desarrollo de la Sociedad de la Información da Bolívia, administradora de domínios de topo de código do país (ccTLD). É formado em Economia pelo Instituto Tecnológico y Estudios Superiores de Monterrey (ITESM) e tem mestrado em Economia e Regulação de Serviços Públicos pela Universidad de Barcelona.

2 Georgina Núñez é Assessora Regional vinculada à Divisão de Desenvolvimento Produtivo e Empresarial da CEPAL desde 2004, doutora em Economia pela Universidad Nacional Autónoma de México, e mestre em Economia e Política Internacional pelo Centro de Investigación y Docencia Económicas, A.C. (México). Trabalha com questões de governança corporativa, emissão de dívida corporativa, políticas de concorrência, proteção de dados e cibersegurança; e é autora e coautora de diversas publicações sobre esses temas.

Nos últimos anos, alguns governos da América Latina e do Caribe melhoraram o planejamento de seus marcos legais e suas políticas em matéria de cibersegurança: em 2015, enquanto apenas seis dos trinta e três países da América Latina e do Caribe tinham alguma estratégia de cibersegurança, hoje esse número subiu para treze (Lehuedé, 2020). A quantidade de países signatários da Convenção de Budapeste sobre Criminalidade Cibernética, elaborada pelo Conselho da Europa em 2004, aumentou de dois para oito. Além disso, há uma Grupo de Resposta a Incidentes de Segurança (Computer Security Incident Response Team – CSIRT) em dezenove desses países (Lehuedé, 2020). Não obstante, como é enfatizado por diversos indicadores e relatórios, ainda existe uma diversidade de âmbitos que requerem atenção por parte dos governos, os quais incluem a adoção não só de novos marcos legais e sua atualização, mas também de aspectos relacionados com sua capacidade técnica e de organização, além do desenvolvimento das equipes encarregadas de implementar as estratégias de cibersegurança. Segundo o Índice Global de Cibersegurança (Global Cybersecurity Index – GCI) da União Internacional de Telecomunicações (UIT), a América Latina e o Caribe, de forma agregada, aparecem como a região do mundo com menor grau de compromisso com a segurança digital, somente à frente da África (ITU, 2019).

GRÁFICO 1 – CARACTERÍSTICAS DO MARCO DE CIBERSEGURANÇA 2020, AMÉRICA LATINA E CARIBE (33 PAÍSES)



FONTE: ADAPTADO DE LEHUEDÉ (2020).

Analisando outras métricas, o Índice Nacional de Segurança Cibernética[3] (National Cyber Security Index – NCSI), desenvolvido pela Fundação da Academia de Governança Eletrônica da Estônia, que recopila diversos indicadores, sugere que existe um número significativo de jurisdições na região que adotou marcos de proteção de dados e que tem tido um desenvolvimento significativo nesse âmbito. Entretanto, quando são avaliados âmbitos em matéria de segurança cibernética como requisitos gerais para os operadores de serviços essenciais ou o monitoramento regular de medidas de cibersegurança, os resultados para a região são deficientes. Com algumas pequenas exceções, não existem requisitos significativos de segurança cibernética dirigidos a empresas além daqueles impulsionados pela proteção de dados (Tabela 1). Embora a região tenha avançado na abordagem da cibersegurança, ainda existem atrasos na regulação de serviços essenciais e de infraestrutura crítica.

TABELA 1 – REGRAS-CHAVE DE SEGURANÇA CIBERNÉTICA RELACIONADAS À PROTEÇÃO DE DADOS (JURISDIÇÕES SELECIONADAS)

	AR	BO	BR	CL*	CO	CR	DO	GT*	MX	PA	PY	PE	UY	VE
Autoridade de proteção de dados	✔	X	✔	X	✔	✔	X	X	✔	✔	X	✔	✔	X
Restrição a transferências internacionais para jurisdições	✔	X	✔	X	✔	X	X	X	X	X	X	X	✔	X
Restrição a transferências para processadores de dados	✔	X	✔	✔	✔	X	X	X	✔	X	X	✔	✔	X
Sanções	✔	✔	✔	✔	✔	✔	✔	X	✔	✔	✔	✔	✔	✔
Notificação obrigatória de violações a autoridades e/ ou aos titulares dos dados	X	X	✔	X	A	✔	X	X	✔	✔	X	X	✔	U
DPOs obrigatórios	E	X	✔	X	✔	X	X	X	✔	X	X	E	✔	X
DPIAs obrigatórios	✔	X	✔	X	R	X	X	X	✔	X	X	X	✔	X
Responsabilização	X	X	✔	X	✔	X	X	X	X	X	X	X	✔	X

FONTE: LEHUEDÉ (2020).
NOTAS: (*): ESSAS JURISDIÇÕES TÊM, ATUALMENTE, PROJETOS DE LEI NO CONGRESSO QUE INCLUEM ALGUMAS DESTAS MEDIDAS: E: EXCEPCIONALMENTE; R: RECOMENDADO; A: NOTIFICAÇÃO APENAS À AUTORIDADE; U: NÃO ESTÁ CLARO QUEM DEVE SER NOTIFICADO.

3 O Índice Nacional de Segurança Cibernética é um índice global que mede a preparação dos países para prevenirem ameaças cibernéticas e gerirem os incidentes cibernéticos. O NCSI também é uma base de dados com materiais em evidência disponíveis publicamente e uma ferramenta para o desenvolvimento de capacidades relacionadas à cibersegurança nacional. Para mais informações, acesse: https://ncsi.ega.ee/

Ressalta-se nesses serviços o baixo nível de preparação em matéria de segurança cibernética por parte das empresas. Os dados disponíveis sugerem que, embora o risco cibernético seja claramente uma prioridade na agenda das empresas na América Latina, o progresso nesse âmbito continua sendo insuficiente. Com base em Marsh e Microsoft (2019, citado por Lehuedé, 2020), 16% a 22% das empresas afirmam compreender, avaliar e quantificar as ameaças cibernéticas, 12% a 20% conseguem prevenir os ataques cibernéticos e apenas 7% a 18% gerenciam e se recuperam dos referidos ataques.

A SEGURANÇA DIGITAL NO CONTEXTO DA COOPERAÇÃO INTERNACIONAL: UMA ESTRATÉGIA NACIONAL CONSENSUAL

Houve uma aceleração do processo de digitalização das economias da região nos últimos anos, potencializado pela atual crise sanitária, o que acarretou aumento de ameaças em matéria cibernética e necessidade de contar com uma estratégia nacional de cibersegurança. Apenas no mês de maio, no começo da pandemia da COVID-19, o Google relatou 18 milhões de *malware* e *phishing e-mails,* além de 240 milhões de mensagens *spam*[4]. A consciência e a sensibilização sobre ataques cibernéticos foram aumentando e, como consequência, os riscos associados à reputação das empresas também se converteram em um atrativo muito valorizado globalmente.

Apesar de alguns aspectos-chave da segurança cibernética terem sua importância reconhecida em diversos âmbitos e acordos internacionais, tanto por seu alto valor como pelo dano em potencial, observam-se deficiências ao se revisarem a incorporação e a implementação desses aspectos na política dos países. Alguns exemplos seriam: falta de identificação de peças de infraestrutura (que deveriam ser consideradas críticas), de padrões de cibersegurança, de regras de monitoramento e de prestação de contas. Nesse sentido, existem vários aspectos, a partir do planejamento e da implementação da política de segurança cibernética, que devem ser ajustados.

A abordagem do tema da segurança digital requer necessariamente um diálogo entre os diferentes atores da sociedade,

4 Recuperado de https://diarioti.com/covid-19-google-bloquea-18-millones-de-emails-fraudulentos-diarios/111571

tanto públicos como privados, para garantir uma governança efetiva e um esforço coordenado em nível nacional para a implementação da estratégia de cibersegurança de um país. Do mesmo modo, é fundamental contar com diversos instrumentos para coordenar ações em matéria de cibersegurança a partir do setor privado. Algumas vezes, as empresas que cuidam da infraestrutura crítica estão nas mãos de operadores púbicos, o que poderia facilitar a adoção de medidas de segurança; todavia, em outros âmbitos, são necessários incentivos e regulações que demandem a implementação de ações com delimitações mais definidas.

A cooperação regional também tem um papel importante para avançar na definição de parâmetros comuns e motivar a ação. Desde 2004, a região conta com uma Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética[5], adotada pela Assembleia Geral da Organização dos Estados Americanos (OEA). Por outro lado, a Comissão Econômica para a América Latina e o Caribe (CEPAL) coordena esforços a partir de outros espaços de diálogo político, como a Agenda Digital para América Latina e o Caribe (eLAC 2020)[6], a qual define alguns compromissos em matéria de segurança digital (CEPAL, 2018). Também se iniciou um trabalho com diferentes grupos da região para a construção de um diálogo público-privado e o planejamento de uma estratégia nacional, caso da relação com os 8 países-membros[7] da Comissão Técnica Regional de Telecomunicações (COMTELCA).

A partir do trabalho da CEPAL, foram identificadas quatro mensagens-chave relacionadas à segurança digital: *(i)* a importância de um esforço coordenado em nível nacional, em

5 A Estratégia Interamericana Integral de Segurança Cibernética baseia-se em esforços e conhecimentos especializados do Comitê Interamericano contra o Terrorismo (CICTE), da Comissão Interamericana de Telecomunicações (CITEL) e da Reunião de Ministros da Justiça ou Ministros ou Procuradores-Gerais das Américas (REMJA). A Estratégia reconhece a necessidade de que todos os participantes de redes e sistemas de informação sejam conscientes de suas funções e responsabilidades com relação à segurança, a fim de criarem uma cultura de segurança cibernética. Mais informações em: http://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp

6 A eLAC é uma estratégia visando 2020, que sugere o uso de tecnologias digitais como instrumentos de desenvolvimento sustentável. Tem como missão promover o desenvolvimento do ecossistema digital na América Latina e no Caribe mediante um processo de integração e cooperação regional, com o objetivo de fortalecer as políticas digitais que impulsionem o conhecimento, a inclusão e a equidade, a inovação e a sustentabilidade ambiental. Mais informações em: https://www.cepal.org/es/proyectos/elac2020

7 Os membros designados são México, Guatemala, El Salvador, Honduras, Nicarágua, Costa Rica, Panamá e República Dominicana.

momentos de crescente digitalização das economias e aumento das ameaças de ataques aos sistemas nacionais de informação; (*ii)* a necessidade de considerar marcos normativos e institucionais acordes, além de uma política pública com delimitações claras sobre a proteção de dados pessoais, no caso de governos e empresas, que acompanhe a estratégia para enfrentar os desafios; (*iii)* a cooperação e o esforço multilateral, fundamentais para enfrentar as ameaças cibernéticas; e, finalmente, (*iv)* a construção de uma estratégia de segurança digital ampla e efetiva, produto de parcerias público-privadas.

Uma estratégia de segurança cibernética que contemple uma governança efetiva requer um marco normativo e mecanismos de resposta efetivos, além de desenvolvimento e proteção de infraestrutura e de sistemas críticos. Requer também uma articulação com a cooperação internacional para formar um marco multilateral, assim como a gestão de talentos e tecnologia para enfrentar os desafios. Dessa forma, é necessário o planejamento de uma agenda holística que inclua as diferentes dimensões que conformam uma estratégia de segurança digital e de segurança de dados.

A ameaça de ataques afeta setores-chave, tais como: serviços públicos e governamentais, alimentos, combustível, transporte, comunicações e finanças, o que pode implicar riscos importantes para a sociedade em seu conjunto, impactar os fundos do tesouro público e atentar contra a rede elétrica, as telecomunicações e o fornecimento de bens e serviços essenciais. Esses temas são importantíssimos para a defesa da segurança nacional, da economia, da saúde, da ordem pública e da política.

Observa-se um aumento gradativo tanto da complexidade como dos custos relacionados aos ataques cibernéticos a pessoas, governos, empresas e sistemas de informação em geral, que se referem ao tratamento dos programas maliciosos e nocivos (ex. *malware, spyware, data breaches* e *ransomware*), a roubos de dados especialmente sensíveis, à manipulação de dados, ao ataque ao funcionamento de sistemas informáticos (incluídos aqueles que controlam infraestruturas críticas) e a programas de extorsão e espionagem cibernética[8].

8 Segundo o Fórum Econômico Mundial (Morgan, 2020), estima-se que, para 2021, o impacto econômico dos incidentes de cibersegurança poderia alcançar 6 trilhões de dólares globalmente. O recente ataque (*ransomware*) ao Banco Estado do Chile representou um gasto de quase 9 milhões de dólares para recuperar o controle de suas plataformas e dados.

A capacidade de resposta dos países aos ataques cibernéticos é cada vez mais necessária, em virtude de depender, em grande parte, do tamanho, da diversidade e do dinamismo das estruturas econômico-sociais dos países. É preciso responder a esses ataques e mitigar seus impactos, especialmente sobre as instituições, já que elas diminuem a governança perante a exposição a diferentes tipos de riscos:

- Ataques a diferentes níveis de governo (nacional, federal, regional, estadual, municipal) com consequências econômicas, em áreas como: receitas de múltiplos fluxos (de contribuintes), em múltiplas formas (imposto de renda, IVA etc.) e o nível de diversificação econômica para atender esses riscos[9].
- Em termos de estrutura "política", um ataque pode ser dirigido ao uso de dados pessoais para fins políticos obtidos de maneira ilícita, e ao uso das redes sociais para influenciar eleitores mediante a manipulação de dados, por meio de mensagens ou do uso de plataformas.
- Roubos de identidade e fraudes a órgãos públicos.
- Construção de talento e de tecnologia em segurança digital que acompanhem o planejamento e a implementação de mecanismos de resposta efetivos.

A dimensão internacional e a necessidade de gerar um acordo multilateral também é fundamental, especialmente no fluxo transfronteiriço de dados no que se refere à sua proteção, à garantia da privacidade e ao consentimento dos proprietários dos dados. Com relação a essa dimensão, é importante mencionar o papel do marco dado pela Convenção de Budapeste[10], que define em seu Artículo 32.b:

---

9 Por exemplo, um relatório da PwC (2019) para a Comissão Europeia indica que o roubo relacionado à segurança digital dos segredos comerciais na Europa em 2018 significou perdas de 60 bilhões de euros para o crescimento econômico e quase 289 mil postos de trabalho. As estimativas que este mesmo relatório faz para 2025 indicam um impacto de um milhão de postos de trabalho perdidos.

10 A Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste, é um tratado internacional de direito penal e direito processual penal firmado no âmbito do Conselho da Europa para definir, de maneira harmônica, os crimes praticados por meio da Internet e a forma como combatê-los. Recuperado de https://rm.coe.int/16802fa428

O acesso a dados transfronteiriços. É uma exceção ao princípio de territorialidade que permite o acesso transfronteiriço unilateral sem necessidade de assistência mútua em situações limitadas, circunscrita a: *(i)* acessibilidade do público a dados (fonte aberta) e (*ii)* quando os dados foram acessados ou recebidos de fora do território, através de um sistema informático de seu território, com o consentimento legal e voluntário da pessoa com autoridade legal para revelar os dados através desse sistema.

Um tema de crescente relevância a ser considerado no planejamento de uma estratégia nacional de segurança cibernética é o chamado monopólio de dados (*data-opolies*), que se converteu em uma das principais ameaças à segurança digital. É necessária uma coordenação entre diferentes instâncias de governo, associada a um limite do poder dos monopólios de dados, em toda a economia. Isso inclui limitar a concentração não apenas das grandes empresas tecnológicas, proprietárias das plataformas digitais, mas também de outras empresas não tecnológicas cujo valor aumenta substancialmente devido ao crescente acesso a dados. Os efeitos da rede, a falta de portabilidade dos dados, os direitos do usuário sobre seus dados e a frágil proteção da privacidade ajudam esses monopólios a manter uma posição dominante (Stucke, 2018). A maior concentração de dados converte-se, portanto, em um importante incentivo para os ataques cibernéticos massivos. Dessa forma, é imprescindível uma forte coordenação entre os encarregados do cumprimento das leis antimonopólio e os de proteção à privacidade do consumidor para aumentar as garantias de condições de uma competência efetiva, sem afetar a inovação.

CONSIDERAÇÕES FINAIS

- Uma estratégia regional em segurança cibernética tem um efeito duplo: conscientização das pessoas sobre o valor de seus dados, a fim de os proteger, e possibilidade de cálculo pelas autoridades, com maior precisão, dos alcances de um ecossistema digital em termos de valor, riscos e rentabilidade.
- Na América Latina, o tema da cibersegurança associa-se fundamentalmente à proteção de dados; logo, o fortaleci-

mento de sua política deve incluir necessariamente a dimensão de segurança cibernética.

- Na discussão atual, o poder dos dados pessoais e seu valor crescente requerem uma maior proteção diante de múltiplos ataques. Este é um tema central nas iniciativas internacionais as quais, entre outras coisas, buscam que o usuário que acessa qualquer plataforma digital possa oferecer e controlar suas informações, as quais devem permanecer devidamente protegidas.
- A colaboração público-privada é fundamental para o sucesso de uma política de segurança efetiva na detecção de riscos associados ao uso e mau uso de dados, para a mitigação dos danos provocados por um ataque à privacidade e para a proteção de dados considerados sensíveis, pessoais, comerciais ou industriais.
- Um esforço multilateral requer amplos marcos legais e institucionais para contemplar formas e graus variados de impactos diante de ataques cibernéticos a empresas, governos e sistemas de informação. Isso deve incluir desde possíveis danos à infraestrutura crítica de um país, até o alcance de programas maliciosos e um marco para o fluxo transfronteiriço de dados.

REFERÊNCIAS

Agenda digital para América Latina y el Caribe (eLAC). (2018, 20 de abril). Declaración de Cartagena de Indias. *Sexta Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe.* Recuperado de https://conferenciaelac.cepal.org/6/sites/elac2020/files/cmsi.6_declaracion_de_cartagena.pdf

International Telecommunications Union (ITU). (2019). *Global Cybersecurity Index 2018*. Recuperado de https://www.itu-ilibrary.org/science-and-technology/global-cybersecurity-index-2018_pub/813559ed-en

Lehuedé, H. (2020). Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean. *Production Development series, 225* (LC/TS.2020/103). Santiago, CL: ECLAC.

Morgan, S. (2020, 13 de novembro). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine.* Sausalito, CA. Recuperado de https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

PricewaterhouseCoopers Advisory SpA (PwC). (2019). *Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber*. Recuperado de https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

Stucke, M. (2018, 27 de março). Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data. *Harvard Business Review*, Boston, MA. Recuperado de https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data?mod=article_inline

Organização das Nações Unidas para a Educação, a Ciência e a Cultura

cetic.br

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação sob os auspícios da UNESCO

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.br

Comitê Gestor da Internet no Brasil

ISBN: 978-65-86949-19-3

CBL

9 786586 949193