IBGC
Orienta

PAPÉIS E RESPONSABILIDADES DO CONSELHO NA GESTÃO DE RISCOS CIBERNÉTICOS

IBGC
Orienta

Papéis e Responsabilidades do Conselho na Gestão de Riscos Cibernéticos

IBGC | Instituto Brasileiro de Governança Corporativa

São Paulo | 2019

IBGC | Instituto Brasileiro de Governança Corporativa

O Instituto Brasileiro de Governança Corporativa (IBGC), organização da sociedade civil, é a principal referência nacional e uma das principais internacionais em governança corporativa. Fundado em 27 de novembro de 1995, contribui para o desenvolvimento sustentável das organizações por meio da geração, educação e disseminação de conhecimento das melhores práticas em governança corporativa, influenciando e representando os mais diversos agentes, visando uma sociedade melhor.

CRÉDITOS

Membros do grupo de trabalho

Esta publicação foi desenvolvida por grupo de trabalho (GT) composto por membros do IBGC e de suas comissões de Conselho de Administração, Gerenciamento de Riscos Corporativos e Jurídica: Camila Cristina da Silva, Eder de Abreu (Deloitte), Eduardo Vieira Mattos, Isis Mara de Oliveira Cerqueira, Júlia Lauria, Luciana Bacci, Renan Perondi, Ricardo Lemos, Talita Lemes e Thomas Brull.

AGRADECIMENTOS

A Célia Assis, Hugo Menezes e Gabriela Paiva Morette pelas valiosas contribuições.

A Edison Fontes, Fernando Ferreira e Nemer Zaguir pela leitura crítica e pelos comentários enviados em audiência restrita.

A Alberto Messano, Alex Silva, Annibal Ribeiro Lima , Atílio Augusto Segantin Braga, Carlos Alberto Ercolin, Carlos Berti Niemeyer, Carlos Donizeti Macedo Maia, Dante Peroco Di Civita, Emerson Siécola, Emilio Angelo Carmignan, Felipe Camiloti, Fernando Brandello, Frank Ned Santa Cruz, Gilmario Ribeiro, José Luís Munhós, Marco Antonio Ferreira Villas Boas, Marcos Semola, Paulo Baraldi, Pedro Coleta, Previ, Roberta Rosenburg e Vladimir Barcellos Bidniuk pelas contribuições ao longo do processo de audiência pública.

À equipe do IBGC, pelo apoio ao grupo de estudos e pelas contribuições.

PRODUÇÃO

Redação: Luciana Del Caro; revisão de provas: Renan Perondi; projeto gráfico, diagramação e capa: Kato Editorial; imagem da capa: Shutterstock.

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

I59p Instituto Brasileiro de Governança Corporativa

Papéis e responsabilidades do conselheiro na gestão de riscos cibernéticos / Instituto Brasileiro de Governança Corporativa. - São Paulo, SP : IBGC Orienta, 2019.

48 p. ; 15cm x 21cm.

Inclui bibliografia, índice e anexo.

ISBN: 978-85-99645-80-2

1. Administração. 2. Conselho de Administração. 3. Riscos cibernéticos. I. Título.

CDD 658.401

2019-1908 CDU 658.011.2

Elaborado por Vagner Rodolfo da Silva - CRB-8/9410

Índice para catálogo sistemático:

1. Conselho de Administração 658.401

2. Conselho de Administração 658.011.2

Sumário

Prefácio

Caro leitor,

Se você é acionista, conselheiro, executivo, investidor, ou se relaciona de alguma maneira com o ambiente empresarial, já sabe que as empresas estão expostas a riscos representados por acessos não autorizados a sistemas, dados e informações estratégicas. É possível, inclusive, que tenha desenvolvido alguma tolerância a alguns destes riscos.

Também sabe que, a qualquer momento, o risco de invasão pode se materializar e culminar em graves consequências: interrupção das atividades da empresa, uso indevido e perda de informações estratégicas, danos reputacionais desastrosos, aumento de custos com litígios, seguros, multas e impactos negativos no relacionamento com *stakeholders* (clientes, acionistas, colaboradores, fornecedores, bancos, reguladores). Em última análise, impactos que podem, de fato, afetar sobremaneira a continuidade do negócio.

Não bastando a complexidade do assunto, investidores, clientes, parceiros de negócios e reguladores estão cada vez mais atentos à forma como as companhias lidam e mitigam os riscos cibernéticos. Logo, a atenção de uma empresa ao tema deve ir muito além da conformidade e do cumprimento das regulações existentes. Deve contemplar uma visão holística e envolver diversos atores em diferentes níveis organizacionais, incluindo o conselho de administração.

O perigo cibernético é um dos mais importantes riscos empresariais do nosso tempo, e é premente que a sua supervisão esteja consolidada na agenda dos conselhos de administração e dos demais responsáveis pela governança corporativa. O papel de supervisão do conselho exige que seus membros compreendam a natureza dos riscos de segurança cibernética e priorizem a sua vigilância.

A supervisão adequada exige que os conselheiros estejam bem informados sobre a eficácia das medidas de segurança cibernética existentes para lidar com quatro aspectos principais: preparação, detecção, resposta e reporte dos incidentes ocorridos e identificados.

O objetivo desta publicação é informar e preparar o conselheiro (e demais agentes de governança) a navegar neste contexto de incertezas e a lidar com os novos riscos que podem impactar diretamente o negócio e as organizações.

Boa leitura!

Henrique Luz
Presidente do conselho de administração – IBGC

Introdução

Suponha que uma organização esteja exposta a um risco relevante, capaz de trazer perdas de reputação, de dados, perdas financeiras decorrentes da interrupção das atividades da empresa, aumento dos custos de seguros e de empréstimos. E, ainda, que a materialização desse risco a deixe exposta a litígios e possa trazer pesadas multas. Agora, pense no papel do conselho de administração dessa empresa – e de todas as outras – no que diz respeito a riscos, que é o de determinar o perfil de riscos da organização, de monitorar o processo de gestão de riscos e os planos de ação que devem ser tomados em resposta a esses potenciais eventos. Seria natural concluir que o conselho dessa organização vem dando a devida atenção ao risco em questão, correto? Mas nem sempre é isso o que acontece. Esse risco a que nos referimos é o risco cibernético, que, embora cada vez mais relevante, frequentemente deixa de receber o merecido cuidado por parte dos conselheiros, executivos e acionistas.

Uma abordagem omissa ou inadequada pode custar caro, dadas as potenciais perdas que expõem a empresa. Em última instância, ela tem potencial para comprometer a sustentabilidade da organização e a confiabilidade da informação sob sua responsabilidade. O risco cibernético vem ganhando importância devido à ampliação do uso da tecnologia digital, sobre a qual se baseia a atuação das empresas e que se tornou indispensável para os negócios atenderem aos objetivos corporativos e para o relacionamento com as partes interessadas. O mundo está cada vez mais conectado. Com as empresas, não é diferente.

A chamada quarta Revolução Industrial – marcada pelo aumento da automação, avanço da internet das coisas, do uso da inteligência artificial, da nanotecnologia e biotecnologia, dentre outras evoluções – já está em curso. A internet das coisas, por exemplo, vem ampliando o

número de dispositivos conectados e, consequentemente, tem aumentado exponencialmente o número de portas de entrada para possíveis ataques cibernéticos. Essa relação crescente com a tecnologia faz com que a ocorrência de algum incidente ou evento cibernético tenha potencial para causar impactos financeiros, operacionais e de reputação, atingindo também o valor da empresa.

Dessa forma, o risco cibernético vem galgando degraus no ranking de riscos mais prováveis a que as empresas estão sujeitas. O roubo e a fraude relacionada a dados ocupou o quarto lugar como o risco mais provável nos próximos dez anos, e os ataques cibernéticos capazes de causar interrupção das operações ou infraestrutura ficaram em quinto lugar em pesquisa realizada pelo Fórum Econômico Mundial 🕮.

🕮 The Global Risks Report 2019 – World Economic Forum. Disponível em: <http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf>.

A ocorrência desses ataques já é uma realidade para todas empresas, inclusive as brasileiras. Quatro em cada dez organizações latino-americanas haviam sofrido um incidente de segurança cibernética de 2016 a 2018 de acordo com uma pesquisa feita com 150 empresas de sete países da América Latina e Caribe 🕮. Nessa mesma enquete, 70% das empresas disseram que não estão certas da eficácia de seus processos para combater incidentes.

🕮 Deloitte. *Riscos Cibernéticos e Segurança da Informação na América Latina e Caribe – Tendências 2019*, mar. 2019.

Considerando que há subnotificação de casos, pode-se inferir que o percentual de empresas afetadas é superior. Os números de outro levantamento ajudam a dar uma dimensão do problema: foram 53 mil incidentes cibernéticos no mundo em 2017, sendo 2,2 mil com violações de dados 🕮.

🕮 Verizon. *Data Breach Investigations Report*, 2018.

Se levarmos em conta que os invasores ✪ demoram minutos para entrar no ambiente de uma empresa e que elas demoram muito para **reconhecer um ataque (de semanas a meses)** ✪, vemos que a dimensão do problema é relevante, uma vez que os dados e sistemas das empresas ficam expostos por longo período. Nem sempre o invasor é uma pessoa externa: ele pode fazer parte do quadro oficial de colaboradores. De acordo com um levantamento 🕮 realizado em 2019, 34% das invasões são efetivadas por atores internos.

✪ Neste documento, usaremos o termo invasores para nos referirmos aos crackers.

✪ De acordo com o levantamento da Verizon, de 2018, em mais de 60% dos casos de violação de dados pesquisados, os invasores demoraram de segundos a minutos para entrar nos sistemas da empresa, e em cerca de 60% dos casos, as empresas demoraram meses para descobrir os ataques.

🕮 Verizon. *Data Breach Investigations Report*, 2019.

Ao mesmo tempo em que esses ataques recrudesceram, as legislações de vários países endureceram e responsabilizaram as empresas pela proteção de dados de pessoas naturais (consumidores, empregados, visitantes, dentro outros) – sujeitando-as a multas e outras penalidades e possivelmente deixando-as mais propensas a enfrentar litígios jurídicos. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) ✪ trata de dados pessoais e estabelece multa que vai até 2% do faturamento anual da companhia, limitada a R$ 50 milhões por infração.

✪ A Lei 13.709 também é chamada de LGPD – Lei Geral de Proteção de Dados Pessoais. Ela foi sancionada em agosto de 2018, modificada pela Lei 13.853/19, e, até a publicação deste documento, estava prevista para entrar em vigor em agosto de 2020.

Nesse cenário, a ocorrência de um incidente cibernético como o vazamento de dados torna-se uma realidade no dia a dia das empresas. É fundamental que os conselheiros e demais agentes de governança não esperem que suas empresas sofram alguma ofensiva para só então agir sobre os pesados

danos em potencial. A preparação para um evento de crise dessa magnitude será determinante para a detecção, reação, monitoramento e mitigação do mesmo.

A conscientização do conselho de administração sobre o tema é importante para que ele contribua por meio do fomento da cultura de segurança cibernética na empresa. Para tanto, os conselheiros precisam entender como os riscos cibernéticos estão evoluindo e afetam as organizações em que atuam, assim como as novas regulamentações impactam os negócios da companhia. A segurança da informação e o risco cibernético devem ser pauta permanente dos órgãos de governança.

Esta publicação visa esclarecer o papel e responsabilidades do conselho de administração e outros agentes de governança em relação ao tema. O primeiro capítulo é dedicado à governança na gestão de riscos cibernéticos e versa sobre o papel de cada agente de governança em busca da resiliência cibernética. Em seguida, trazemos um panorama sobre os ataques cibernéticos na atualidade. No terceiro capítulo, tratamos dos aspectos práticos da gestão de riscos cibernéticos. Esperamos que a publicação contribua para que os conselheiros aprofundem os seus conhecimentos sobre risco cibernético, fortalecendo a resiliência e a sustentabilidade das empresas em que atuam.

1

Governança na gestão de riscos cibernéticos

Embora pareça um assunto técnico e de interesse apenas de profissionais da tecnologia da informação, o risco cibernético deve ser examinado de perto pelos conselheiros de administração. Engana-se quem pensa que esse tipo de risco tem efeitos apenas sobre a parte de tecnologia da empresa: ele tem implicações diretas sobre o negócio, podendo inclusive comprometer sua sustentabilidade.

Cabe ao conselho informar-se e liderar a conscientização e o comprometimento da empresa sobre a importância da segurança cibernética, assim como acompanhar a implantação da cultura e de iniciativas concretas, voltadas para a segurança da informação. Veremos, mais adiante, quais são as principais atribuições dos conselheiros, da liderança e dos demais agentes envolvidos com a gestão da segurança cibernética.

Mas, antes de nos debruçarmos sobre a governança desse tipo de risco, precisamos começar conceituando-o e falar um pouco sobre a gestão do risco cibernético. Há várias definições para esse risco, mas neste documento, utilizaremos a dada pela International Organization of Securities Commissions (IOSCO), que é ampla: "Risco cibernético refere-se aos potenciais resultados negativos associados a ataques cibernéticos. Por sua vez, ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade, disponibilidade de dados ou sistemas computacionais."

Nota-se, por essa definição, que o risco cibernético é vasto e pode incluir dados em qualquer tipo de dispositivo ou serviço, como a computação em nuvem e a internet das coisas. Esse risco está ligado à digitalização dos negócios e à ultra conexão de pessoas e ativos dentro e fora da organização – e daí vem a preocupação com a segurança da informação,

International Organization of Securities Commissions. *Cyber Security in Securities Markets – An International Perspective Report on IOSCO's cyber risk coordination efforts*, 2016.

ou com um conjunto de práticas que visam a confidencialidade, integridade e disponibilidade da informação. Essa preocupação é crescente, dado que o uso das tecnologias digitais também se expande exponencialmente e que novas modalidades de trabalho, como o teletrabalho, podem abrir novas portas e vulnerabilidades para ataques e que também requerem atenção e conscientização.

Um incidente de segurança de informação – como um ataque cibernético bem-sucedido – pode acarretar perdas relevantes para uma empresa. Aqui, vale lembrar de que dados são ativos das empresas e que, como todos ativos, devem ser protegidos. Veja, a seguir, uma lista não exaustiva das consequências de um ataque cibernético:

Potenciais impactos dos ataques cibernéticos:

- perda e/ou exposição de dados estratégicos ou confidenciais;
- perda no valor da empresa;
- perda de receita;
- roubo de propriedade intelectual;
- ameaças à vida ou à segurança;
- danos à reputação;
- perda de clientes;
- interrupção nas operações;
- sujeição a multas e litígios, e;
- geração de custos de diversas naturezas para reparação de danos.

Por dentro dos conceitos:

As normas da família ISO/IEC 27.000 versam sobre o Sistema de Gestão de Segurança da Informação (SGSI), contemplando as normas ISO 27.001, ISO 27.002, ISO 27.032, dentre outras. Elas estão relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico. O conceito de segurança da informação vai além do quesito informático e tecnológico, apesar de andarem bem próximos. O SGSI é uma forma de segurança para todos os tipos de dados e informações, e possui como atributos básicos a confidencialidade, integridade e a disponibilidade. Há ainda outro atributo secundário, a autenticidade, que é garantia da veracidade das fontes das informações.

Confira as definições, dadas pela norma ISO 27.001 ✪, para integridade, confidencialidade e disponibilidade da informação:

"Integridade – propriedade de salvaguarda da exatidão e completeza de ativos;

Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

Disponibilidade – propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada".

✪ As normas da família 27.000 podem ser consultadas em português no catálogo da Associação Brasileira de Normas Técnicas (ABNT): <https://www.abntcatalogo.com.br/norma.aspx?ID=385777>.

O desenho de um Sistema de Gestão da Segurança da Informação (SGSI) robusto e a sua respectiva implementação, por meio da adoção de processos e ações técnicas (controles) que coloquem em prática as políticas estabelecidas, devem ser capazes de proteger os ativos tangíveis e intangíveis de informação das organizações e de mitigar o risco cibernético, garantindo a integridade, disponibilidade, confidencialidade e autenticidade, e evitando que a organização registre perdas de qualquer tipo em função de falhas e lacunas em seus sistemas e processos. O desafio é permanente, dado que os métodos de ataque cibernético estão em constante mudança.

1.1. Benefícios da efetiva gestão de riscos cibernéticos

A gestão de riscos da informação deve ser entendida como uma prática dinâmica e contínua capaz de manter os gestores cientes dos riscos integrados de negócio e seus componentes, para que eles sejam capazes de compreender o contexto e tomar decisões que envolvem a aceitação, redução e transferência, orientando a escolha dos melhores controles e seus respectivos níveis de maturidade a depender do apetite da própria organização.

Ela tem vários pilares: a identificação dos riscos, a classificação em seus tipos, a avaliação sob as óticas de **risco potencial e risco residual** ✪, a identificação e a avaliação da efetividade dos controles, o monitoramento, o escalonamento e a comunicação do nível de riscos. A gestão de risco também envolve o tratamento dado aos riscos: aceitar, reduzir e transferir, sempre considerando o apetite e a tolerância a riscos da organização.

✪ Risco potencial é o risco que existe em estado "puro", ou seja, antes da inserção de qualquer tipo de controle para reduzi-lo. O risco residual, em contrapartida, é o risco que subsiste após a inserção de controles e o tratamento de riscos.

A gestão da segurança da informação é parte integrante da gestão de riscos corporativos, e envolve a identificação de probabilidades, impactos, vulnerabilidades e ameaças, a aplicação de ações mitigatórias e soluções abrangentes para garantir que a organização esteja adequadamente protegida dentro dos critérios próprios de tolerância ao risco.

A boa gestão de riscos cibernéticos traz uma série de benefícios:

- aumenta a compreensão e o comprometimento *(awareness and commitment)* das pessoas em relação ao papel e responsabilidade de cada indivíduo na gestão do risco da informação e para com as práticas de segurança dele;
- protege os ativos, dados, informações e conhecimento;
- protege a imagem e a reputação das empresas;
- valoriza a empresa frente a parceiros, clientes, bancos, seguradoras e ao mercado em geral;
- propicia a continuidade do negócio em momentos de estresse operacional e crises;
- viabiliza o cumprimento de leis e regulamentações aplicáveis;
- aprimora a governança corporativa;
- contribui para a perenidade e sustentabilidade da empresa.

Para minimizar o risco cibernético, as empresas podem se utilizar de várias soluções físicas, tecnológicas, humanas e processuais, mas como é praticamente impossível estar imune aos ataques cibernéticos, muitas já fazem uso do seguro contra riscos cibernéticos.

1.2. Conselho de administração

Como guardião do sistema de governança corporativa, o papel do conselho abarca a compreensão de todos os riscos integrados de negócio, inclusive os advindos do risco cibernético. Esses últimos não devem ser vistos como apenas mais um item, mas como parte do sistema de gestão de riscos da empresa.

Como se sabe, a gestão de riscos é fundamental para evitar imprevistos e fracassos corporativos e desempenha hoje um papel estratégico para as organizações, na medida em que contribui para a tomada de decisões empresariais, para a proteção de ativos e para a geração de valor. E essas são tarefas da alçada da diretoria.

O conselho desempenha papel fundamental ao garantir o alinhamento da estratégia do negócio com a estratégia de segurança da informação. Ele também é importante para ratificar o apetite a riscos da companhia em relação a riscos cibernéticos, pois eles afetam a informação necessária para o atendimento dos objetivos corporativos.

Para embasar a atuação do conselho, é importante que antes tenha ocorrido uma identificação das informações ou ativos mais sensíveis e cruciais da organização, e que devem ser protegidos de forma mais intensa. A ideia aqui é que, quanto mais importante o ativo (ou o dado), mais fortes devem ser os controles.

Vale lembrar que, na hora de decidir sobre o tipo de medida a ser adotada com relação aos riscos cibernéticos, o conselho também precisa conhecer o aparato legislativo e a forma como ele se aplica à empresa, inclusive por meio de sanções. Sabendo que essas sanções podem ser materialmente relevantes, elas têm impactos também sobre o desempenho financeiro (veja mais informações sobre as legislações em texto à página 33). Cabe ressaltar que os conselheiros têm dever de diligência nas empresas em que atuam e devem empenhar seus melhores esforços para aumentar a resiliência cibernética delas.

Mas as atribuições do conselho não param na determinação do apetite a riscos. Elas incluem a aprovação da política corporativa de segurança da informação e os planos de ação para mitigar os riscos cibernéticos. O envolvimento com o assunto pressupõe também o acompanhamento de simulações periódicas sobre ataques cibernéticos e planos de crise, de forma a garantir que a organização esteja preparada quando ocorrerem crises de verdade – uma das poucas certezas que se pode ter atualmente, no mundo dos negócios, é a da ocorrência de um incidente cibernético que afeta diretamente a informação.

As simulações são exercícios que podem contribuir para o enfrentamento de ataques reais e ajudam a aumentar a resiliência cibernética da empresa. O conselho também precisa assegurar que, na ocorrência de um incidente cibernético, a empresa conte com responsáveis pela comunicação a todos os *stakeholders* internos e externos.

A resiliência cibernética é a capacidade de uma organização de gerenciar e implementar os controles necessários para prevenir, detectar e gerenciar ataques cibernéticos, tais como os mecanismos de identificação, proteção e detecção dos ataques e, também, a capacidade de resposta e recuperação de suas atividades quando ele ocorre.

Outro ponto importante é que o conselho leve em conta dados e avaliações concretas sobre risco cibernético quando estiver decidindo sobre a política de investimentos da empresa. Medidas para mitigar risco cibernético não geram uma contrapartida direta de receita, mas, como já visto no item anterior, trazem benefícios que, em última instância, protegem o valor da empresa.

A dedicação com relação ao tema terá implicações relevantes na resiliência cibernética da organização. Aqui precisamos fazer um parêntese para falar da resiliência em riscos cibernéticos e de que forma o conselho pode contribuir para aumentá-la. A resiliência implica na preparação da empresa para responder aos ataques e demais ameaças por meio da prevenção, detecção, monitoramento, promoção de rápidas respostas, minimização de danos e continuidade das operações, mesmo sob ataque.

A resiliência tem importância vital para as organizações, pois permite que a empresa possa inovar em produtos e serviços com segurança, fortalecendo a confiança de todas as partes envolvidas nas atividades. A resiliência cibernética é uma das bases para a resiliência corporativa, ou seja, a capacidade de a empresa se adaptar a novas realidades concorrenciais e de se recobrar de revezes e crises no ambiente que atua. Como afirmamos no início deste capítulo, o risco cibernético é um risco relacionado ao negócio e extrapola em muito a parte tecnológica.

Em muitas das companhias mais avançadas em termos de resiliência cibernética, os conselheiros têm ciência não apenas dos orçamentos direcionados à segurança cibernética, mas também das questões operacionais, dos testes de segurança e do progresso da companhia com relação à área.

Ou seja, o interesse pelo tema faz a diferença. Nesse sentido, é importante que os conselheiros busquem aumentar seus conhecimentos sobre o assunto, de forma a qualificarem-se para fazer as perguntas mais apropriadas e a formar opiniões sobre o tratamento dado à segurança cibernética na empresa, buscando balancear a busca pela inovação com a preocupação com o risco.

Você sabia?

A detecção de um ataque cibernético nem sempre é simples. Frequentemente, as empresas demoram a percebê-lo e, consequentemente, a combatê-lo – o que eleva os custos de um ataque. Levantamento feito pela Accenture e Instituto Ponemon, em 2018, mostrou que 21% das empresas participantes da pesquisa foram avisadas de ataques por parte de integrantes da comunidade de segurança, e 17% por competidores ou pares, evidenciando que nem sempre a detecção ocorre dentro de casa, e que a colaboração de terceiros é também fundamental.

Accenture e Ponemon Institute – *Gaining Ground on the cyber attacker 2018 - State of Cyber Resilience.*

Já um estudo realizado pelo Instituto Ponemon publicado em 2017 mostrou que os ataques provocados por *malicious code* eram os mais demorados para serem resolvidos: isso levava, na média, 55,2 dias. Em seguida, vinham os ataques por *malicious insiders*, com 50 dias, na média, e *rasomware*, com 23,1 dias. Os mais rápidos de serem resolvidos eram os ataques provocados por *malware* e robôs (*botnets*), cujos problemas eram sanados em 6,4 dias e 2,5 dias, em média.

Ponemon Institute. *Cost of cyber crime study 2017 – Insights on the security investments that make a difference*, 2017.

O conselho deve, também, acompanhar a maturidade do ambiente de segurança cibernética da empresa. Para que os conselheiros possam fazer face a todas essas atribuições, precisam ter incluído as questões relacionadas a risco cibernético dentro do portfólio de gestão de riscos empresariais na pauta das reuniões. Além disso, precisam estar cientes da relevância de considerar os investimentos em segurança da informação, levando em conta de que nem sempre é possível quantificar os ganhos (ou perdas evitadas) proporcionados por esses investimentos.

A cultura de segurança cibernética

A falha humana está relacionada ao sucesso de muitos dos ataques cibernéticos. Por conta disso, a promoção da cultura de segurança cibernética dentro de uma empresa é essencial: ela aumenta a resiliência cibernética. Se os funcionários e colaboradores estão cientes dos riscos cibernéticos, entendem a importância da prevenção e, ainda, se eles se engajam na proteção dos ativos da empresa, reduz-se a probabilidade de que os atacantes causem algum dano relevante.

A preocupação com segurança cibernética deve ser vista como parte das atribuições dos funcionários, que devem incorporá-la nas suas atividades. Assim como em outros aspectos relacionados à cultura organizacional, a cultura cibernética também pode ser aprimorada. Nesse sentido, o envolvimento da alta gestão é essencial para que a empresa como um todo avance na proteção de seus ativos. O estabelecimento de políticas e guias sobre o tema, assim como os treinamentos são importantes ferramentas para promover a cultura de segurança cibernética.

Cabe aos conselheiros supervisionar a tarefa dos gestores de implantar a cultura voltada para a promoção da segurança cibernética que pode contribuir para proteger a empresa contra invasões. Para executar essa tarefa, devem questionar se a liderança:

- direciona recursos suficientes, e de forma adequada, para o orçamento relacionado a riscos cibernéticos;
- promove programas de treinamento e educação para conscientizar os funcionários da importância do risco cibernético;
- ajuda a construir a cultura de responsabilização pelo sistema de controles internos da companhia;
- implementa sistemas que permitem o cumprimento de todas as normas de proteção de dados que se aplicam à empresa;
- comunica-se de forma adequada com os funcionários, mostrando que a proteção de dados é um valor da empresa.

Além desses aspectos ligados à promoção da cultura, os conselheiros podem também verificar se os gestores:

- possuem o diagnóstico da maturidade de segurança cibernética atual e os próximos passos para otimização;
- conseguem prevenir e detectar ataques cibernéticos;
- implantaram medidas para mitigar os riscos advindos de parceiros de

negócios, que têm acesso aos sistemas da empresa ou a seus dados;
- elaboraram um plano de ação para lidar com incidentes cibernéticos e acompanhar periodicamente a evolução dos planos de mitigação relevantes.

Tarefas dos conselheiros de administração:

- ✓ compreender os riscos cibernéticos integrados e inerentes aos negócios da organização;
- ✓ garantir o alinhamento da estratégia do negócio com a estratégia de segurança cibernética;
- ✓ contribuir para a definição dos ativos críticos da empresa;
- ✓ ratificar o apetite a riscos da companhia em relação a riscos cibernéticos;
- ✓ aprovar a política de segurança da informação corporativa e seu efetivo modelo de governança;
- ✓ acompanhar a evolução na maturidade do ambiente de segurança cibernética da companhia;
- ✓ supervisionar a implantação da cultura voltada para a promoção da segurança cibernética;
- ✓ obter conhecimento interno ou buscar orientação externa com especialistas em riscos cibernéticos;
- ✓ informar-se sobre planos de crise e contingência para lidar com ataques cibernéticos, aprová-los e monitorá-los;
- ✓ participar de simulações periódicas sobre crises cibernéticas.

1.3. Diretoria executiva

O papel da diretoria executiva na gestão de riscos cibernéticos está relacionado a implementar as recomendações do conselho de administração e garantir a existência e a efetividade do ambiente e atividades de controle esperados para alcançar os objetivos propostos, reportando ao conselho a evolução desse quadro. A diretoria tem papel preponderante para municiar o conselho com informações relevantes para a tomada de decisões referentes aos riscos cibernéticos.

No papel de implementação, a diretoria é responsável pela participação ativa na elaboração da estratégia da segurança da informação e alinhamento com a estratégia do negócio, pela definição da estrutura organizacional e diretrizes de processos para a implementação da segurança da informação e, ainda, por trabalhar em conjunto com a governança da segurança da informação no sentido de garantir a implementação de suas políticas. Quando viável, deve-se buscar o diagnóstico e a análise do nível de maturidade de segurança da informação da organização por meio de áreas independentes internas e/ou empresas externas especializadas.

1.4. A função do profissional de segurança da informação

A segurança da informação é um tema mais amplo que a segurança cibernética, pois engloba não apenas os ativos digitais, mas também as pessoas, os processos, os ativos físicos (equipamentos), bem como informações que transitam em papéis e contratos. Além do conselho de administração e da diretoria executiva outras áreas e funções também desempenham papel fundamental na gestão da segurança cibernética de uma organização: a auditoria interna, o comitê de auditoria, o Chief Information Security Officer (CISO) – responsável pela segurança da informação e o Chief Risk Officer (CRO) – responsável pela gestão dos riscos.

No entanto, nem todas as organizações possuem todas essas funções – a estrutura de cada uma está relacionada ao seu porte, setor de atuação e o grau de maturidade em segurança da informação e cibernética. O importante é que haja um responsável pela gestão dos riscos cibernéticos, e que ele seja qualificado para exercer essa atividade. Quando não existe a figura do CISO, a responsabilidade pela segurança da informação da empresa pode ser de outro diretor, como o CRO, ou de algum gerente (a depender do porte da empresa, área de atuação, estratégia, etc.). O ideal é que o profissional responsável pela função esteja em nível hierárquico equivalente a outros diretores, tendo assim condições de fazer as suas demandas a partir do mesmo patamar dos demais executivos.

É fundamental que o responsável pela segurança da informação tenha total independência para supervisionar, monitorar, escalar e comunicar sobre qualquer tema relacionado a riscos cibernéticos. Como boa prática, e tendo em vista a redução de possíveis conflitos de interesse, recomenda-se que esta função não esteja subordinada diretamente à área de tecnologia da informação (CIO – Chief Information Officer). Trata-se de um requisito básico para que possa exercer seu papel sem que haja nenhum tipo de conflito de interesse com o seu líder.

Como a área de tecnologia da informação (TI) possui metas desafiadoras para atender os objetivos de negócio, isso pode, em alguns casos, não garantir a adequada implementação de todos os programas de segurança da informação, e como consequência, aumentar a exposição ao risco cibernético. Quando há independência do responsável pela segurança da informação, e todo um arcabouço de governança da informação, esse conflito de interesse é minimizado. Organizações mais maduras possuem suas estruturas de segurança da informação segregadas das áreas de TI e sem nenhuma relação com o líder da função (CIO).

Nas empresas em que há um gerente de segurança da informação que presta contas ao CIO – que é da área de tecnologia – este último costuma se reportar ao presidente, permitindo que a questão da segurança cibernética seja vista de forma mais ampla, com impactos sobre todo o negócio, e não como restrita à área de TI. No entanto, o mais adequado é a segregação: o responsável pela segurança da informação responde ao CEO/Presidente ou área de gestão de riscos, enquanto o profissional da segurança de TI fica encarregado de implementar as decisões corporativas, buscando as melhores alternativas tecnológicas para tanto.

Espera-se que o profissional responsável por proteger as informações na empresa tenha papel importante não apenas no desenho de estratégias, mas também que assegure que essas foram implementadas de forma correta, em consonância com o perfil e o apetite a risco da empresa. Ele se torna a principal referência da empresa no que diz respeito à segurança da informação.

Além disso, espera-se que ele contribua para a avaliação e quantificação de riscos cibernéticos e que atue para que os demais executivos e conselheiros de administração compreendam melhor as exposições da empresa a um ataque cibernético. As demandas do mercado requerem que, cada vez mais, esse profissional esteja atento não apenas às questões técnicas, mas ao conhecimento do negócio e à capacidade de interação com diversas áreas da organização para fomentar a cultura da segurança cibernética. Ou seja, é necessário que o profissional detenha conhecimento técnico e visão de negócio.

O profissional responsável pela função de segurança da informação exerce o papel de guardião e supervisão do cumprimento da política de segurança da informação, sempre baseado em boas práticas de mercado, como por exemplo, nos controles definidos pelas normas da família ISO 27.000.

A ISO 27.032 apresenta diretrizes para segurança cibernética, bem como recomendações para a mitigação deste tipo de risco.

O conselho de administração, na tarefa de monitorar a gestão dos riscos, pode contar com o suporte dos comitês de assessoramento do conselho, como os comitês de gestão de riscos e/ou de auditoria. Quando há um comitê de gestão de riscos, o responsável pela segurança da informação reporta hierarquicamente ao CEO/área de riscos e periodicamente ao comitê. Na inexistência de um comitê de gestão riscos, o comitê de auditoria – que assessora o conselho em assuntos relacionados às demonstrações financeiras, a controles internos e à gestão de riscos – é o responsável pela gestão dos riscos cibernéticos. Esse comitê contribui também para a análise da adequação de recursos para gerenciamento desses riscos, para a análise de alguns controles internos pertinentes ao assunto e para o acompanhamento da adequação por parte da empresa à legislação.

Como vimos, são vários os agentes que atuam para gerenciar os riscos cibernéticos de uma empresa ou organização. A atuação de todos está interligada pelo responsável pela segurança da informação, mas cada um tem o seu papel:

- os conselheiros de administração estabelecem diretrizes relativas à segurança cibernética e definem limites de risco. Suas atribuições variam de empresa para empresa e podem incluir ainda o monitoramento da efetividade do sistema para mitigação do risco cibernético, a obrigação de informar, de dar transparência às partes interessadas sobre a estrutura de controle específica para esse fim, existente na empresa, bem como as eventuais ocorrências relevantes e as respectivas consequências e providências para a sua correção;
- os diretores recebem as diretrizes dos conselheiros, as implementam e os municiam com informações relevantes para a tomada de decisões;
- o responsável pela segurança da informação funciona como o principal elo entre as diversas áreas da empresa e atua para tornar operacionais as diretrizes dos conselheiros, além de identificar falhas no processo e possíveis ameaças que devem ser comunicadas e tratadas.

O profissional responsável pela função de segurança da informação se relaciona intensamente com a área de TI, com o conselho, os diretores e com todas as áreas de negócio, uma vez que as informações permeiam a atuação da empresa como um todo:

- recebe informações da área de TI como dados relevantes, métricas para controle e insumos para o *design* de monitoramento da segurança cibernética;

- envia ideias e sugestões para a área de TI referentes ao combate às ameaças cibernéticas e soluções para o *design* de sistemas;
- mantém contato com o mercado para se manter atualizado sobre as melhores práticas;
- é responsável por garantir que as soluções para combate às ameaças cibernéticas sejam implementadas;
- recebe informações do conselho de administração relacionadas aos eventos e estratégias de negócio;
- submete para aprovação do conselho sugestões de linhas de ação referentes às ameaças cibernéticas, aos negócios e relatórios sobre a segurança cibernética da organização.

1.5. A gestão de riscos cibernéticos e as três linhas de defesa

O modelo de três linhas de defesa definido pelo Instituto dos Auditores Internos (IIA) tem sido utilizado pelas organizações para delimitar os papéis, responsabilidades e interações entre os diferentes agentes no que diz respeito à gestão de riscos, na qual se inclui a gestão do risco cibernético.

A primeira linha de defesa tem responsabilidade direta em relação às práticas de gestão de riscos e controles internos. Nela estão os gestores das unidades e os responsáveis diretos pelos processos. É ela que implementará os controles necessários para gerenciar e reduzir os riscos cibernéticos. Todas as áreas de primeira linha de defesa desempenham papel relevante na gestão de riscos, uma vez que é na ponta, no processo em execução, que o risco cibernético se materializa.

Na primeira linha, vale destacar a importância dos "sineiros", os funcionários que observam um sinal de perigo de invasão e soam os alarmes para que os responsáveis atuem prontamente. Uma vez que esse papel é destacado e disseminado na empresa, a tendência é que as ocorrências sejam mais rapidamente identificadas e solucionadas.

A segunda linha de defesa é responsável por monitorar a visão integrada de riscos, desenvolver políticas e metodologias, dar suporte, supervisionar e monitorar o desempenho da gestão de risco feita pela primeira linha de defesa (áreas operacionais), realizando também testes de controle e simulações. A função de segurança da informação dentro de uma empresa encontra-se na segunda linha, e é a responsável por implementar e monitorar os programas de prevenção de ataques cibernéticos, tais como gestão de vulnerabilidades de aplicação, prevenção de perdas, treinamento em segurança das ameaças e os testes de intrusão como os Ethical Hacking Tests (EHT) – que avaliam o grau de segurança técnica de um sistema ou rede por meio da simulação de um ataque. Espera-se que a segunda linha prepare um cronograma de simulações que contemple diretrizes, aspectos que devem ser priorizados e vulnerabilidades que precisam ser mitigadas. Recomenda-se que o cronograma seja apresentado ao conselho de administração.

As atribuições da segunda linha de defesa relacionadas aos riscos cibernéticos, responsabilidade da função de segurança da informação dentro da organização, podem ser assim elencadas:

- definir a visão, missão e estratégia para gestão dos riscos cibernéticos na organização alinhada à estratégia do negócio e apetite ao risco;
- definir as diretrizes e dar suporte à primeira linha de defesa na imple-

mentação das políticas, normas e procedimentos, considerando seus papéis e responsabilidades;
- realizar o treinamento e conscientização dos colaboradores da organização fomentando uma cultura de segurança cibernética e estabelecendo um sistema de educação continuada;
- identificar, classificar, quantificar, analisar, priorizar, tratar, monitorar e reportar os incidentes e os riscos cibernéticos;
- apoiar a gestão de riscos em fornecedores e parceiros, durante a seleção do terceiro e de todo o ciclo de vida do relacionamento da organização com o mesmo;
- atuar na resiliência e continuidade de negócios (plano de continuidade operacional, plano de recuperação de desastres de TI e gestão de crises);
- realizar o monitoramento dos indicadores e da conformidade da organização e dos terceiros; 🕮

🕮 Sergio Kogan e Henrique Quaresma, "Integração da gestão de riscos cibernéticos nas três linhas de defesa", *IBGC Análises & tendências*, número 4, julho 2018, pág. 7.

- Elaborar um cronograma, apresenta-lo ao CA e realizar simulações periódicas de ataques.

A terceira linha de defesa é realizada pela auditoria interna. É recomendável que esta área tenha profissional especializado em segurança da informação. Na ausência de um profissional capacitado, o conselho deve, periodicamente, avaliar a necessidade de contratar especialistas externos para executarem testes independentes das atividades de gestão de riscos cibernéticos.

A auditoria interna pode, por meio da atuação de profissionais internos ou contratados, realizar avaliações independentes sobre a eficácia dos processos da companhia em proteger os dados e informações da empresa, especialmente sobre os ativos e informações mais valiosas e críticas. Para tanto, pode levar em conta as principais vulnerabilidades, a eficácia dos controles internos, a realização de testes e simulações de ataques cibernéticos e seus resultados.

A auditoria se debruça sobre os processos da organização e não somente sobre as áreas de TI e segurança da informação. Os resultados obtidos pela auditoria podem e devem ser usados para a proposição de melhorias na resiliência cibernética.

2

Os ataques cibernéticos e as leis

Já é conhecido que os riscos cibernéticos fazem parte do cotidiano das empresas. Mas de que forma eles se manifestam no dia a dia? Neste capítulo faremos um breve panorama das motivações dos ataques cibernéticos, do perfil dos criminosos e as técnicas que utilizam e procuraremos responder à seguinte pergunta: por que as empresas falham em guardar e processar informações sensíveis, facilitando a ação dos atacantes? Falaremos, ainda, sobre as principais leis que versam sobre segurança cibernética.

2.1. Como os alvos dos ataques são escolhidos? E quais as consequências para as empresas?

Ataques cibernéticos são ofensivas aos sistemas, infraestrutura e dados (operacionais e pessoais) de uma organização e que visam destruir, expor, modificar, roubar ou ter acesso a um ativo ou de usá-lo sem autorização.

Os ataques sempre têm algo em comum: o objetivo de prejudicar o seu alvo e/ou obter vantagem para si ou terceiros. Mas as formas pelas quais causam danos variam muito. Estas podem incluir roubo ou destruição de ativos, propriedade intelectual ou outras informações confidenciais pertencentes a empresas, seus clientes ou seus parceiros de negócios. Outra modalidade de ataque cibernético é o direcionado à interrupção das operações de empresas públicas ou seus parceiros. Isso inclui segmentar empresas que operam em setores responsáveis por infraestrutura crítica, tais como companhias de energia, saneamento e de telefonia, e

costuma ser feito por meio de ataques a áreas vulneráveis da companhia.

Enganam-se aqueles que pensam que apenas as grandes organizações serão alvos de ataques. Os invasores buscam invadir sistemas com fragilidades, independentemente do porte das empresas. Um ataque cibernético nem sempre é bem-sucedido – e a luta das organizações é para que nunca o seja. São necessários vários ataques até que algum prospere. E, quando isso ocorre, costumam deixar um rastro de prejuízos e ocasionam vários tipos de danos. Há perdas diretas e indiretas, essas de mais difícil quantificação.

A organização pode experimentar interrupção nos seus negócios, deixando de fechar transações e de faturar em função da impossibilidade de operar de forma normal e rotineira. Pode perder propriedades intelectuais que possui em seu nome ou posse, além de importantes dados utilizados para suas operações e seus negócios, como informações sobre clientes, projetos e funcionários. Também pode se ver obrigada a consertar equipamentos e a reparar a infraestrutura. Ou, ainda, perder clientes e fornecedores, uma vez que fica impossibilitada de atendê-los adequadamente.

Mas os custos não param por aí. A empresa fica exposta a demandas judiciais ou administrativas. Uma vez que a não observância das novas regulamentações sobre privacidade e proteção de dados (General Data Protection Regulation na União Europeia – GDPR – e Lei Geral de Proteção de Dados Pessoais – LGPD – no Brasil) , também podem acarretar em multas. Demandas administrativas ou judiciais podem ser movidos contra a empresa por seus clientes, outras partes prejudicadas pela exposição ou roubo das informações ou ainda por instituições de defesa de interesse coletivo, por meio de ações civis públicas ou outros procedimentos. Processos administrativos também podem ser movidos pela Autoridade Nacional de Proteção de Dados (ANPD), resultando na aplicação de sanções, inclusive de multas.

O risco percebido pelas seguradoras e bancos pode aumentar, levando a um aumento do prêmio dos seguros e do custo do crédito. Um ataque cibernético de grandes proporções costuma ocasionar uma queda no valor de mercado de qualquer organização.

E, ainda, há custos mais difíceis de serem mensurados, como a perda de tempo, foco e esforços dos funcionários da organização para lidar com o ataque e suas consequências.

Não menos importante é o custo trazido pela perda de reputação e confiança na capacidade de a empresa manter os dados íntegros e em sigilo – que pode ser significativo para a sustentabilidade dos negócios. Esse tipo de risco é especialmente grave no setor de saúde, por exemplo,pois expõe informações sensíveis dos pacientes, conforme define a lei ✪.

Em casos mais graves, e setores mais críticos, os ataques podem implicar até mesmo em perda de vidas (é o caso, por exemplo, de ataques já registrados ao fornecimento de energia elétrica).

✪ A Lei Geral de Proteção de Dados Pessoais (LGPD) define, em seu artigo 5, dado pessoal sensível como: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

2.2. Como os criminosos entram nas organizações? E que técnicas utilizam?

Embora tenham algo em comum – a intenção de causar danos às organizações e/ou de obter vantagens – os ataques variam muito em complexidade: podem ser bem simples, explorando vulnerabilidades conhecidas dos sistemas, até bem complexos, explorando vulnerabilidades pouco evidentes ou mesmo voltando-se para a descoberta de lacunas e pontos fracos de tecnologias emergentes. Vejamos, abaixo, as principais técnicas utilizadas pelos criminosos.

- Negação de serviços – por meio dessa técnica, os atacantes sobrecarregam sistema de informação com requisições, ou seja, enviam requisições superiores à capacidade de resposta do sistema. Como este não pode suportar essa quantidade de requisições, fica indisponível ou com o desempenho prejudicado.
- Interceptação – o atacante se insere no meio da comunicação entre o usuário e um determinado sistema, com foco no roubo de informações trocadas entre eles.
- Engenharia social – é o uso de comunicações falsas para enganar os usuários e obter informações privilegiadas ou confidenciais de forma indevida. É um "ataque de persuasão", que conta com a ingenuidade ou o descuido do usuário para obter informações que serão usadas em potenciais ataques. O modo mais conhecido de crime cibernético do tipo é o *phishing*, que consiste no envio de uma mensagem, geralmente por e-mail, com um link ou um arquivo em anexo que baixa o *malware*. Outra variação é o *pretexting*, que se assemelha com o *phishing*, mas que em geral envolve a construção de uma narrativa falsa visando obter informações. Geralmente, ele implica na troca de mensagens entre o criminoso e a vítima. É o caso, por exemplo, de e-mails enviados no nome de executivos, que pedem que o funcionário da empresa, geralmente da área financeira, transfira recursos para determinada conta. No entanto, a engenharia social ainda pode ser realizada, por exemplo, por meio de ligações telefônicas, pesquisas no lixo das organizações para buscar informações sensíveis não destruídas adequadamente. A engenharia social pode ser considerada um tipo eficiente de ataque, já que depende da não observância de usuários e profissionais sobre determinadas práticas preventivas. Portanto, surte efeito por uma questão cultural ou de comportamento inadequado.
- Roubo de senha – utilização de técnicas para identificação de credenciais válidas de usuários e suas respectivas senhas.
- Manipulação de dados em sistemas – utilização de técnicas para contornar os controles de validação de dados nos sistemas, com o intuito de obter informações de forma indevida.
- *Malware* ou software malicioso – *malware* é uma palavra genérica que vem da junção de *malicious* software. Como os nomes originais dão a entender, ela designa a utilização de arquivos ou aplicações que embarcam conteúdo malicioso para comprometer o ambiente das organizações, seja através do roubo de informações, do fechamento do ambiente, entre outras técnicas.

Um breve passeio pelo mundo do crime cibernético

Os ataques cibernéticos vêm se tornando mais constantes, custosos e danosos. E não é apenas o incremento do uso da tecnologia que está ocasionando esse fenômeno. Eles estão se tornando mais populares também por conta da disseminação de informações sobre como perpetrar um ataque. Hoje, é possível comprar com facilidade sistemas de ataque na internet.

Esta, vale lembrar, tem "*deep web*" e a "*dark web*". Ambas são partes não visíveis da internet, não são indexadas e, por conta disso, inacessíveis a mecanismos de busca. Nas duas camadas, coexistem conteúdos legítimos com outros ofensivos e criminosos. A "*deep web*" contém sites que não têm URL permanente, sites de empresas e pessoas que não desejam incluir suas páginas nas ferramentas de busca por diversos motivos, bem como por páginas que precisam ser acessadas em um ambiente específico.

Já a "*dark web*" é uma parte da *"deep web"*, encriptada e que muitas vezes requer softwares específicos para o acesso. Nela são comercializadas armas, drogas, todo tipo de conteúdo ilícito e dados obtidos por meio do crime cibernético. Ela também propicia a troca de informações entre *invasores*. Na *"dark web"* predomina conteúdo ilegal.

No entanto, não é necessário sequer acessar essas outras camadas da internet: hoje em dia, há até mesmo vídeos com tutoriais sobre ataques cibernéticos em sites como o Youtube e venda de informações roubadas por meio do Facebook.

Geralmente, antes de tentar invadir organizações de países mais desenvolvidos, os criminosos cibernéticos testam as resistências de organizações de países mais vulneráveis. Se, na Rússia, China, Estados Unidos e União Europeia a conscientização sobre o risco cibernético é maior, em países como o Brasil ainda não há a devida atenção ao tema e tratamento – o que torna nossas organizações mais expostas.

Vale dizer ainda que há subnotificação dos casos, uma vez que as empresas frequentemente demoram algum tempo para detectá-los e, quando os detectam, nem sempre admitem que não conseguiram evitar a perda ou o roubo de seus dados.

Alguns ataques cibernéticos fazem parte da história recente. Um ataque de grandes proporções foi o Petya, utilizado na Ucrânia em 2016 – quando o *malware* conseguiu desligar estações de energia, deixando mais de 200 mil pessoas sem energia por oito horas. O Petya chegou ao Brasil, mas causou danos contidos, porque, por conta do fuso horário, as empresas tiveram algum tempo para se proteger.

O Mirai também foi perpetrado em 2016 e paralisou vários serviços providos pela internet, como plataformas de mensagens e de música, além de atacar câmeras desprotegidas e roteadores – mostrando que *malwares* podem atacar qualquer dispositivo conectado à internet, inclusive os da internet das coisas.

No ano seguinte, seria a vez do WannaCry, com o seu sugestivo nome. Ele trouxe distúrbios e teve amplitude sem precedentes. O *malware* infectou, por meio da tática de *phishing*, operadoras de telefonia, empresas de serviços públicos, bancos, hospitais e outras organizações em vários países. O *malware* pedia um resgate em criptomoeda para que os dados roubados não fossem destruídos.

O tipo de *malware* que mais vem crescendo é o *ransomware*, que ataca tanto indivíduos quanto organizações. Geralmente, após infectar os computadores com softwares que bloqueiam acesso ao computador ou aos seus dados, os atacantes pedem uma recompensa financeira (*ransom*, em inglês, ou resgate) para que o usuário possa voltar a usar o seu equipamento ou ter acesso aos seus dados.

2.3. Os criminosos cibernéticos e suas motivações

Criminosos cibernéticos podem ser grupos terroristas, integrantes do crime organizado ou mesmo Estados interessados em desestabilizar governos ou outras nações. Mas podem ser também qualquer outra pessoa e, até mesmo, ex-empregados ou empregados insatisfeitos.

Como se vê, os atacantes podem ser internos (ligados à organização) ou externos. Os ataques podem ter várias motivações: tirar proveito financeiro, obter algum tipo de vantagem competitiva por meio da espionagem, vingar-se, prejudicar as atividades de outrem por diversão e manifestação de poder, influenciar países e opiniões, etc. Ou, eventualmente, quando são agentes internos, podem ter agido por desconhecimento das regras e políticas de segurança e imprudência. Incidentes e eventos cibernéticos nem sempre são ocasionados por criminosos e podem ocorrer sem intenção e má fé.

Tarefas dos conselheiros de administração:

Alguns grupos de *invasores* fazem associações informais e descentralizadas para perpetrar ataques cibernéticos em busca de dinheiro e fama. Mas a guerra cibernética também tem outro lado. É o caso da organização sem fins lucrativos *Malware must die*, composta por profissionais que buscam pesquisar e descobrir ataques por *malware* na internet. Também é possível contratar empresas para simular ataques e invasores para fazer simulações e testes relacionados a riscos cibernéticos.

Mas há também quem atue por questões políticas ou sociais, os hacktivistas. Nesta última categoria, está o famoso grupo descentralizado Anonymous, cujo símbolo é a máscara de Guy Fakes (mais conhecida pelo filme *V de vingança*), tido como responsável por ataques à igreja da Cientologia, a agências do governo dos Estados Unidos, ao grupo terrorista Estado Islâmico, a sites de pornografia infantil, e que ajudou no vazamento de dados do caso WikiLeaks e apoiou o movimento Occupy.

Ao contrário do que muitos imaginam, nem sempre os criminosos estão em busca de informações que podem trazer ganhos óbvios, como dados de cartões de crédito e de informações financeiras dos consumidores. Como suas motivações são inúmeras, eles podem também visar obter informações estratégicas das empresas (como planos de negócios e documentos sigilosos), algoritmos, contratos, listas de funcionários e suas credenciais, informações sobre as instalações e equipamentos das empresas e sobre suas patentes.

Seja como for, o fato é que os criminosos estão escalando as operações – ou seja, buscando aumentar a escala e o impacto dos ataques – por meio de técnicas mais sofisticadas.

2.4. Onde as empresas falham

Como vimos, são várias as táticas que os criminosos cibernéticos costumam usar. Eles conseguem penetrar nos sistemas das organizações e empresas pelos diversos tipos de dispositivos e equipamentos, pertencentes a parceiros, clientes, funcionários e colaboradores e toda a possível rede de partes relacionadas com que a empresa lida.

Em grande medida, os criminosos cibernéticos contam com falhas humanas para obter sucesso em seus ataques. Vale ressaltar que esses estão entre os principais fatores que levam as empresas a fracassar.

Essas falhas estão ligadas a questões gerenciais, como a ausência ou ineficácia de processos, procedimentos e controles que poderiam minimizar o risco de a empresa ser vítima de um ataque. Conforme citamos na introdução deste documento, em pesquisa feita com 150 empresas latino-americanas ao longo de 2018, 70% delas consideraram que não têm certeza da eficácia de suas respostas face aos incidentes cibernéticos 🕮. E apenas 3% disseram realizar simulações para testar a eficácia de suas respostas frente a um ataque cibernético.

🕮 Deloitte. *op. cit.*, 2019.

Nota-se que os desafios para evitar ataques cibernéticos vêm de várias frentes: desde a implementação de controles, ao aprimoramento do processo de gestão do risco cibernético e de aspectos relacionados à cultura organizacional, até as próprias questões tecnológicas que envolvem a questão.

Veja abaixo quais são os principais motivos que levam as empresas a falhar na guarda e processamento de informações sensíveis, levando ao crime cibernético:

- Escopo impróprio – frequentemente, as empresas focam seus esforços apenas nos seus sistemas principais, onde estão os mais importantes dados a serem salvaguardados. Elas deixam de proteger os sistemas secundários. Só que estes dão suporte para a operação dos sistemas principais e podem ser uma porta de entrada de ataques cibernéticos. O ideal, portanto, é ampliar o escopo de proteção, incluindo também os sistemas secundários, e tornar a proteção abrangente.
- Falha ao atualizar sistemas regularmente – os softwares costumam sempre ser atualizados por seus criadores para corrigir eventuais falhas e vulnerabilidades ou para melhorar o desempenho dos mesmos. Essas correções se dão por meio de *patches* (remendos), que são programas que atualizam os softwares. Um dos erros comuns das empresas é o de não fazer essas atualizações e não instalar os *patches* críticos de segurança – o que abre espaço para ataques. Por conta desse problema

com atualização, muitas empresas estão optando por sw em *cloud* (nuvem) ou SaaS (Software as a Service), que atualizam os *patches* de forma gratuita.

- Falha ao encerrar o acesso – aqui está um erro muito comum, facilmente evitável, e que conta com dois aspectos. O primeiro é a falha ao encerrar o acesso do ex-funcionário, e ocorre quando a empresa não encerra o acesso dos funcionários e demais colaboradores a seus sistemas, mesmo após eles serem desligados do quadro de colaboradores. O encerramento do acesso deveria ser incluído no processo de desligamento do funcionário, uma vez que o acesso não se faz mais necessário e pode ser utilizado para fins indevidos. Outro aspecto está relacionado ao funcionário efetuar o *logoff* do sistema após o uso, e que consiste num erro do próprio funcionário. Políticas e soluções de IAG/IAM (governança ou gestão de acesso e identidade) e o uso de metadiretórios são aliados importantes para resolver essas questões.
- Falha ao identificar e alterar as configurações-padrão do fornecedor – mais uma vez, aqui está um problema facilmente solucionável. Geralmente, os softwares e programas vêm com uma senha padrão por parte do fornecedor, mas nem sempre eles exigem que ela seja mudada logo durante o primeiro acesso. É necessário alterar a senha para não deixar a empresa exposta a criminosos que desejam roubar dados.
- Redução de escopo – algumas organizações querem reduzir o escopo das verificações de segurança, pois isso pode reduzir o custo, o tempo e o esforço para alcançar, manter e demonstrar a segurança. No entanto, vale lembrar que as empresas são responsáveis pelas informações dos clientes, não importa onde elas estejam (leia mais sobre as responsabilidades legais no item 2.5). Portanto, a ideia é ampliar o escopo das verificações para aumentar a segurança.
- Falha ao rastrear onde os dados são armazenados – não é incomum que as empresas não saibam onde os seus dados estão armazenados e qual o nível de proteção aplicado a esses dados. Frequentemente, o armazenamento é feito na nuvem, e alguns acreditam que a terceirização de armazenamento os isenta de responsabilidades. Na verdade, mesmo que a empresa terceirize o processamento para um fornecedor, ela ainda é responsável por conhecer e atestar onde e como os dados são armazenados, gerenciados e acessados. As empresas precisam saber se esses fornecedores estão suscetíveis a ataques cibernéticos que podem levar ao roubo ou vazamento dos dados.
- Falha na medição da eficácia da segurança cibernética – essa medição consiste no esforço executivo de avaliar e monitorar continuamente a eficácia das ações e de medir os investimentos em segurança cibernética. O trabalho de segurança e conformidade deve ser constante. Ao realizar os trabalhos de conformidade apenas para que a auditoria não constate falhas, a empresa deixa de perceber que, durante o restante do tempo, pode estar exposta e vulnerável a ataques cibernéticos.
- Desconsideração dos integrantes da cadeia de valor – em muitas em-

presas, há integração das cadeias de valor, ou seja, entre parceiros como fornecedores de insumos e matérias-primas e distribuidores dos produtos. Frequentemente, esses participantes da cadeia estão também integrados com o sistema da empresa. Com isso, há portas de acesso aos sistemas da empresa que não estão sob supervisão e controle das linhas de defesa dela, e que sim dependem dos parceiros. Especial atenção deveria ser dada a essa possível vulnerabilidade.

2.5 Proteção de dados pessoais e segurança cibernética

A emergência das preocupações com segurança e resiliência cibernética não é fruto apenas das ameaças de ataques que pairam sobre as empresas. Ela também resulta de mudanças no arcabouço jurídico. Vários países adotaram legislações que versam sobre proteção de dados pessoais e que já começam a provocar uma mudança cultural em relação ao tratamento de dados das pessoas físicas e à segurança aplicada a esses dados. Cabe às empresas proteger os dados pessoais de ataques cibernéticos que exporiam esses dados a terceiros não-autorizados.

2.5.1. Principais normas e estruturas relacionadas à segurança cibernética

As novas leis e normas são um motivo a mais para transformar a cultura das empresas, introduzindo a preocupação com segurança da informação de forma permanente na lista de prioridades.

No Brasil, a primeira lei a prever a proteção de dados foi o Marco Civil da Internet, de 2014. Em seguida, em 2018, vieram a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Decreto 9.637, que instituiu a Política Nacional de Segurança da Informação. O presente documento não pretende se aprofundar na LGPD e nem em outras normas e legislações referentes à segurança cibernética. Pelo fato de sofrerem contínua evolução, as normas aqui citadas devem ser consultadas diretamente em suas fontes. Também não devem ser consideradas a única fonte para a tomada de decisão.

O Marco Civil da Internet, Lei nº 12.965 de 23 de abril de 2014, estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil e determinou as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. Foi o Marco Civil que trouxe os princípios da proteção da privacidade, de dados pessoais, da responsabilização dos agentes de acordo com suas atividades, bem como instituiu a obrigatoriedade de se preservar a intimidade, a vida privada, a honra e imagem das pessoas quando da guarda e disponibilização dos registros de conexão e de acessos à internet. Dispôs ainda sobre a responsabilidade por danos decorrentes de conteúdo gerado por terceiros, gerando obrigatoriedade das empresas em se adequar para atender aos requisitos previstos na lei.

No Brasil, a mais importante lei a respeito da privacidade e proteção de dados pessoais veio em 2018 por meio da Lei Geral de Proteção de Dados Pessoais (LGPD, ou Lei 13.709/18, alterada pela Lei 13.853/19). Até a impressão deste documento, ela estava prevista para entrar em vigor em agosto de 2020, mas já requer adaptação e mudança cultural por parte das empresas. O principal aspecto da lei é o conceito de que os dados pertencem às pessoas, e não às empresas. Nesse sentido, nossa lei se assemelha à legislação europeia, a General Data Protection Regulation (GDPR), que começou a produzir efeitos em maio de 2018 – embora na União Europeia já houvesse uma diretiva, de 1995, sobre o tema.

A lei brasileira entende que os dados pessoais pertencem às pessoas naturais, mas que cabe aos responsáveis pelas diversas etapas dos tratamentos de dados protegê-los. Ela criou as figuras do operador, do controlador e do encarregado dos dados – e todos esses são responsáveis, em alguma medida, pela proteção dos dados pessoais sob sua tutela. Ao controlador competem as decisões referentes ao tratamento de dados pessoais. Já o operador realiza o tratamento dos dados pessoais em nome do controlador. O encarregado deve ser uma pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Esse órgão, criado em julho de 2019, tem como principais atribuições: zelar pela proteção dos dados pessoais, fomentar o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, fiscalizar e aplicar sanções em caso de descumprimento da lei. As três figuras – controlador, operador e encarregado – podem ser exercidas por pessoas naturais ou jurídicas.

Lei nº 13.853 de 08 julho de 2019, que alterou a LGPD (13.709/2018).

A lei define dado pessoal como informações relacionadas a pessoas naturais identificadas ou identificáveis.

Veja a definição que a lei traz para tratamento de dados: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

A LGPD cria a necessidade de comunicação, por parte das organizações, de vazamentos ou violações de dados pessoais para a ANPD. Portanto, além dos já conhecidos prejuízos advindos de incidentes cibernéticos – como a perda de confiança, o desgaste da imagem e as perdas decorrentes da paralisação das atividades – as empresas passam a estar sujeitas à comunicação desses incidentes e, também, a penalidades como multas de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, referente ao seu último exercício, e limitada a R$ 50 milhões, por evento de infração.

Algumas leis e normas se ocupam da segurança cibernética – assunto que não trata apenas de dados pessoais, mas de informações de uma forma geral englobando também a proteção da infraestrutura crítica da empresa (como os seus sistemas e equipamentos).

O Decreto 9.637 (26/12/2018) instituiu a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação. Ele é aplicável à administração pública federal. A segurança da informação inclui segurança e defesa cibernética, segurança física e proteção de dados organizacionais e ações para assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

Como o sistema financeiro é bastante sensível ao tema e, também, é fortemente regulado, conta com normas específicas sobre segurança cibernética. A Resolução 4.658, de 26/4/2018, do Conselho Monetário Nacional, e a Circular 3.909, de 16/8/2018, do Banco Central, dispõem sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem aplicáveis a instituições financeiras.

Há, ainda, estruturas e padrões de segurança que podem ser aplicados a setores específicos ou mesmo a empresas de vários setores, mas que não contam com a obrigatoriedade imposta pelas leis e normas. A indústria de meios de pagamento conta com o padrão obrigatório PCI-DSS: Payment Card Industry Data Security Standards (Padrão de Segurança de Dados da Indústria de Cartões de Pagamento).

3

Aspectos práticos da gestão de riscos cibernéticos

Dadas as diretrizes, por parte do conselho de administração, sobre riscos cibernéticos, caberá à diretoria a execução de programas e de políticas aplicáveis à resiliência cibernética. E, ao conselho, o monitoramento da condução dos programas de gestão de riscos cibernéticos. No entanto, como o conselho poderá saber se os programas estão implementados, são efetivos e estão alinhados com o apetite a riscos da organização? Buscando auxiliar os conselheiros a cumprir essa tarefa, neste capítulo examinaremos os componentes e aspectos práticos que os programas de gestão de riscos cibernéticos devem ter.

3.1. Por onde começar?

Uma boa forma de começar é realizar uma auto avaliação para entender o nível de maturidade da empresa no que diz respeito à gestão de segurança da informação, onde está inserido o risco cibernético.

O modelo de governança de gestão de riscos reflete o nível de maturidade da organização em relação às práticas adotadas de governança corporativa.

Existem distintas alternativas para a construção da governança de gestão de riscos e cada organização deverá desenhar aquela mais adequada ao seu perfil de negócio, cultura organizacional, modelo de gestão e nível desejado de maturidade em relação às suas práticas de gestão de riscos.

Desta forma, podemos destacar que o nível de maturidade em gestão de riscos em uma organização representa:

- as ações adotadas para alcançar suas metas e objetivos em relação à gestão de riscos e ao sistema de controles internos;
- o nível de esforço (tempo e investimento) empreendido para alcançar essas metas e objetivos;
- os resultados obtidos, a eficácia e a eficiência com as práticas implementadas;
- o nível de envolvimento dos profissionais em relação a essas práticas;
- o nível de entendimento da maturidade da organização, assim como das oportunidades de melhorias.

Em última instância, o nível de maturidade significa a compreensão de onde se está, de onde se quer chegar e de como se quer chegar lá.

3.1.1. Mensurando a maturidade

As organizações devem avaliar suas atuais capacidades em relação às práticas de gestão de riscos e compreender como e por que devem desenvolver melhorias que as preparem para implementar a estratégia de gestão de riscos estabelecida pelo conselho de administração. A avaliação do modelo de maturidade permitirá que organização possa documentar, comunicar e programar melhorias no seu modelo. Para tanto, devem ser levadas em conta suas principais ameaças (e de sua indústria ou segmento) e as regulamentações aplicáveis.

Existem alguns modelos de classificação do nível de maturidade da gestão de riscos, como o modelo de maturidade de Gerenciamento de Riscos Corporativos 🕮. Para efeito de gerenciamento de riscos cibernéticos, podemos dizer que as organizações podem ser classificadas em cinco estágios ou níveis de maturidade quanto à segurança da informação:

🕮 IBGC, *Gerenciamento em riscos corporativos: evolução em governança e estratégia*, 2017.

- Parcial – processo de informação *ad hoc* ou reativo. As prioridades de segurança da informação não são relacionadas aos riscos ou objetivos de negócio.
- Risco informado – o processo de gestão dos riscos de segurança da informação é aprovado, mas não estabelecido por toda organização.
- Repetitivo – a gestão do risco de segurança da informação é formalmente aprovada e formalizada por política. As práticas são relacionadas aos objetivos de negócio.
- Adaptativo – o processo de gestão de riscos de segurança da informação é continuamente aprimorado e incorpora as melhores práticas de mercado.

3.2. Ciclo de ações na gestão de riscos cibernéticos

A partir da constatação do estágio de maturidade, os executivos devem estabelecer ou aprimorar programas de gestão de risco condizentes com o apetite a risco e as diretrizes dadas pelo conselho.

Para estabelecer ou aprimorar o programa, uma das alternativas é utilizar a estrutura proposta pelo National Institute of Standards and Technology (NIST), órgão do Departamento de Comércio dos Estados Unidos, que traz diretrizes sobre a segurança cibernética. Ela é aplicável a organizações de todos setores, portes e níveis de segurança cibernética e visa reduzir os riscos por meio do aprimoramento

da gestão de riscos cibernéticos, de forma alinhada aos objetivos da empresa.

A estrutura é baseada em cinco conjuntos de temas, pilares ou "domínios" de ações que estruturam a gestão de risco cibernético: identificar, proteger, detectar, responder e recuperar. Cada um desses pilares, por sua vez, sugere ações, processos ou atividades específicas para avançar rumo à resiliência cibernética. Veremos, a seguir, o que cada um desses pilares engloba:

3.2.1. Identificar

Cada informação da empresa é um ativo, e o objetivo da gestão da segurança cibernética é proteger esses ativos. Tendo isso em mente, é importante primeiro saber quais são esses ativos – daí vem o primeiro pilar proposto pela estrutura do NIST, o de identificação. Além de especificar e nomear os ativos, esse "domínio" implica também em entender o contexto de negócios, estabelecer foco e priorizar esforços de acordo com a estratégia de gestão de riscos e necessidades do negócio.

Os pontos sobre os quais a empresa ou organização precisa identificar e entender nesse pilar são, de acordo com o NIST, os seguintes:

- gestão de ativos;
- ambiente de negócios;
- governança;
- avaliação de riscos;
- estratégia de gestão de risco;
- gestão de riscos da cadeia de suprimentos.

3.2.2. Proteger

Aqui, a ideia é desenvolver e implementar salvaguardas que garantam o funcionamento da empresa e seus principais serviços e processos. Por meio desses mecanismos de proteção, a empresa limita o efeito de ataques ou incidentes cibernéticos. Para tanto, ela precisa tomar iniciativas e ações referentes aos seguintes itens:

- gerenciamento de identidades, autenticação e controle de acesso;
- conscientização e treinamento;
- segurança de dados;
- processos e procedimentos de proteção da informação;
- manutenção;
- tecnologia de proteção.

3.2.3. Detectar

A detecção de incidentes cibernéticos – ou seja, a capacidade de desenvolver e implementar atividades para identificar esses eventos ou ataques – é fundamental para a resiliência cibernética. Nem sempre as empresas conseguem detectar esses eventos, o que amplia as potenciais perdas trazidas pelos mesmos. A estrutura do NIST propõe ações nas seguintes áreas relacionadas à detecção:

- anomalias e eventos;
- monitoramento contínuo de segurança;
- processos de detecção.

3.2.4. Responder

Uma vez detectado o evento ou incidente cibernético, entra em cena a capacidade de responder ao mesmo por meio do desenvolvimento e da implementação de atividades para conter o impacto do ataque. Para tanto, o NIST recomenda ações relativas aos seguintes tópicos:

- planejamento de respostas (plano de contingências);
- comunicações;
- análise;
- mitigação;
- melhorias.

3.2.5. Recuperar

Caso o evento ou incidente cibernético tenha causado danos, a recuperação busca restaurar serviços ou operações prejudicadas pelo ataque. Essa atividade de recuperação permite a volta às operações normais e contribui

para minimizar os efeitos do ataque. O NIST prevê as seguintes atividades relacionadas à recuperação:

- planejamento de recuperação;
- melhorias;
- comunicações.

Considerações finais

Como apresentado neste documento, a gestão do risco cibernético deve ser uma preocupação constante dos conselheiros de administração, uma vez que ela tem implicações na sustentabilidade das empresas. Ao conselho, cabe supervisionar a gestão de riscos cibernéticos e a salvaguarda dos ativos da empresa, evitando perdas de todos os tipos e danos à reputação. Sempre mantendo em mente que a gestão de riscos cibernéticos é parte da segurança da informação, que por sua vez deve estar inserida e alinhada às práticas de gestão de riscos da organização.

Vale destacar que essa preocupação não deve ser um entrave ao desenvolvimento da empresa, obstáculo que poderia existir se esses riscos fossem tidos como inviabilizadores de qualquer tipo de inovação. A resiliência cibernética, trazida por uma boa gestão dos riscos cibernéticos, contribui para que a empresa tenha mais segurança e qualificação para promover inovações e utilizar novas tecnologias.

Vale lembrar que essa resiliência é duramente conquistada, mas que pode ser perdida se não houver uma constante preocupação e atenção. A gestão de riscos cibernéticos deve estar permanentemente em pauta para que possa ser aprimorada e fazer face a novas táticas usadas pelos perpetradores de ataques. E nunca é demais ressaltar que o objetivo estratégico com segurança (de todos os tipos e, no caso, com a segurança cibernética) deve ser incorporada no dia a dia das empresas, de forma a permitir o crescimento e a sustentabilidade das mesmas.

Bibliografia

ACCENTURE. *Gaining ground on the cyber attacker – 2018 State of Cyber Resilience*, 2018. Disponível em: <https://www.accenture.com/_acnmedia/PDF-92/Accenture-810412-S-P-State-of-Cyber-Resilience-Survey-POV-v3-0-fins.pdf>. Acesso em: 4 jul. 2019.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, agosto de 2018.

DELOITTE. Riscos Cibernéticos e Segurança da Informação na América Latina e Caribe - Tendências 2019. Mar. 2019. Disponível em: <https://www2.deloitte.com/br/pt/pages/risk/articles/cyber-survey-2019.html>. Acesso em: 4 jul. 2019.

IOSCO (INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS). *Cyber Security in Securities Markets – An International Perspective Report on IOSCO's cyber risk coordination efforts*, 2016. Disponível em: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf>. Acesso em: 4 jul. 2019.

IBGC (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA). *Integração da gestão de riscos cibernéticos nas três linhas de defesa*. São Paulo, IBGC, 2018 (série *IBGC Análises & tendências*, n. 4). Disponível em: <https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=23839>. Acesso em: 7 out. 2019.

_____. *Gerenciamento em riscos corporativos: evolução em governança e estratégia.* São Paulo, IBGC, 2017 (série Cadernos de Governança Corporativa, n. 19).

ISO (International Organization for Standardization). *Norma ISO/IEC 27.000:2018*. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=385777>. Acesso em: 7 out. 2019.

_____. *Norma ISO/IEC 27.032:2015*. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=385777>. Acesso em: 7 out 2019.

National Institute Of Standards And Technologies. *Framework for Improving Critical Infrastructure Cybersecurity,* 2018. Disponível em: < https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11>. Acesso em: 7 out. 2019.

Ponemon Institute. *Cost of cyber crime study 2017 – Insights on the security investments that make a difference*, 2017. Disponível em: <https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf>. Acesso em: 4 jul. 2019.

Verizon. *Data Breach Investigations Report*, 2018. Disponível em: <https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf>. Acesso em: 4 jul. 2019.

Verizon. *Data Breach Investigations Report*, 2019. Disponível em: <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>. Acesso em: 4 jul. 2019.

World Economic Forum. *The Global Risks Report 2019*. Disponível em: <http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf>. Acesso em: 7 out. 2019.

Anexo – Glossário

- **Ataque cibernético –** Tentativas de comprometer a confidencialidade, integridade, disponibilidade de dados ou sistemas computacionais.
- **Autoridade Nacional de Proteção de Dados (ANPD) –** Órgão criado pela Lei nº 13.853 de 08 julho de 2019, que alterou a LGPD (13.709/2018). Ele tem como missão zelar pela proteção dos dados pessoais, fomentar o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, fiscalizar e aplicar sanções em caso de descumprimento da LGDP.
- **Botnet –** Termo oriundo da junção das palavras *robot* e *network*, e que designa um tipo de *malware* que afeta as empresas por meio do roubo das credenciais dos usuários para posterior uso nos sistemas da empresa, ou torna as máquinas afetadas pelo *malware* espécies de zumbis que executam tarefas relacionadas a outros ataques cibernéticos. De acordo com a definição da ISO 27.032, *botnet* é um "software de controle remoto, especificamente uma coleção de bots mal-intencionados, que funcionam de forma autônoma ou automática em computadores comprometidos."
- **Chief Information Officer (CIO) –** Profissional responsável pela tecnologia da informação dentro de uma empresa.
- **Chief Information Security Officer (CISO) –** Profissional responsável pela segurança da informação dentro de uma empresa.
- **Chief Risk Officer (CRO) –** Professional responsável pela gestão de riscos dentro de uma empresa. A depender da estratégia da mesma, ele também pode exercer as funções do CISO e ser responsável pela segurança da informação.

- **Confidencialidade –** É uma das propriedades do Sistema de Gestão de Segurança da Informação (SGSI). Ela pressupõe a autorização para que indivíduos, entidades ou processos tenham acesso a dados e informações.
- ***Dark web* –** É uma parte da deep web, encriptada e que requer softwares específicos para o acesso. Geralmente é usada para atos criminosos, como venda de armas e drogas, pedofilia infantil e troca de informações entre invasores, entre outros.
- ***Deep web* –** Parte não visível da internet, que não requer a instalação de programas específicos para navegação. Seu conteúdo não pode ser acessado por mecanismos de busca tradicionais, pois suas páginas não são indexadas.
- **Disponibilidade –** É uma das propriedades do Sistema de Gestão de Segurança da Informação (SGSI). Pressupõe que dados e informações estejam acessíveis e possam ser utilizados por entidades autorizadas.
- **Ethical Hacking Tests (EHT) –** Testes que avaliam o grau de segurança técnica de um sistema ou rede por meio da simulação de um ataque cibernético.
- **General Data Protection Regulation (GDPR) –** Lei europeia que versa sobre proteção de dados pessoais. Ela trabalha com o conceito de que os dados pertencem às pessoas e não as empresas. Começou a produzir efeitos em maio de 2018.
- **Hacktivistas –** Como a origem do nome sugere, hacktivista vem da junção das palavras *hacker* e ativista. São os invasores que promovem ataques cibernéticos, motivados por suas visões de mundo ou com finalidades política e social.
- **IAG/IAM –** IAM (Identity and Access Management) é a plataforma/ferramenta voltada à segurança da informação que visa administrar os acessos à determinado serviço, sistema, plataformas. IAG (Identity and Access Governance) refere-se à governança de identidade e acesso, que engloba um processo de requisição, aprovação, certificação, auditoria dos acessos às aplicações, dados, ferramentas e outros serviços da área de TI. Os IAG/AIM visam autenticar os usuários que terão acesso e utilizarão determinado serviço, plataforma de TI, monitorando e controlando estes acessos.
- **Incidente de segurança ou incidente cibernético –** "Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores", de acordo com definição do CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Alguns exemplos são o uso, acesso ou modificações não autorizadas em um sistema; ataques de negação de serviço; o desrespeito à política de segurança ou uso de uma empresa.
- **Integridade –** É uma das propriedades do Sistema de Gestão de Segurança da Informação (SGSI). Ela pressupõe que os ativos e dados serão salvaguardados com exatidão e completeza.
- **Invasor –** Pessoa que conhece profundamente softwares, redes de computadores e computadores, e que usa esse conhecimento de forma ilegal para provocar vazamentos de dados ou violações de dados. Em inglês, o termo equivale ao *cracker.* Ele se contrapõe ao *hacker*, palavra que tem sentido positivo, pois se refere a pessoas que também contam com conhecimento profundo, mas que podem contribuir para o aperfeiçoamento dos sistemas ou que não usam suas habilidades para causar danos.
- **Lei Geral de Proteção de Dados Pessoais (LGPD) –** Lei 13.709/18, alterada pela Lei 13.853/19). Ela considera que dados pessoas pertencem a pessoas, e não a empresas, e que cabe aos responsáveis pelas diversas etapas dos tratamentos de dados protegê-los. Ela também cria a necessidade de comunicação, por parte das organizações,

de vazamentos ou violações de dados pessoais para a ANPD e impõe penalidades como multas de até 2% do faturamento da pessoa jurídica.

- *Malicious code* – É um código dentro de algum sistema ou software, e que visa causar danos no sistema ou vazamentos de dados.
- *Malicious* insider – Funcionários, trabalhadores temporários e até parceiros que realizam intencionalmente ataques cibernéticos para roubar dados, destruir dados/informações e manusear inadequadamente as informações.
- *Malware* – Termo que vem da junção das palavras *malicious* software. É um software que embarca conteúdo malicioso. Pode comprometer o ambiente das organizações pelo roubo de informações ou pelo fechamento do ambiente, entre outras técnicas. Pela definição da ISO 27.032, *malware* é um "software criado com más intenções contendo características ou capacidades que podem potencialmente causar danos diretos ou indiretos para o usuário e/ou para o sistema de computador do usuário". Exemplos são vírus, *worms* e trojans.
- Marco Civil da Internet – Lei nº 12.965 de 23 de abril de 2014, que apresenta normas, garantias, princípios, direitos e deveres para a utilização da internet no Brasil, seja por usuários ou por empresas, provedores de conexão e provedores de internet. A proteção da privacidade, de dados pessoais e a responsabilização dos agentes, conforme as suas atividades, são exemplos práticos das dimensões cobertas pela lei.
- Metadiretórios – Também conhecido pelo termo "gerenciamento de identidades e acesso". Consiste num repositório central de usuários, no qual consta a identidade de cada pessoa, os sistemas a que ela tem acesso, seu *login* e data de criação ou revogação do mesmo etc.
- National Institute of Standards and Technology (NIST) – Órgão do Departamento de Comércio dos Estados Unidos que dispõe de uma estrutura com diretrizes sobre a segurança cibernética. A estrutura (*framework*) é baseada em cinco conjuntos de temas, pilares ou "domínios" de ações que estruturam a gestão de risco cibernético: identificar, proteger, detectar, responder e recuperar.
- *Patches* – Atualizações dos softwares feitas para corrigir falhas de segurança ou vulnerabilidades.
- *Phishing* – É um processo fraudulento de tentativa de adquirir informações particulares ou confidenciais, passando-se por entidades confiáveis em uma comunicação eletrônica. Exemplos práticos consistem no envio de mensagens de e-mails contendo anexo e links, ou mesmo um link em um website, uma mensagem por SMS no telefone celular, entre outros.
- *Ramsomware* – Tática usada pelos invasores que consiste no sequestro do acesso ao computador ou aos seus dados, via instalação de algum *malware*. Para que o usuário possa voltar a usar o equipamento ou acessar os dados, tem de efetuar algum pagamento para os invasores.
- Resiliência cibernética – Capacidade de uma empresa ou organização resistir a ataques cibernéticos e de se recuperar rapidamente caso o ataque seja bem-sucedido. A resiliência é obtida por meio da implantação de controles para prevenir, detectar e gerenciar os ataques, e está relacionada também à cultura de segurança cibernética.
- Risco cibernético – Segundo a International Organization of Securities Commissions (IOSCO), o risco cibernético refere-se aos potenciais resultados negativos associados a ataques cibernéticos.

PATROCÍNIO

Deloitte.

A Deloitte, com seus 312 mil profissionais em todo o mundo, lidera a transformação de negócios e digital, gerando impactos que realmente importam em empresas de todos os setores. Dentro de nosso portfólio abrangente de soluções, está um conjunto de serviços de gestão de riscos cibernéticos, reconhecidos mundialmente pela excelência na aplicação de tecnologias de ponta e abordagens inovadoras. No Brasil, a prática de gestão de riscos cibernéticos da Deloitte é robusta e atende a todos os desafios das organizações nessa área.

Acesse mais em www.deloitte.com.br.

EDIÇÃO

IBGC | Instituto Brasileiro de Governança Corporativa

PATROCÍNIO

Deloitte.

Agência Brasileira do ISBN
ISBN 978-85-99645-80-2
9 788599 645802

"A gestão do risco cibernético deve ser uma preocupação constante dos conselheiros de administração, uma vez que ela tem implicações na sustentabilidade das empresas. Ao conselho, cabe supervisionar a gestão de riscos cibernéticos e a salvaguarda dos ativos da empresa, evitando perdas de todos os tipos e danos à reputação. Sempre mantendo em mente que a gestão de riscos cibernéticos é parte da segurança da informação, que por sua vez deve estar inserida e alinhada às práticas de gestão de riscos da organização".