Outubro 2018

Como lidar com a supervisão de riscos cibernéticos?

As empresas sofrem ataques constantes, por isso é crucial que adotem medidas adequadas para a segurança cibernética e a proteção da privacidade de dados.

Riscos cibernéticos e proteção de dados são temas que exigem atenção dos conselheiros. Há diversas dimensões a serem avaliadas nessas áreas e muito tem sido feito pelas empresas em relação a esses assuntos. No desempenho de sua função de supervisão de riscos estratégicos, o conselho de administração deve atuar no direcionamento das ações e na aprovação dos investimentos necessários para a segurança da organização. Nesta publicação, delineamos o ambiente de ameaças e destacamos os principais pontos para uma boa interação entre o conselho e a administração a respeito desses temas. Apresentamos também sugestões de medidas concretas para conselhos e comitês aprimorarem sua atuação nessas áreas complexas e dinâmicas.

pwc

Apresentação

Empresas de todos os países e segmentos estão investindo fortemente no uso de tecnologias emergentes para crescerem em um mundo interconectado. Cada vez mais operam em ecossistemas digitais, interagindo e compartilhando informações críticas com clientes, fornecedores e parceiros de negócio. À medida que aumentam as suas conexões e a sua exposição às novas tecnologias, as organizações ficam mais vulneráveis aos riscos relacionados à segurança e à privacidade de dados.

Nesse contexto, monitorar e avaliar as ameaças e as medidas de proteção e remediação a serem adotadas pela administração das empresas deve ser preocupação permanente dos conselhos de administração.

Esta publicação tem como objetivo contribuir para a reflexão dos conselheiros sobre a relevância desse tema para a sustentabilidade das empresas. Procuramos também apresentar ideias práticas que os ajudem a exercer, de maneira eficaz, o seu papel na supervisão desses riscos estratégicos e dos esforços das organizações em relação à segurança cibernética e à proteção da privacidade de dados.

Marco Castro
Sócio e líder de Auditoria
PwC Brasil

Fábio Cajazeira
Sócio e líder de Clientes e Mercados
PwC Brasil

Introdução

Ataques cibernéticos com impactos operacionais, financeiros e reputacionais significativos são cada vez mais frequentes. Episódios relevantes de vazamento de informações pessoais ou corporativas crescem de forma assustadora em todo o mundo. Os sequestros de dados por meio de *ransomware*, com o propósito de negociar pagamentos de resgates, inclusive por meio de criptomoedas, para a "liberação dos dados" se tornaram uma realidade em todos os segmentos empresariais.

As inovações digitais não param de surgir e, com elas, os movimentos de transformação dos hábitos dos consumidores e dos modelos de negócio. À medida que os processos produtivos da indústria 4.0 incorporam novas tecnologias, como IoT (*Internet of Things*), robotização, inteligência artificial, *machine learning*, *blockchain* e drones, cresce o ecossistema digital das empresas e se amplia a superfície de ataque cibernético nos ambientes de TI e TO (Tecnologia da Informação e Tecnologia de Operação).

Outros casos relevantes de vazamento de dados têm acontecido com a exploração de modelos de negócios digitais não devidamente projetados em termos de segurança e proteção de dados. Os avanços em *analytics e Big Data* ampliaram a capacidade das empresas de inovar e criar modelos de negócios. De fato, melhorar a experiência dos consumidores, oferecer serviços e produtos sob medida ou monetizar dados exige análises estatísticas sofisticadas e intensa coleta de dados pessoais sobre hábitos de consumo, comportamentos e relacionamentos.

Não por acaso, as ameaças cibernéticas estão entre as quatro principais preocupações dos líderes empresariais em todo o mundo, de acordo com a *21ª Pesquisa Anual Global com CEOs*, realizada pela PwC. E o ritmo das violações cibernéticas segue aumentando, em parte porque há muita facilidade para aqueles que promovem os ataques.

Os colaboradores são alvos e vítimas de esquemas de *phishing* sofisticados e, muitas vezes, por negligenciarem políticas e procedimentos de segurança, utilizam senhas "fracas", ignoram atualizações de segurança (*patches*) e mantêm hábitos pouco seguros de navegação em e-mails e redes sociais, entre outros.

Pessoas e organizações conectadas a qualquer hora e em qualquer lugar são características do mundo digital que exige que as empresas tenham programas estruturados de segurança cibernética e proteção de dados. Nem sempre, porém, as empresas fazem os investimentos suficientes e necessários em segurança cibernética e proteção de dados ou tomam medidas corretivas quando os problemas já estão instalados.

A natureza das ameaças cibernéticas também está evoluindo. O ataque autopropagado *WannaCry*, por exemplo, é capaz de infectar computadores mesmo sem o usuário clicar em um link. De fato, os últimos dois anos foram marcados por vários casos de sequestro de dados (*ransomware*) que paralisaram sistemas de computação e mantiveram empresas inoperantes (offline) durante semanas.

Apesar da crescente propagação das ameaças e dos ataques, 44% dos 9.500 executivos entrevistados na Pesquisa Global de Segurança da Informação da PwC (*2018 PwC Global State of Information Security® Survey*) afirmam que ainda não definiram uma estratégia para a área de segurança da informação. Isso mostra quanto trabalho as empresas ainda precisam desenvolver nessa direção.

Governos, autoridades públicas, reguladores, empresários e consumidores estão cada vez mais atentos aos riscos cibernéticos e exigentes em relação à prontidão das empresas em termos de segurança cibernética e proteção de dados, bem como à capacidade de identificação, reação, apuração e comunicação de incidentes de segurança cibernética ou vazamento de dados e seus respectivos impactos. Com a recente aprovação da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018 – o Brasil se juntou a diversos países que já têm legislação sobre o tema, como os que integram a União Europeia.

A LGPD trará implicações para a sociedade e para as empresas privadas e públicas no Brasil, que, além de reverem suas políticas de tratamento de dados pessoais, deverão rever seus sistemas, processos e, inclusive, seus modelos de negócios baseados em *analytics* e monetização de dados.

Ameaças cibernéticas são motivo de grande preocupação

Os custos dos danos causados pelo crime cibernético podem chegar a US$ 6 trilhões ao ano até 2021 (em 2015 ficou na casa dos US$ 3 trilhões).

Fonte: *Cybersecurity Ventures*, 2017 *Cybercrime Report*, outubro de 2017.

Desafios que os conselheiros enfrentam na supervisão do risco cibernético

Desafios	*Ações do conselho*
Desafio: Como o conselho pode monitorar o nível de prontidão da empresa em relação aos riscos cibernéticos e seu estado de resiliência cibernética? Como avaliar se o programa de segurança cibernética estabelecido reduz a exposição a riscos de ataque ou de violação de dados a níveis aceitáveis?	***Ação do conselho:*** Concentrar-se em obter informações corretas e completas, por meio de um painel de controle executivo, e construir relacionamentos com os líderes de tecnologia, de segurança cibernética e com o responsável pela proteção de dados pessoais da empresa, para ter uma visão completa sobre a suficiência das ações da administração e o nível de resiliência cibernética e de proteção de dados da empresa.
Desafio: A empresa sofre muitas tentativas de ataque? Quantos ataques e vazamentos de dados se concretizam? Qual é a origem e a natureza desses ataques e vazamentos? Enfim, como os conselheiros podem avaliar se a empresa está preparada para lidar com violações de segurança e de proteção de dados da maneira adequada?	***Ação do conselho:*** Analisar regularmente o plano de gestão de crises, considerando o cenário de ataques cibernéticos ou de vazamento de dados, seja pela análise dos resultados de casos reais, seja pelas lições aprendidas com os testes de efetividade realizados pela administração.

Desafio do conselho

Como o conselho pode monitorar o nível de prontidão da empresa em relação aos riscos cibernéticos e seu estado de resiliência cibernética? Como avaliar se o programa de segurança cibernética estabelecido reduz a exposição a riscos de ataque ou de violação de dados a níveis aceitáveis?

Muitos conselheiros ainda não estão plenamente confiantes na efetividade dos controles sobre ameaças cibernéticas. Recente pesquisa anual realizada pela PwC com conselheiros de empresas mostra que somente:

39%

deles estão muito seguros de que a empresa identificou claramente seus ativos digitais mais valiosos e confidenciais.

1/4

desses conselheiros têm pouca ou nenhuma confiança de que suas empresas mapearam os potenciais atacantes.

É evidente que existem diversas variáveis envolvidas e que a administração precisa dar o encaminhamento adequado.

Muitas empresas alinham seus programas e investimentos com uma estrutura de segurança cibernética a fim de assegurar que estejam abordando todos os aspectos relevantes.

Para supervisionar os riscos cibernéticos de forma adequada, o conselho precisa ter as informações corretas e completas sobre como a organização aborda esses riscos.

Entretanto,

63%

dos conselheiros afirmam não ter certeza de que a empresa está fornecendo ao conselho métricas adequadas de segurança cibernética.

Os conselhos também destinam pouco tempo para discutir os riscos cibernéticos. Em geral, as agendas dos conselhos dedicam relativamente pouco tempo ao assunto.

A *Pesquisa Global de Segurança da Informação 2018* da PwC revela que muitos conselhos ainda consideram riscos cibernéticos e proteção de dados um tema de TI.

O estudo aponta também que, no Brasil,

73%

das companhias indicam que a prioridade de investimento em segurança cibernética deve ser o programa de transformação digital dos negócios.

Outra questão importante é que poucos conselhos têm membros capacitados em temas como inovação tecnológica, segurança cibernética e proteção de dados. Esse fato amplia as dificuldades para avaliar se a administração está realmente fazendo o necessário e suficiente para lidar com essa área de risco significativo.

Por que a segurança cibernética falha com frequência nas empresas?

Situação	*Caminho estratégico*
Não existe inventário dos ativos digitais da empresa	Para definir a adequada proteção dos ativos digitais da empresa, é preciso identificá-los e classificá-los de acordo com o grau de criticidade estratégica, tática e operacional para o negócio. A administração deve estar apta a explicar quais informações e dados ela possui, por que são necessários, o nível de criticidade estratégica, onde eles se encontram e como são tratados (Ex.: dentro dos sistemas da empresa ou por terceiros) e a que nível de proteção estão submetidos. Essa análise deve revelar quais dados são os mais críticos e valiosos ("as joias da coroa") e orientar níveis de proteção diferenciados.
A empresa não consegue determinar com precisão com quais terceiros ela mantém conexão digital ou compartilha informações	De forma geral, as empresas operam em um ecossistema digital, interagindo e compartilhando informações críticas com milhares de clientes, fornecedores e parceiros de negócios. Quase sempre, o objetivo dos hackers é explorar vulnerabilidades nos integrantes desse ecossistema, buscando estabelecer uma porta de entrada para a rede da empresa que é alvo do ataque. Há empresas que mantêm um programa estruturado de certificação independente em segurança cibernética para fornecedores e parceiros de negócio. No entanto, mais da metade das organizações não têm um inventário abrangente dos terceiros com quem elas compartilham informações confidenciais.
A empresa não tem visão do perfil e dos prováveis grupos cibernéticos que podem ter interesse na execução de ataques direcionados	Compreender quem são os potenciais atacantes ajuda a empresa a atuar preventivamente e definir de modo mais preciso sua estratégia e seu programa de cibersegurança. Do ponto de vista tático, isso ajuda a definir as ações e os mecanismos de prevenção e a planejar ações críticas na iminência de um ataque. No plano operacional, ajuda a definir e testar as ações de gestão de crise, de continuidade de negócios, de resposta a incidentes e de investigação da violação. Os serviços de inteligência de ameaças cibernéticas, de modelagem preditiva e de gerenciamento contínuo de segurança são fundamentais para ampliar essa compreensão de maneira sistemática.
Os fundamentos de segurança cibernética da empresa são fracos	Sistemas que não são configurados ou desenvolvidos de maneira adequada são mais vulneráveis a ataques. Por isso, é essencial adotar boas práticas de proteção, como autenticação multifator, desenvolvimento seguro (*DevSecOps*) e gestão de *patches*. É preciso também remover dos sistemas de forma tempestiva os colaboradores que se desligam ou se afastam do emprego. Não menos importante, o acesso privilegiado deve ser controlado de forma preventiva, com o uso até mesmo de métodos de identificação de operações "fora do padrão" e de tecnologia de *User Behavior Analytics*.

Situação	*Caminho estratégico*
A empresa não corrige vulnerabilidades conhecidas do sistema	Novas vulnerabilidades de sistemas são constantemente descobertas, mas nem todas as empresas de software divulgam para os clientes as correções disponíveis. A organização precisa ter certeza de que existe um procedimento para monitorar regularmente atualizações de *patches* disponíveis e confirmar se essas correções foram feitas. Os alertas de ameaças dos serviços de inteligência facilitam a gestão integrada das vulnerabilidades conhecidas.
A empresa tem uma ampla superfície de ataque	Ampliar as formas de acesso aos sistemas da empresa melhora a experiência de colaboradores, clientes e terceiros – mas a dos hackers também. Por isso, as empresas precisam de arquiteturas de segurança mais robustas, controles eficientes e operantes e sensores de segurança bem calibrados. A concessão de acessos privilegiados a sistemas e dispositivos sem controles rígidos, ou sem alinhamento com as matrizes de risco e segregação de funções, amplia os riscos de acesso indevido. É preciso aumentar o monitoramento de atividades suspeitas.
Os colaboradores não são treinados em suas funções em relação à segurança da informação e à proteção de dados	Colaboradores são a maior fonte de incidentes de segurança – intencionais ou não. Ainda assim, somente metade (52%) dos executivos afirma que suas empresas têm um programa de treinamento para conscientizar os colaboradores sobre a importância da segurança.
Terceiros e parceiros de negócio não recebem orientação formal sobre os cuidados em segurança da informação e proteção de dados esperados na relação com a empresa	Prestadores de serviços e terceiros precisam receber orientações básicas sobre as políticas de segurança da informação que devem seguir em seu relacionamento com a empresa.
Os clientes muitas vezes desconhecem as diretrizes gerais de segurança da informação e proteção de dados	É recomendável fazer uma comunicação geral aos clientes sobre o compromisso da empresa com a segurança da informação e a proteção de dados. Órgãos reguladores, como o Banco Central do Brasil, solicitam essa comunicação de maneira explícita.
A segurança cibernética é vista como responsabilidade exclusiva do diretor de TI (CIO) ou do diretor de Segurança da Informação (CISO)	O CIO ou o CISO não devem realizar o trabalho sozinhos. Outros executivos de TI, Marketing, RH, Jurídico, Financeiro, Digital e Operações devem cooperar e fornecer recursos para tratar das questões de riscos cibernéticos. De fato, todos na organização devem contribuir para a proteção dos ativos digitais. A segurança cibernética e a proteção de dados devem ser contempladas em todas as linhas de defesa da organização e permear as discussões e o trabalho “do conselho até a operação”.

Situação	*Caminho estratégico*
Questões de riscos cibernéticos e de proteção de dados pessoais não foram consideradas nos processos de *due dilligence* para aquisições	Fragilidades nas práticas de uma determinada organização em relação à gestão dos riscos cibernéticos e à proteção de dados pessoais pode ser um ponto importante de atenção em processos de fusão e aquisição. Os processos de *due diligence* podem identificar informações a esse respeito.
A empresa ainda não designou o responsável pela proteção de dados conforme exigido pela LGPD (Lei Geral de Proteção de Dados)	A LGPD determina a designação do responsável pelo tratamento de dados, cujas funções são: i) receber reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar as providências cabíveis; ii) receber comunicações da autoridade nacional e adotar providências; iii) orientar funcionários e contratados da empresa a respeito das práticas a serem adotadas em relação à proteção de dados pessoais; e iv) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
A jornada de conformidade com as regulações setoriais ou com a legislação de proteção de dados não tem tido a prioridade ou os investimentos adequados	Os reguladores estão cada vez mais atentos à capacidade das empresas de tratar os riscos cibernéticos, definir uma política de segurança cibernética ampla e ter um plano efetivo e testado de resposta a incidentes cibernéticos ou vazamento de informações. O regulador do setor de instituições financeiras no Brasil vai além, disciplinando os controles de contratação de serviços de computação e armazenamento de dados em nuvem. A LGPD estabelece responsabilidades e multas para empresas e seus administradores por descumprimento da lei, além de abrir a possibilidade de reclamações individuais ou coletivas no âmbito da Lei de Proteção ao Consumidor. A jornada de conformidade com a regulação deve estar claramente definida e os investimentos necessários aprovados pela administração e pelo conselho.

Ação do conselho

Concentrar-se em obter informações corretas e completas por meio de um painel de controle executivo e construir relacionamentos com os líderes de tecnologia, de segurança cibernética e com o encarregado de proteção de dados pessoais da empresa, para ter uma visão completa da suficiência das ações da administração e do nível de resiliência cibernética e de proteção de dados da empresa.

Essa é uma área em que a supervisão é desafiadora. Listamos a seguir várias perguntas que facilitam a abordagem do assunto.

1. Considerando que a segurança cibernética e a proteção de dados são questões críticas, todo o conselho deveria supervisioná-las?

Metade dos conselheiros afirma que o comitê de auditoria é responsável pelo risco cibernético, enquanto 16% o deixam a cargo de um comitê de risco separado ou de um comitê de TI independente. Somente 30% dizem que essa responsabilidade é do conselho como um todo.[1] Se a decisão for não atribuir ao conselho como um todo a função de supervisionar o risco cibernético e a proteção de dados, seus membros devem se assegurar de que o comitê designado para assumir esse papel, no mínimo, forneça relatórios regulares e abrangentes de posicionamento para todo o conselho. É necessário também avaliar a criação de comitês de especialistas no tema para apoiar os trabalhos dos comitês de auditoria e do conselho.

2. O nosso conselho precisa de mais capacitação em segurança cibernética, em proteção de dados ou em inovação tecnológica?

Algumas empresas podem optar por nomear um conselheiro com conhecimento de segurança cibernética e proteção de dados. Outras podem escolher ir por caminho diferente. Encontrar pessoas que reúnam esses conhecimentos talvez seja desafiador, especialmente porque há carência de pessoas experientes nesse mercado e a evolução tecnológica é cada vez mais rápida. Alguns conselhos podem não ter lugar para mais um membro. Outros talvez não queiram admitir alguém com essa capacitação específica, a menos que tenham certeza de que a pessoa também será capaz de tratar de outros assuntos. Dessa forma, eles procuram maneiras diferentes de tratar essa deficiência, o que inclui a educação continuada e o apoio de consultores externos.

[1] PwC, 2017 Annual Corporate Directors Survey (Pesquisa Anual realizada em 2017 pela PwC com Conselheiros de Empresas), outubro de 2017.

3. Quais são os papéis e as responsabilidades corporativas?

A discussão sobre segurança cibernética e proteção de dados deve incluir líderes de negócios, tecnologia, área jurídica, RH, gestão de risco, encarregado de proteção de dados, além do CEO e do CFO. Por quê? Por um lado, essa postura transmite a mensagem de que a segurança cibernética e a proteção de dados são questões que envolvem toda a empresa e que os conselheiros esperam que todos sejam responsáveis pela gestão dos riscos associados. A discussão também pode expor outras áreas em que haja falhas na segurança ou na proteção de dados. Por exemplo, o CISO inclui com frequência o departamento de TI em seus relatórios. Contudo, muitas organizações industriais também precisam proteger o departamento de TO, cuja responsabilidade é fazer a gestão da tecnologia aplicada a plantas físicas ou processos produtivos e logísticos. Assim, se o CISO não incluir o TO, o conselho precisará receber informações situacionais de quem quer que esteja monitorando os riscos cibernéticos da TO. Outro exemplo é a prática de *privacy by design*, que considera que exigências legais e regulatórias sejam levadas em conta desde a concepção das iniciativas de inovação conduzidas na empresa.

4. Temos as informações necessárias para supervisionar o risco cibernético e a proteção de dados?

Em primeiro lugar, é preciso avaliar se foram disponibilizadas as informações básicas necessárias sobre o ambiente de TI e TO, o ecossistema interconectado, o mapeamento de ativos digitais e informações críticas e o nível de terceirização existente. Sem essas informações, é difícil avaliar o nível de risco e de resiliência cibernética associados. Algumas áreas principais são descritas a seguir.

Os conselheiros veem uma necessidade clara de mais expertise sobre segurança cibernética e proteção de dados em seus conselhos.

72%
dizem que seu conselho precisa dessa expertise

33%
dizem que não têm essa expertise e precisam dela

39%
dizem que têm, mas precisam de mais conhecimento

Fonte: PwC, 2017 Annual Corporate Directors Survey, outubro de 2017.

Perguntas úteis para avaliação da maturidade do ambiente de segurança cibernética e de privacidade de dados

Sistemas e aplicativos da empresa

- Os sistemas legados foram desenvolvidos internamente ou comprados e customizados? Rodam em instalações próprias, terceirizadas ou estão em nuvem? Todos ainda recebem suporte do fabricante?
- A nova plataforma de desenvolvimento é ágil? Em que medida as fábricas de desenvolvimento são próprias ou de fornecedores de software?
- Como a prática de desenvolvimento seguro de aplicativos está integrada na plataforma ágil?
- Como os requisitos de proteção de dados da LGPD estão incorporados na dinâmica de desenvolvimento ágil?
- Que requisitos de segurança foram exigidos na contratação de serviços de processamento e armazenamento de dados e de computação em nuvem?
- A empresa está executando várias versões dos sistemas principais em diferentes departamentos?
- Até que ponto a empresa integrou os sistemas das empresas que adquiriu?
- Como é feita a gestão de acesso aos sistemas? E a concessão de acessos privilegiados aos sistemas, banco de dados e redes?
- Como é protegida a privacidade das informações de funcionários, clientes, fornecedores, terceiros, entre outros, que são tratadas pelos sistemas da companhia?

Fundamentos e recursos de segurança

- Há um programa de segurança cibernética e de proteção de dados?
- Quem tem a responsabilidade pela segurança cibernética na empresa? E pela proteção de dados?
- A política de segurança cibernética e o plano de ação de resposta a incidentes cibernéticos estão definidos, implantados e divulgados?
- Qual o nível de experiência profissional da equipe de segurança? Que *gaps* de competência técnica e gerencial existem? Podem ser complementados por *headcount* ou por consultoria externa?
- Quais são os principais objetivos anuais da segurança cibernética? O orçamento para a área é adequado e suficiente? Está de acordo com referências de Opex e Capex do setor?
- A empresa adota *frameworks* de segurança cibernética? Ex.: National Institute of Standards and Technology (NIST), ISO 27001, Information Security Forum (ISF), Control Objectives for Information and Related Technologies (CobIT) e International Electrotechnical Commission (IEC 62443-3.1).
- Os riscos cibernéticos de TI e de TO são analisados de maneira convergente e recebem a atenção necessária da administração?
- As iniciativas de inovação e transformação digital da empresa consideram desde o início os temas de riscos cibernéticos e proteção de dados (*cyber & privacy by design*)?
- Os processos de *due diligence* consideram os temas de riscos cibernéticos e privacidade de dados da empresa-alvo?

Como esse tipo de informação básica não muda muito, é provável que os conselheiros precisem apenas de reciclagens periódicas. Por outro lado, convém que os conselheiros recebam com mais frequência relatórios sobre o que realmente muda. Cada empresa precisa definir quais itens – quantitativos e qualitativos – são mais relevantes.

Também é útil que os conselheiros sejam informados pela administração se esta acredita que o risco cibernético e a exposição de dados pessoais estão aumentando, permanecem estáveis ou estão diminuindo. Um *dashboard* adequado fornece aos conselheiros entendimento imediato da situação do risco cibernético e da proteção de dados da empresa.

Existem várias formas diferentes de montar um *dashboard* executivo. Uma delas é simplesmente classificar as questões como fatores externos e internos, conforme exemplificado a seguir. Os conselheiros devem avaliar se o *dashboard* apresenta uma descrição completa e precisa.

Exemplo de como um dashboard *deve ser apresentado*

Tipo de medida	*Classificação do risco*	*Tendência*
Panorama da ameaça externa • Informações sobre o nível de ameaça do setor. • Número de vulnerabilidades de segurança cibernética identificadas publicamente que surgiram desde o último relatório. • Natureza dos principais eventos cibernéticos nos noticiários. • Fatores geopolíticos (p.ex., atividade por países etc.).		 ***Nível de risco aumentando***
Situação dos programas internos • Percentual de sistemas que cumprem as normas de segurança e de proteção de dados da empresa. • Tempo médio para identificar um evento de violação da segurança ou da proteção de dados. • Tempo médio para corrigir vulnerabilidades conhecidas. • Situação dos principais trabalhos de correção. • Número de pedidos de portabilidade, suspensão de consentimentos e de eliminação de dados pessoais solicitados pelos titulares.		 ***Nível de risco estável***

5. O relacionamento que construímos com o CISO e o responsável pela proteção de dados estimula o diálogo transparente?

O CISO tem muitas responsabilidades. O responsável pela proteção de dados tem papéis e funções definidos por lei. Entretanto, nem sempre eles têm poder para exigir que outros líderes de tecnologia e negócios estejam em sintonia. Um relacionamento sólido com o conselho permite que o CISO e o encarregado se sintam confortáveis para apresentar um quadro real (que inclua todos os detalhes) dos riscos cibernéticos e da exposição na proteção de dados, inclusive suas percepções sobre a adequação dos recursos e investimentos. Sessões privadas periódicas com eles são fundamentais para entender se a empresa está tomando medidas suficientes para administrar esses riscos.

6. Como determinar se os controles e processos destinados a evitar violações de dados estão funcionando?

É importante que o conselho fale com grupos específicos, como a auditoria interna, para obter diferentes pontos de vista. Também é recomendável que o conselho contrate, periodicamente, seus próprios consultores externos para que eles analisem a situação da segurança cibernética e da proteção de dados na empresa e compartilhem suas impressões e conclusões.

Como os conselheiros podem melhorar seu conhecimento sobre segurança cibernética e proteção de dados?

- Mantendo discussões aprofundadas sobre a situação da empresa. Isso pode incluir a estratégia de segurança cibernética da empresa, os tipos de ameaças cibernéticas que enfrenta, a natureza dos principais ativos digitais e a criticidade das informações pessoais tratadas.
- Participando de programas externos. Existem várias conferências e programas de curta duração com enfoque na supervisão do risco cibernético e da proteção de dados.
- Perguntando à administração o que ela aprendeu com pares e grupos setoriais com os quais se relaciona.
- Solicitando que especialistas e peritos em segurança pública (p.ex., autoridades constituídas) façam apresentações sobre o ambiente de riscos, inteligência de ameaças, tendências de mercado, ataques e vazamentos de dados mais comuns. Isso oferece uma base para conversar com a administração sobre como a empresa está lidando com o tema.

Desafio do conselho

A empresa sofre muitas tentativas de ataque? Quantos ataques e vazamentos de dados se concretizam? Qual é a origem e a natureza desses ataques e vazamentos? Enfim, como os conselheiros podem avaliar se a empresa está preparada para lidar com violações de segurança e de proteção de dados da maneira adequada?

Nenhuma empresa é imune a ameaças de violação. Um aspecto especialmente preocupante relacionado à segurança cibernética é a possibilidade de as empresas ficarem sabendo que sofreram uma violação apenas quando notificadas por terceiros, clientes, concorrentes ou mesmo autoridades públicas. Por isso, é preciso questionar o que fazer a respeito e como proceder no caso de uma violação. Naturalmente, a organização precisa investigar a causa raiz, aplicar as ações corretivas e melhorar os controles.

Nos Estados Unidos e em muitos outros países, a legislação exige que as organizações notifiquem os indivíduos em caso de violação de dados de identificação pessoal, sempre com uma data-limite, às vezes em até 72 horas. Além disso, essas leis sofrem alterações periódicas, e é um desafio manter-se atualizado em relação a elas.

Na União Europeia, a Lei de Proteção de Dados Pessoais – GDPR (General Data Protection Regulation), que entrou em vigor em 25 de maio de 2018, estabelece regras rígidas para as empresas que manipulam, tratam ou armazenam dados pessoais dos cidadãos europeus – independentemente de a organização estar ou não estabelecida na UE.

No Brasil, o Marco Civil da Internet estabelece diretrizes gerais e a LGPD estabelece ações específicas, muitas delas tendo como base a GDPR. A LGPD dispõe sobre o tratamento de dados pessoais (funcionários, terceiros, clientes, fornecedores, entre outros), inclusive nos meios digitais, por pessoa natural ou jurídica de direito público ou privado, independentemente do país de sua sede ou do país onde estejam localizados os dados, desde que i) a operação de tratamento ocorra no território nacional; ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; e iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional. O prazo para a conformidade com a lei é 16 de fevereiro de 2020.

As autoridades públicas brasileiras têm atuado tempestivamente quando o tema é o vazamento em massa de informações pessoais. O nível de atenção à proteção de dados no país cresce, em especial, nos setores de saúde, seguros, e-commerce, serviços digitais, além do setor financeiro, geralmente mais maduro que o mercado em geral.

O estado de resiliência cibernética das empresas e a tempestividade em informar publicamente casos relevantes de incidentes cibernéticos é uma preocupação crescente dos reguladores de mercado e das autoridades públicas em muitos países. A Securities and Exchange Commission (SEC) divulgou recentemente novas diretrizes exigindo maior transparência no tratamento de riscos de segurança cibernética e na divulgação de violações de dados, além de maior tempestividade na comunicação de incidentes de invasão, mesmo que haja uma investigação policial em andamento. Exigiu também postura ética empresarial diante de informações privilegiadas sobre ataques cibernéticos e violações que podem afetar o preço das ações (*insider trading*).

No Brasil, os reguladores também estão atentos às tendências americanas e europeias a respeito das exigências de divulgação de incidentes e violações de segurança e os impactos associados. A Resolução nº 4.856/18 e a Circular nº 3.909/18 do Banco Central do Brasil são orientadas às instituições financeiras e de meios de pagamento e dispõem sobre i) a política de segurança cibernética, sua implantação e divulgação; ii) o plano de ação de resposta a incidentes

cibernéticos; e iii) os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, exigindo maior atenção e controles mais rígidos dessas instituições em relação aos riscos cibernéticos.

Violações podem levar à aplicação de multas elevadas pelas agências reguladoras e a ações coletivas. Também podem prejudicar a reputação e a marca de uma empresa, resultando em possível perda de clientes e redução da confiança dos investidores. Elas também representam aumento de custos relacionados a investigações, reparação e compensação dos que foram prejudicados. Somente metade das empresas dos EUA tem seguro cibernético,[2] apesar do número e do porte crescente dos incidentes. Em parte, isso se deve à falta de clareza quanto à forma de precificar os seguros. No Brasil, o interesse pelo seguro cibernético tem crescido e a oferta de produtos "sob medida" é um diferencial para algumas seguradoras.

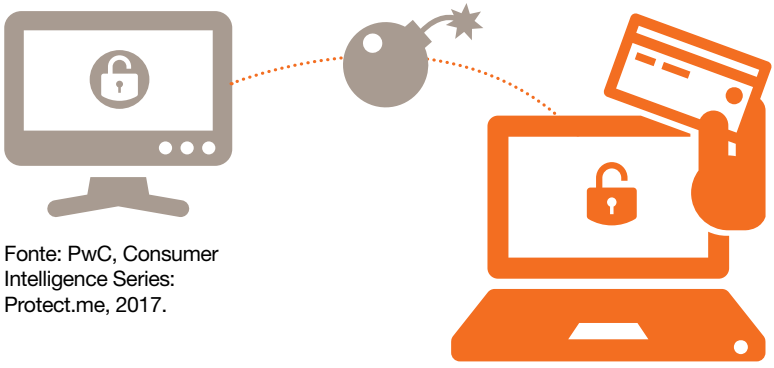
Considerando a probabilidade de uma violação e o esforço necessário para responder a um ataque, é surpreendente que

54%

dos executivos afirmem que suas empresas não têm um plano de resposta a incidentes.[3]

As empresas mais preparadas reagiram adequadamente a uma violação e geralmente saíram melhor da crise do que aquelas que não tinham um plano estabelecido para lidar com essas situações.

Os consumidores estão preocupados com a proteção dos seus dados pessoais?



Fonte: PwC, Consumer Intelligence Series: Protect.me, 2017.

85%

dos consumidores não farão negócios com uma empresa se não se sentirem seguros com relação às práticas de segurança e proteção de dados.

[2] *Insurance Journal*, "Why 27% of U.S. Firms Have No Plans to Buy Cyber Insurance" (Por que 27% das firmas dos EUA não têm planos para adquirir seguro cibernético), 31 de maio de 2017; http://www.insurancejournal.com/news/national/2017/05/31/452647.htm.

[3] PwC, Global State of Information Security® Survey 2018 (Pesquisa Global realizada em 2018 pela PwC sobre a Situação da Segurança da Informação), outubro de 2017.

Ação do conselho

Analisar regularmente o plano de gestão de crises, considerando o cenário de ataques cibernéticos ou de vazamento de dados, seja pela análise dos resultados em casos reais, seja pelas lições aprendidas com os testes de efetividade realizados pela administração.

É importante questionar a administração sobre os planos de gestão de crises, de continuidade de negócios e de resposta a incidentes cibernéticos e de vazamento de dados pessoais. Se ainda não houver planos, recomenda-se solicitar que a administração informe as ações e o respectivo cronograma para a criação dos planos e testes de efetividade.

Com os planos devidamente criados, discuta o nível de cobertura, os riscos residuais e como a empresa planeja operar em caso de um ataque disruptivo. Eles devem especificar todos os que precisam ser envolvidos nas ações de resposta a incidentes de gestão de crises, o que pode incluir a equipe de comunicação, os líderes financeiros, os líderes de negócios, a assessoria jurídica e uma equipe multidisciplinar de resposta a crises e especialistas em TI. O plano deve especificar quais recursos externos estão identificados, como advogados e especialistas forenses que podem ser acionados imediatamente para apoiar as equipes internas.

É importante prever também quem será o responsável pela interlocução com as autoridades públicas e legais, além do encarregado de proteção de dados.

Uma parte importante do plano deve incluir a notificação da violação e os processos de comunicação interna. Quando o conselho será notificado? Qual é o plano da empresa para informar os órgãos reguladores? Como e quando os outros *stakeholders* – inclusive os indivíduos cujas informações pessoais possam ter sido violadas – serão informados?

Além disso, é importante indagar se o plano foi testado e quais alterações foram feitas como resultado do último teste. Alguns conselheiros podem observar ou participar de exercícios de testes teóricos para obter um melhor entendimento de como a administração planeja abordar uma crise cibernética.

Por fim, é importante solicitar à administração comentários sobre a atualização dos planos de recuperação e continuidade baseados em incidentes ocorridos recentemente em outras organizações.

Conclusão

As empresas estão crescentemente adotando novas tecnologias, fazendo maior uso de análise de dados para fomentar a inovação e operando cada vez mais em ambientes interconectados. No Brasil e no mundo, à medida que as organizações se tornam mais dependentes de processos cibernéticos, elas também precisam saber identificar e gerir os riscos inerentes e aumentara sua resiliência a incidentes e ataques.

Os incidentes de segurança cibernética são cada vez mais comuns e muitas empresas demonstram dificuldade de lidar com tais eventos, o que é perceptível não só pela inexistência de medidas e processos para mitigá-los, mas também pelos impactos e as consequências que têm gerado em várias situações.

Nesse contexto, para o pleno desempenho de sua função de supervisão de riscos estratégicos, o conselho de administração deve ampliar sua atuação no direcionamento das ações relacionadas à segurança cibernética e privacidade de dados.

"As instituições líderes bem-sucedidas definem uma abordagem abrangente de governança em segurança cibernética e proteção de dados, do conselho à operação."

Edgar D'Andrea,
Sócio e líder de Segurança Cibernética e Privacidade de Dados

Contatos

Para uma discussão mais profunda sobre como esse tema pode afetar o seu negócio, entre em contato conosco.

Marco Castro
Sócio e líder de Auditoria
+55 (11) 3674 3647
marco.castro@pwc.com

Edgar D'Andrea
Sócio e líder de Segurança Cibernética e Privacidade
+55 (11) 3674 3826
edgar.dandrea@pwc.com

PwC Brasil @PwCBrasil @PwCBrasil

PwC Brasil PwC Brasil