

MANUAL DE SUPORTE SOBRE RISCO CIBERNÉTICO PARA O CONSELHO ADMINISTRATIVO

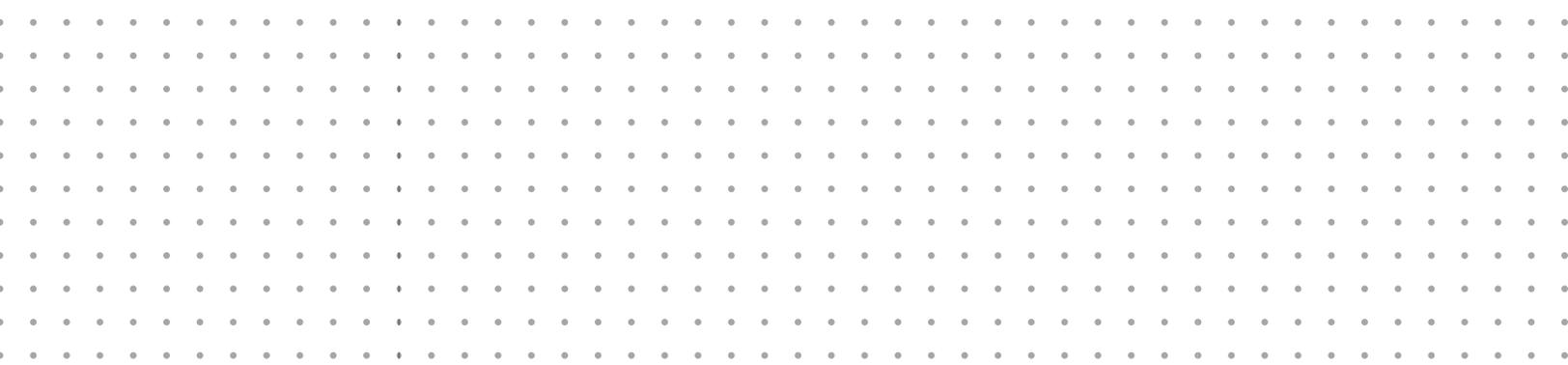


OEA

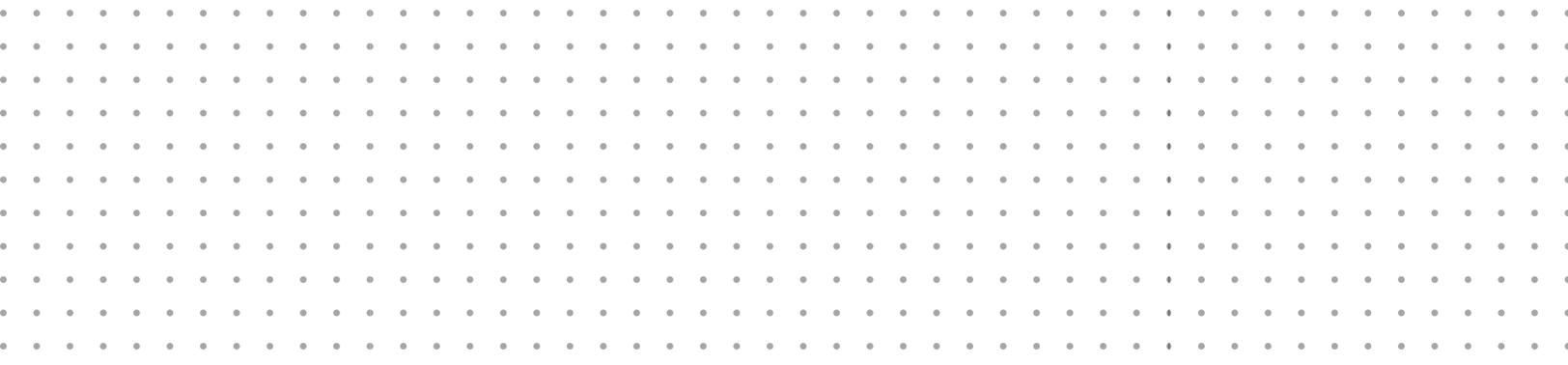
Mais direitos para mais pessoas



**INTERNET
SECURITY
ALLIANCE**



**MANUAL DE
SUPORTE
SOBRE RISCO
CIBERNÉTICO
PARA O
CONSELHO
ADMINISTRATIVO**





OEA

Mais direitos para mais pessoas



**INTERNET
SECURITY
ALLIANCE**

POR QUE DEFINIR UM MANUAL DE SUPORTE SOBRE RISCO CIBERNÉTICO PARA O CONSELHO ADMINISTRATIVO?

Ataques Cibernéticos são a ameaça de crescimento mais rápido, e talvez a mais perigosa, que as empresas enfrentam atualmente. Vários relatórios mostraram que a revolução digital está afetando mais a América Latina do que qualquer região do mundo. Embora esta revolução ofereça uma esperança de melhorias econômicas e sociais significativas para a América Latina, ela também traz riscos substanciais. De acordo com um estudo do Instituto SWIFT, “a Internet de banda larga e as redes móveis 3G e 4G se espalharam pela América Latina, permitindo que os empresários aproveitassem a tecnologia para trazer novos clientes para o sistema financeiro global. No entanto, isso também resultou em um rápido crescimento do crime cibernético, já que os hackers se aproveitam de defesas cibernéticas fracas, práticas inadequadas de higiene cibernética, capacidades limitadas de imposição da lei e governança precária da segurança cibernética”.¹

Os Conselhos de Administração devem assumir um papel de liderança na supervisão da segurança dos sistemas cibernéticos de sua empresa. No entanto, um estudo recente da Organização dos Estados Americanos e do Banco Interamericano de Desenvolvimento descobriu que os conselhos corporativos na América Latina geralmente têm níveis baixo ou médio de maturidade relacionados à segurança cibernética, com a maioria dos conselhos tendo apenas um conhecimento “formativo” de segurança cibernética². Por consequência, eles podem não ter consciência de como as ameaças cibernéticas podem afetar especificamente suas organizações. No entanto, devido à natureza em constante mudança da ameaça, os conselhos estão buscando uma abordagem coerente para lidar com a questão no nível do conselho. Em resposta, a Internet Security Alliance (ISA) e a National Association of Corporate Directors (NACD) criaram em 2014 o primeiro Manual de Suporte sobre Risco Cibernético para o Conselho de Administração. O manual provou um sucesso imediato ao ajudar os Conselhos a endereçarem riscos cibernéticos em escala global. De fato, a PricewaterhouseCoopers, em sua Pesquisa Global de Segurança da Informação, referenciou o manual pelo nome e informou que:

“Diretrizes da National Association of Corporate Directors (NACD) recomendam que os Conselhos examinem os riscos cibernéticos do ponto de vista de toda a empresa e entendam os possíveis impactos legais. Eles devem discutir com a gestão os riscos de segurança cibernética e a preparação organizacional, e considerar as ameaças cibernéticas no contexto da tolerância geral da organização ao risco.”

“Os entrevistados disseram que esse envolvimento aprofundado da Diretoria ajudou a melhorar as práticas de segurança cibernética de várias maneiras. Pode não ser coincidência que, à medida que mais membros do conselho participaram das discussões sobre orçamento de segurança cibernética, vimos um aumento de 24% nos gastos com segurança.”

“Outros resultados notáveis citados pelos entrevistados da pesquisa incluem a identificação dos principais riscos, a promoção de uma cultura organizacional de segurança e um melhor alinhamento da segurança cibernética com o gerenciamento de risco corporativo e as metas de negócios. Mais do que tudo, a participação do conselho abriu as linhas de comunicação entre executivos e diretores tratando a segurança cibernética como uma questão econômica.”

Embora muitos elementos da governança corporativa em geral, e a supervisão do risco cibernético em particular, sejam generalizáveis, também existem características únicas que se aplicam a países e regiões específicos. A Organização dos Estados Americanos (em inglês, OAS) e a ISA estão trabalhando para aprimorar ainda mais a versão original do já bem-sucedido manual de risco cibernético, adaptando-o às necessidades únicas da região latino-americana. Esta publicação é o resultado de um processo gradual através do qual a OAS e a ISA envolveram centenas de partes interessadas de conselhos administrativos, governo e alta gestão em toda a região em um esforço para apoiar as organizações a se protegerem das ameaças cibernéticas.

**MANUAL DE
SUPORTE
SOBRE RISCO
CIBERNÉTICO
PARA O
CONSELHO
ADMINISTRATIVO**



01 Agradecimientos	5
02 Introdução	7
03 Princípio 1 Os conselhos precisam entender e abordar a segurança cibernética como um problema de gerenciamento de riscos em toda a empresa, e não apenas um problema de TI.	12
04 Princípio 2 Os conselhos devem entender as implicações legais dos riscos cibernéticos, já que se relacionam com as circunstâncias específicas da empresa.	15
05 Princípio 3 Conselhos de Administração devem ter acesso adequado à conhecimentos especializados sobre segurança cibernética, e discussões sobre gestão de riscos cibernéticos devem receber tempo regular e adequado como parte das agendas de reuniões dos conselhos.	18
06 Princípio 4 Os conselhos devem estabelecer a expectativa de que a administração estabelecerá uma estrutura de gerenciamento de riscos cibernéticos para toda a empresa, com pessoal e orçamento adequados.	21
07 Princípio 5 A discussão sobre o risco cibernético pelo conselho administrativo deve incluir a identificação de quais riscos evitar, quais aceitar e quais mitigar ou transferir através de seguro, bem como planos específicos associados a cada abordagem.	24
08 Apêndice A Avaliando a cultura de segurança cibernética do conselho	26
09 Apêndice B Perguntas Fundamentais que Administração deve se fazer sobre Segurança Cibernética	28
10 Apêndice C Perguntas para a Diretoria fazer à Administração sobre Segurança Cibernética na Consciência Situacional	29
11 Apêndice D Perguntas para o Conselho fazer à Administração sobre Estratégia e Operações	30
12 Apêndice E Perguntas para o conselho fazer à Administração sobre Segurança Cibernética relativas a Ameaças Internas	31
13 Apêndice F Perguntas para o Conselho fazer à Administração sobre Segurança Cibernética na Cadeia de Suprimentos	32
14 Apêndice G Perguntas para o Conselho fazer à Administração sobre Planejamento em caso de um Potencial Incidente, Gerenciamento de Crises e Resposta	33
15 Apêndice H Considerações sobre segurança cibernética durante as fases de Fusões & Aquisições	35
16 Apêndice I Métricas de Segurança Cibernética para o Conselho Administrativo	39
17 Apêndice J Construindo um relacionamento com a Gestão de Segurança Cibernética e o time de Segurança	42

AGRADECIMIENTOS

Os seguintes profissionais são reconhecidos por suas contribuições para o desenvolvimento deste Manual, através da participação em reuniões de projetos, seminários, teleconferências e criação de conteúdo.

O Manual foi revisado a partir da versão dos EUA de 2017 com base em suas contribuições coletivas, seguindo um processo de consenso, e não reflete necessariamente as opiniões das empresas e organizações listadas.

Organização dos Estados Americanos (OEA)

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Miguel Ángel Cañada

Conselho de Administração da Internet Security Alliance

INTERNET SECURITY ALLIANCE - Larry Clinton
INTERNET SECURITY ALLIANCE - Josh Higgins
USAA - Gary McAlum
LEIDOS - JR Williamson
AIG - Tracie Grella
RAYTHEON - Jeff Brown
BNY MELLON - Adrian Peters
LOCKHEED MARTIN CORPORATION - Jim Connelly
UNISYS CORPORATION - Jonathan Goldberger
VODAFONE - Richard Spearman
ERNST AND YOUNG - Andrew Cotton
CARNEGIE MELLON UNIVERSITY - Tim McNulty
SECURE SYSTEMS INNOVATION CORPORATION - John Frazzini
NORTHROP GRUMMAN - Mike Papay
CENTENE - Lou DeSorbo
SYNCHRONY FINANCIAL - Matt Fleming
DIRECT COMPUTER RESOURCES - Joe Buonomo
NATIONAL ASSOCIATION OF MANUFACTURERS - Robyn Boerstling
BUNGE LIMITED - Robert Zandoli
FIS - Greg Montana
SAP - Tim McKnight
RSA - Shawn Edwards
MUFJ UNION BANK, N.A. - Lisa Humbert
GENERAL ELECTRIC - Nasrin Rezai
STARBUCKS - Dave Estlick
CENTER FOR AUDIT QUALITY - Catherine Ide
THOMSON REUTERS - Richard Puckett

Colaboradores

DELOITTE - Santiago Gutierrez
PINKERTON - Edith Flores
SECRETARIA DE RELACIONES EXTERIORES - Valeria Solis
CISCO - Gilberto Vicente
AIG - Ricardo Millan
BANBAJIO - Barbara Mair
HUAWEI TECHNOLOGIES - Francisco Cabrera
CENAGAS - Luis Lopez
HONEYWELL - Nahim Dias S.
CENTRO MEDICO ABC - Mary O'Keefe
GRUPO INDUSTRIAL SALTILLO - Lorena Cardenas HP - Aiza Romero Maza
ESTUDIOS Y ASESORIAS SCASOCIADOS LTDA - Cecilia Gutierrez
MINISTERIO DEL INTERIOR - Catherine Narvaez
SUBSECRETARIA DE TELECOMUNICACIONES (SUBTEL) - Jozsef Markovitz
DERECHOS DIGITALES - Pablo Viollier
CIBERSEGURIDAD HUMANA - Cristian Bravo Lillo
BANCO DE CREDITO E INVERSIONES, BCI - Lionel Olavarria Leyton
TRICOT - Susana Carey
MICROSOFT CHILE - Alex Pesseo
DREAMLAB TECHNOLOGIES - Gabriel Bergel
CLEVERIT - Diego Stevens
ENTEL - Antonio Moreno Cano
MINISTERIO DEL INTERIOR Y SEGURIDAD PUBLICA - Hernan Espinoza
SUBSECRETARIA DEL INTERIOR - Juan Pablo Gonzalez Gutierrez
SONDA - Juan Ernesto Landaeta
UNIVERSIDAD DE LOS ANDES - Pedro Anguita Ramirez
EY - Marcelo Zanotti
TECHNOLOGICAL UNIVERSITY OF CHILE - Karin Quiroga
ACTI - Jaime Pacheco
UNIVERSIDAD DE CHILE - Alejandro Hevia
REDBANC S.A. - Carolina Flisfisch
GLOBALSECURE - Manuel Moreno
FISCALIA PRIVADA - Gonzalo Errazuriz
SOLUCIONES ORION - Andres Cargill
RETAIL FINANCIERO AG - Claudio Ortiz T.
VINSON CONSULTING - TRANSBANK, REDBANK,

NEXUS - Alvaro Alliende
 GACOF CONSULTING - Orlando Garces
 CANCELLERIA - Diana Carolina Kecan Cervantes
 CCIT - Juan Alcazar
 ITM COLOMBIA - Armando Cuervo Vanegas
 PRESIDENCIA - Martha Sanchez
 HEINSOHN - Adriana Lucia Rios Sanchez
 CORREO POLICIA - Alex Duran
 ASO BANCARIA - Sandra Galvis
 MINSAIT - Hernando Diaz Bello
 ASO BANCARIA - Daniel Absalon Tocaria Diaz
 CORREO POLICIA - Alvaro Rios
 MINMINAS - Oscar Sanchez Sanchez
 OPENLINK - Leonardo Rincon Romero
 MINTRABAJO - Nidia Nayibe Gonzalez Pinzon
 FONCEP - Hector Pedraza
 MIN JUSTICIA - Adriana Aranguren
 DAVIVIENDA - Fabian Ramirez
 ESDEGUE - Jairo Becerra
 MINTIC - Fabiana Garcia
 ESDEGUE - Gladys Elena Medina Ochoa
 TIGOUNE - Laura Botero
 O4IT -Diana Carolina Echeverria Rojas
 MGM INGENIERIA - Julian E. Morales Ortega
 FIDUCOLDEX - Mabel Leonor Orjuela G.
 SONDA - Carlos Bastidas
 TIGOUNE - Alejandra Otalora
 UROSARIO - Valerie Gauthier
 CRCOM - Leidy Diana Rojas Garzon
 COLCERT - Wilson Arturo Prieto H.
 FOGAFIN - Edgar Yesid Garay Medin
 COINTERNET - Gonzalo Romero
 METRAIT - Juan Delgado
 CRCOM - Felipe Sarmiento
 DNP - Sandra Fernanda Poveda Avila
 CCB - Jaime Gonzalez
 TELEFONICA - Angela Maria Pava Orozco
 GEC RISK ADVISORY - Andrea Bonime-Blanc
 Graciela Braga
 NYU and NJIT - Arnold Felberbaum
 Passworld Technical College -Jeffrey Davis Jusino
 Sonda - Marcos Gutierrez
 Banco Central de Chile - Atilio Mashii
 Banco del Austro - Fernando Aguilar Ochoa
 Claro Colombia - Juan David Valderrama Silva
 Instituto Federal de Telecomunicaciones - Cynthia Daniela Alvarez
 Gerente TI - Giovanni Pachon
 Ing.- Miguel Gaspar
 Langtech - Luis Alfonso Nunez Gutierrez
 Superintendencia de Bancos - Daniel Monzon
 Lic. En Sistemas - Carin Molina
 TTCSIRT - Angus Smith

INTRODUÇÃO

O uso da Internet está aumentando na América Latina em uma das taxas mais altas do mundo . E de maneira correspondente, uma digitalização do risco corporativo tem ocorrido. Nos últimos anos, o valor dos ativos corporativos mudou drasticamente, de modo que agora quase 90% dos ativos corporativos são digitais. Como resultado, mais do que nunca, os formuladores de políticas, os reguladores, os acionistas e o público estão conscientes dos riscos corporativos relativos à segurança cibernética. Organizações estão sob o risco de perder propriedade intelectual e planos comerciais, ter dados destruídos ou alterados, experimentar um declínio de confiança das partes interessadas (públicas ou internas), sofrer interrupção da infraestrutura crítica, e sujeitas a sanções regulamentares em evolução. Cada um desses riscos pode afetar adversamente as posições competitivas, o preço das ações e o valor para os acionistas.

As empresas líderes veem os riscos cibernéticos e outros riscos críticos da mesma maneira - em termos de compensação de risco e recompensa. Isso é especialmente desafiador no domínio cibernético por dois motivos. Em primeiro lugar, a complexidade e a persistência das ameaças cibernéticas cresceram dramaticamente. Corporações, e mesmo empresas relativamente pequenas, agora enfrentam eventos cada vez mais sofisticados que ultrapassam as defesas tradicionais. À medida que a complexidade desses ataques aumenta, aumenta também o risco que representam para as organizações. Os efeitos potenciais de um vazamento de dados estão se expandindo muito além da perda, modificação ou interrupção de informações. Ataques cibernéticos podem ter um grave impacto na reputação e marca de uma organização. As empresas e os diretores poderão também incorrer em riscos legais e financeiros decorrentes de ataques cibernéticos.

Apesar destes riscos, a motivação para implantar tecnologias novas e emergentes para impulsionar o desenvolvimento econômico, reduzir custos, melhorar o serviço ao cliente e promover inovação é mais forte do que nunca. À medida que as ameaças à segurança cibernética crescem, os conselhos corporativos podem ser proativos em segurança cibernética, realizando avaliações de risco e tendo diálogos regulares com a gerência sênior em toda a organização. Falhas em endereçar essas vulnerabilidades pode resultar em criminosos cibernéticos chantageando as organizações através de ameaças de divulgação de vulnerabilidades, riscos e segredos competitivos da organização. Há vários outros benefícios para as organizações ao implementar medidas de segurança cibernética mais robustas que vão além de simplesmente protegê-las contra ataques, incluindo:

- Vantagem competitiva frente às empresas que possuem segurança menos robusta;
- Melhoria na relação custo-efetividade através de protocolos eficazes de gestão de riscos;
- Preservação da reputação da empresa;
- Contribuição para manter a integridade de toda infraestrutura, e proteção da confiança do consumidor e das partes interessadas;
- Além dos clientes, demonstração direta da responsabilidade corporativa em relação a todas as partes interessadas que potencialmente possam ser impactadas - funcionários, acionistas, fornecedores e a comunidade.

O Fórum Econômico Mundial relata que o ritmo acelerado da inovação e conectividade de rede continuará a aumentar nos próximos anos, tornando ainda mais crítico que ações do Comitê de Administração com relação à segurança cibernética sejam tomadas⁵.

Essas pressões concorrentes significam que a supervisão conscienciosa e abrangente no nível do conselho é essencial. É fundamental que o conselho reconheça que a gestão e mitigação do impacto do risco cibernético requer pensamento estratégico que vai além do departamento de TI. Um estudo da Organização dos Estados Americanos e do Banco Interamericano de Desenvolvimento recomenda, no mínimo, que os conselhos entendam os riscos cibernéticos que suas empresas enfrentam, os métodos primários de ataque que poderiam ser empregados contra eles e como a empresa trata e avalia questões cibernéticas⁶.

A rápida evolução do panorama de ameaça cibernética

Qual é a responsabilidade do conselho?

Tão recentemente quanto há alguns anos, os ataques cibernéticos foram amplamente a província de hackers e alguns indivíduos altamente sofisticados. Embora problemático, muitas corporações poderiam registrar esses eventos como simplesmente um custo frustrante de fazer negócios.

Hoje, as empresas estão sujeitas a atacantes que fazem parte de equipes ultrassofisticadas que implantam um crescente número de malwares dirigidos contra sistemas e indivíduos em ataques multi-faseados e silenciosos. Esses ataques, às vezes chamados de APTs (ameaças persistentes avançadas), foram empregados pela primeira vez contra entidades governamentais e prestadores de serviço de defesa. Mais recentemente, eles migraram por toda a economia, o que significa que praticamente qualquer organização está em risco.

Uma das características que define esses ataques é que eles podem penetrar virtualmente em todos os sistemas de defesa perimetral de uma empresa, como firewalls ou sistemas de detecção de intrusão. Esses ataques são meticulosamente calculados para atacar um alvo específico, e os intrusos buscam vários caminhos para explorar vulnerabilidades em todas as camadas de segurança até atingirem suas metas. A realidade é que, se um invasor sofisticado tiver como alvo os sistemas de uma empresa, eles quase certamente os violarão. Isso não significa que a segurança é impossível, apenas significa que a segurança cibernética precisa ser mais do que simplesmente segurança de perímetro baseada em TI. À medida que os ataques se tornam mais sofisticados, as defesas precisam se tornar mais sofisticadas. **Não é responsabilidade do conselho se tornar especialista em TI, mas o conselho deve saber quais perguntas fazer aos departamentos de TI. Além disso, conselhos devem demonstrar a liderança e o compromisso necessários – através de supervisão proativa e reforçando a responsabilidade da gestão e dos executivos de primeira linha – para assegurar que a proteção da organização contra ataques cibernéticos seja uma prioridade⁷.**

Não são apenas os sistemas de TI que precisam ser protegidos, trabalhadores contratados e funcionários, descontentes ou simplesmente mal treinados, representam no mínimo uma exposição tão grande para as empresas quanto os ataques externos. Isso destaca a necessidade de um programa de segurança forte e adaptável, igualmente equilibrado entre ameaças cibernéticas internas e externas. A liderança precisa assegurar que os sistemas de TI recebam proteção básica e que todo o ecossistema cibernético esteja protegido. Organizações não podem lidar com ameaças avançadas se elas não conseguirem impedir ataques de baixo custo e devem fazê-lo de maneira contínua e persistente, pois a ameaça cibernética nunca desaparece⁸.

Maior conectividade, maior risco

A crescente natureza interconectada dos sistemas tradicionais de informação e dos sistemas não tradicionais, tais como dispositivos móveis, câmeras de segurança, copiadoras, plataformas de videogames e carros (a chamada Internet das Coisas, ou IoT), resultou em um grande aumento no número de pontos de entrada potenciais para atacantes cibernéticos; e, por consequência, houve a necessidade das organizações expandirem seu pensamento sobre o risco cibernético.

Os atacantes cibernéticos tentam rotineiramente roubar todos os tipos de dados, incluindo informações pessoais de clientes e funcionários, dados financeiros, planos de negócios, segredos comerciais e endereços IP. Por exemplo, em fevereiro de 2019, o Blind Eagle, um grupo avançado de hackers de ameaças persistentes, tem se apresentado como a polícia cibernética da Colômbia em um esforço para roubar segredos de negócios de organizações-alvo. Cada vez mais, os atacantes cibernéticos estão empregando táticas que criptografam os dados de uma organização, efetivamente mantendo-os como reféns até receberem um pagamento - o chamado "ransomware".

Um exemplo: WannaCry

O que foi WannaCry?

O WannaCry foi um ataque cibernético em todo o mundo, que teve como alvo computadores que executavam o Microsoft Windows, criptografando dados e exigindo pagamentos em criptomoeda Bitcoin. WannaCry foi uma forma de ataque de ransomware. O ataque ocorreu em 12 de maio de 2017, começando na Ásia e se espalhando por mais de 230.000 computadores em mais de 150 países. O México foi o quinto país mais afetado pelo ataque cibernético.

Qual o impacto que WannaCry teve?

Uma das maiores organizações impactadas pelo ataque WannaCry foi o Serviço Nacional de Saúde (NHS) no Reino Unido. O malware infectou cerca de 70.000 dispositivos, incluindo computadores, scanners de ressonância magnética e refrigeradores de armazenamento de sangue, resultando em interrupção significativa dos serviços do NHS. Além disso, a Nissan Motor Manufacturing interrompeu a produção em uma de suas instalações como resultado das infecções da WannaCry, e importantes organizações como a FedEx também foram afetadas. As perdas econômicas do ataque em todo o mundo foram estimadas em \$ 4 bilhões de dólares.¹

Devido ao imenso número de conexões com sistemas de dados externos, não é mais adequado que as organizações protejam apenas "sua" rede. Prestadores, fornecedores, parceiros, clientes ou qualquer entidade conectada eletronicamente à empresa podem se tornar um potencial ponto de vulnerabilidade. Por exemplo,

os sistemas de uma grande empresa de petróleo foram violados quando um invasor sofisticado que não conseguiu penetrar na rede inseriu malware no menu on-line de um restaurante local popular entre os funcionários. Quando os funcionários usavam o menu on-line, eles inadvertidamente concediam acesso ao sistema corporativo aos criminosos. Uma vez dentro do sistema da empresa, os intrusos foram capazes de atacar o core business da organização¹⁰.

Ameaças Cibernéticas em Números

- Estimar os danos dos ataques cibernéticos é difícil, mas algumas estimativas apontam para US \$ 400-500 bilhões ou mais por ano, com uma parcela significativa dos custos não sendo detectados¹¹. Os custos de crimes cibernéticos quintuplicaram entre 2013 e 2015 e poderiam chegar a US \$ 2 trilhões por ano até 2019¹².
- A segurança cibernética está no topo dos riscos para os mercados da América Latina, de acordo com uma pesquisa com profissionais de risco ou não¹³.
- Brasil, Argentina e México estão em 3º, 8º e 10º lugares, respectivamente, no ranking mundial de países de origem para os ataques cibernéticos¹⁴.
- México e o Brasil ocupam a sétima e oitava posição no mundo para a maioria dos ataques de ransomware¹⁶.
- 34% de toda fraude de originação de nova conta vem da América do Sul¹⁷.
- 80% dos ataques cibernéticos são afiliados ao crime organizado¹⁸.
- O número médio de dias que uma organização é comprometida antes de descobrir uma violação cibernética é 146¹⁹. 53% dos ataques cibernéticos são identificados pela primeira vez por terceiros (por exemplo, agentes policiais ou parceiros corporativos), apenas 47% são descobertos internamente²⁰.
- 48% dos profissionais de segurança de TI não inspecionam a nuvem em busca de malware, apesar do fato de que 49% de todos os aplicativos de negócios agora estão armazenados na nuvem. Desses aplicativos baseados em nuvem, menos da metade é conhecida, sancionada ou aprovada pela TI²¹.

- 38% das organizações de TI não têm um processo definido para revisar seus planos de resposta à violação cibernética, e quase um terço não revisou ou atualizou seus planos desde que eles foram inicialmente desenvolvidos²².

Smaller Business, Bigger Risk

Historicamente, embora muitas pequenas e médias empresas tenham acreditado serem demasiado insignificantes para serem alvos, tal percepção está equivocada. Na verdade, a maioria das pequenas e médias empresas têm sido vítimas de ataques cibernéticos. Um estudo da OAS-Symantec revelou que as pequenas e médias empresas (PMEs) estão se tornando uma área de ameaça significativa, com o número de incidentes entre as PMEs aumentando rapidamente.²³ O estudo identificou o ransomware Cryptolocker como uma ameaça cada vez mais direcionada às PMEs, enquanto, de forma mais geral, os malwares que utilizam criptografia de segurança complexa estão sendo empregados contra as PMEs.²⁴ Além de serem alvos, as empresas menores são frequentemente um caminho de ataque para organizações maiores por meio de relacionamentos com clientes, fornecedores ou joint-ventures, tornando o gerenciamento de fornecedores e parceiros uma função crítica para todas as entidades interconectadas.

Existe um consenso geral na área de segurança cibernética que os atacantes cibernéticos estão muito à frente das corporações que precisam defender-se contra eles.

Isso não significa que a defesa é impossível, mas sim que os membros do conselho precisam garantir que a liderança esteja totalmente empenhada em fazer com que os sistemas da organização sejam tanto resistentes quanto economicamente viáveis. Isso inclui o desenvolvimento de planos de defesa e resposta capazes de abordar métodos sofisticados de ataque. Embora programas complexos de segurança cibernética possam ser difíceis de implementar em organizações menores que são limitadas pela disponibilidade de recursos, todas as organizações

devem ser capazes de implementar os cinco princípios fundamentais apresentados neste manual.

Por que eles nos atacarão?

Algumas organizações acreditam que é improvável que sejam vítimas de um ataque cibernético, porque elas são relativamente pequenas em tamanho, não são uma marca bem conhecida e/ou não contêm grandes quantidades de dados confidenciais de consumidores, como números de cartão de crédito ou informações médicas.

Na verdade, os adversários visam organizações de todos os tamanhos e de todos os setores, buscando tudo o que possa ser valioso, incluindo os seguintes ativos:

- Planos de negócios, incluindo fusões ou estratégias de aquisição, licitações, etc;
- Algoritmos de negociação;
- Contratos ou propostas de acordos com clientes, fornecedores, distribuidores, parceiros de joint venture, etc;
- Credenciais de acesso de funcionários e outras informações úteis;
- Informações sobre instalações, incluindo desenhos de plantas e equipamentos, mapas de edifícios e planos futuros;
- Informações de Pesquisa & Desenvolvimento, incluindo novos produtos ou serviços em desenvolvimento;
- Informações sobre os principais processos de negócios;
- Código fonte;
- Listas de funcionários, clientes, prestadores e fornecedores;
- Dados de clientes, doadores ou administradores.

Fonte: Internet Security Alliance

Equilibrando a segurança cibernética com lucratividade

Luis Alberto Moreno, presidente do Banco Interamericano de Desenvolvimento, destacou a ligação central entre segurança e desenvolvimento econômico bem-sucedido no relatório OAS-IADB: “Se quisermos aproveitar ao máximo a chamada Quarta Revolução Industrial, precisamos criar não apenas uma infraestrutura digital moderna e robusta, mas também uma infraestrutura segura. Proteger nossos cidadãos do crime cibernético não é uma mera opção; é um elemento chave para o nosso desenvolvimento.”²⁵⁾

Como outros riscos críticos que as organizações enfrentam, a segurança cibernética não pode ser considerada isoladamente. Os membros da administração e do conselho devem encontrar o equilíbrio adequado entre a proteção da segurança de uma organização e mitigar as perdas, continuando a assegurar a rentabilidade e crescimento em um ambiente competitivo.

Muitas inovações técnicas e práticas de negócios que aumentam a lucratividade também podem solapar a segurança. Por exemplo, muitas tecnologias, como a tecnologia móvel, a computação em nuvem e os dispositivos “inteligentes”, podem gerar economias de custo significativas e eficiências de negócios, mas também podem criar grandes preocupações de segurança se implementadas incorretamente. Corretamente implantadas, elas poderiam aumentar a segurança.

Da mesma forma, tendências como BYOD (traga seu próprio dispositivo), acesso 24 horas por dia, 7 dias por semana, o crescimento de análises sofisticadas de “big data” e o uso de longas cadeias de suprimentos internacionais podem ser tão rentáveis que são elementos essenciais para uma empresa se manter competitiva. No entanto, essas práticas também podem enfraquecer drasticamente a segurança da organização.

É possível que as organizações se defendam enquanto permanecem competitivas e mantendo a lucratividade. No entanto, métodos de segurança cibernética bem-sucedidos não podem simplesmente ser “incluídos” no final dos processos de negócios. A segurança cibernética precisa ser entrelaçada nos principais sistemas e processos de uma organização, de ponta-a-ponta; e quando feito com sucesso, pode ajudar a construir vantagem competitiva. Um estudo descobriu que quatro controles básicos de segurança foram eficazes na prevenção de 85% das invasões cibernéticas:

- Restringindo a instalação de aplicativos por usuários (“lista branca”).
- Garantir que o sistema operacional esteja “atualizado” com as correções atuais.
- Garantir que os aplicativos de software sejam atualizados regularmente.
- Restringir privilégios administrativos (ou seja, a capacidade de instalar software ou alterar as configurações de um computador).²⁶⁾

O estudo mostrou que estas práticas de segurança não foram somente efetivas, elas também melhoraram a eficiência dos negócios e criaram um retorno sobre o investimento imediato, mesmo antes de considerar o impacto econômico positivo decorrente da redução de violações cibernéticas²⁷⁾.

Para ser eficaz, no entanto, a estratégia cibernética deve ser mais do que reativa. Organizações líderes também empregam uma postura proativa, voltada para o futuro, que inclui a geração de inteligência sobre o ambiente de risco cibernético e a previsão de onde os invasores em potencial podem atacar. Isso inclui submeter seus próprios sistemas e processos a testes regulares e rigorosos para detectar vulnerabilidades.

Os cinco princípios para a fiscalização efetiva do risco cibernético detalhados neste manual são apresentados de forma relativamente generalizada, de forma a estimular a discussão e a reflexão dos conselhos de administração.

Naturalmente, os diretores adaptarão essas recomendações com base nas características exclusivas de sua organização; incluindo tamanho, estágio do ciclo de vida, estratégia, planos de negócios, setor industrial, presença geográfica, cultura, laços de empresa familiar e controle das preocupações das partes interessadas, e assim por diante.

PRINCÍPIO 1

Os conselhos precisam entender e abordar a segurança cibernética como um problema de gerenciamento de riscos em toda a empresa, e não apenas um problema de TI.

Historicamente, as corporações classificaram a segurança da informação como uma questão técnica ou operacional a ser tratada pelo departamento de tecnologia da informação (TI). Em uma pesquisa com empresas latino-americanas, 42% disseram que seus esforços de segurança cibernética são liderados pelo departamento de TI²⁸. Essa situação é agravada pelas estruturas corporativas que deixam funções e unidades de negócios dentro da organização se sentindo desconectadas da responsabilidade pela segurança de seus próprios dados. Em vez disso, essa responsabilidade crítica é deixada para a TI, um departamento que na maioria das organizações está trabalhando com recursos e orçamento restritos. Além disso, repassar a responsabilidade para a TI inibe a análise crítica e a comunicação sobre questões de segurança e dificulta a implementação de estratégias de segurança eficazes.

Em um ecossistema cada vez mais interconectado, cada empresa é um negócio tecnológico no qual a TI cria e agrega valor e, se não for bem financiada ou implantada, pode prejudicar o valor. A maioria das empresas investe pesado em inovação de TI e torna as infraestruturas tecnológicas cada vez mais centrais para a estratégia e as operações gerais de negócios. Dependendo do setor e dos serviços oferecidos, algumas empresas dependem mais da TI do que outras.

Os riscos cibernéticos devem ser avaliados da mesma forma que uma organização avalia a segurança física de seus ativos humanos e físicos e os riscos associados ao seu potencial comprometimento. Em outras palavras, a segurança cibernética é uma questão de gerenciamento de riscos em toda a empresa que precisa ser tratada a partir de uma perspectiva estratégica, interdepartamental, entre divisões e econômica²⁹. Não é apenas uma questão de TI (ou tecnologia), mas também sobre processos de negócios, pessoas, dados ou informações e valor. Por exemplo, a segurança cibernética deve ser incorporada em processos e programas de recursos humanos por meio de uma abordagem corporativa. Além disso, uma vez que os conselhos na América Latina são muitas vezes completamente ou parcialmente compostos por membros da família, é importante que as famílias proprietárias de empresas sejam adequadamente informadas sobre e conscientes das preocupações relativas à segurança cibernética. A OAS e o IADB identificam que a governança corporativa madura em segurança cibernética exigiria o engajamento regular do conselho e ajustes rápidos e apropriados na estratégia de segurança cibernética baseados em ameaças e riscos, bem como alocação eficaz de financiamento e atenção em toda a organização para lidar com ameaças conhecidas (e desconhecidas). O Fórum Econômico Mundial também enfatiza a necessidade de que os conselhos assegurem que a administração integre a resiliência cibernética e a avaliação de riscos na estratégia geral de negócios e no gerenciamento de riscos em toda a empresa, bem como no orçamento e na alocação de recursos.

El riesgo cibernético y el ecosistema empresarial

Algumas das violações de dados mais importantes até o momento tiveram pouco a ver com o hacking tradicional. Por exemplo, o spear phishing (um ataque comum por email direcionado à indivíduos específicos) é uma das principais causas de comprometimento dos sistemas. Estratégias de produto ou produção que usam cadeias de suprimentos complexas que abrangem vários países e regiões podem aumentar o risco cibernético. Da mesma forma, fusões e aquisições que exigem a integração de sistemas complicados, muitas vezes em cronogramas acelerados e sem a devida diligência, podem aumentar o risco cibernético.

Outro obstáculo que as empresas enfrentam na criação de um sistema seguro é como gerenciar o grau de conectividade que a rede corporativa tem com parceiros, fornecedores, afiliados e clientes. Várias violações cibernéticas significativas e bem conhecidas não começaram realmente dentro dos sistemas de TI do alvo, mas resultaram de vulnerabilidades em um de seus prestadores ou fornecedores. Exemplos disto são fornecidos abaixo na seção, “uma maior conectividade, maior risco”, na página 5. Especificamente na América Latina, uma grande quantidade de dados sensíveis está incorporada na cultura, já que muitas organizações desenvolveram relações familiares com seus provedores de serviços e geralmente compartilham grandes quantidades de informações do consumidor entre os fornecedores. Além disso, um número crescente de organizações possui dados que residem em redes externas ou em “nuvens” públicas, das quais não são proprietários ou operam, e possuem baixa vocação para proteger. É um erro supor que um provedor de nuvem automaticamente irá proteger adequadamente os dados de uma organização. Muitas organizações também estão conectadas com elementos da infraestrutura crítica nacional, elevando a perspectiva de segurança cibernética de uma empresa ou instituição a uma questão de segurança pública, ou mesmo afetando a segurança nacional.

Conselhos de administração devem assegurar que a gestão está avaliando a segurança cibernética não só no que se refere às próprias redes da organização, mas também em relação ao ecossistema maior em que opera. Progressivamente, conselhos irão envolver a liderança em discussões sobre os diferentes níveis de riscos que existem no ecossistema da empresa e irão responsabilizá-los por estimar a postura e a tolerância adequadas para riscos cibernéticos para suas próprias corporações. Eles devem prestar especial atenção às “joias da coroa” da organização - os dados altamente sensíveis que a empresa precisa proteger mais. A gestão deve assegurar ao conselho que eles possuem uma estratégia de proteção para os alvos de alto valor. O conselho deve instruir a gestão a considerar não somente os ataques de maior probabilidade, mas também os de baixa probabilidade e alto impacto que possam ser catastróficos³¹. O Apêndice “A” fornece orientações mais detalhadas sobre as perguntas que o conselho pode fazer à gestão sobre essas questões.

A responsabilidade de supervisão do risco cibernético no nível do conselho

Como preparar o conselho para supervisionar o risco cibernético, e o risco em nível corporativo de forma mais ampla, é uma questão de considerável debate. O risco cibernético pode ser mitigado e minimizado significativamente se abordado como um problema de gerenciamento de risco em toda a empresa. No entanto, como ocorre com os riscos tradicionais, os riscos cibernéticos não podem ser totalmente eliminados, e os conselhos precisam entender a natureza do ambiente de ameaças da empresa. A NACD Blue Ribbon Commission on Risk Governance recomendou que a supervisão do risco deve ser uma responsabilidade de todo o conselho³². A pesquisa da NACD considera que isso é verdade na maioria dos conselhos de empresas públicas dos EUA para os chamados “grandes riscos” (ou seja, riscos com amplas implicações para a direção estratégica ou discussões sobre a interação entre vários riscos). No entanto, pouco mais da metade dos conselhos atribui a maioria das responsabilidades de supervisão de risco relacionadas à segurança cibernética ao já sobrecarregado comitê de auditoria (Figura 2), que também assume responsabilidade significativa pela supervisão dos relatórios financeiros e riscos de conformidade.

Não existe uma abordagem única que sirva a todos os conselhos: alguns optam por conduzir todas as discussões relacionadas a riscos cibernéticos no nível do conselho; outros atribuem responsabilidades específicas de supervisão relacionadas à segurança cibernética a um ou mais comitês (auditoria, risco, tecnologia, internacional, etc.); e outros ainda usam uma combinação desses métodos. O comitê de nomeação e governança deve garantir que a abordagem escolhida pelo conselho está claramente definida nos estatutos do comitê para evitar confusão ou duplicação de esforços. Praticamente todas as decisões de negócios significativas, incluindo fusões / aquisições, desenvolvimento de novos produtos - especialmente aqueles que envolvem questões e oportunidades de transformação digital - e parcerias têm importantes implicações de segurança cibernética e portanto tais discussões devem estar inseridas dentro das discussões de negócios, da mesma maneira que as questões legais e financeiras são inseridas minuciosamente nas mesmas. Todos os membros do conselho devem ser informados sobre questões globais de segurança cibernética pelo menos semestralmente, bem como sobre incidentes específicos ou garantia de questões de negócios (por exemplo, uma fusão, uma nova parceria estratégica, o lançamento de um novo produto e sua cadeia de suprimentos). Comitês com responsabilidade designada pela supervisão do risco (e pela supervisão de riscos cibernéticos em particular) devem receber instruções gerais sobre segurança cibernética pelo menos trimestralmente ou quando incidentes ou situações específicas surgirem.

Veja o Apêndice A para perguntas sugeridas para ajudar os diretores a avaliar o nível de entendimento do conselho sobre questões de segurança ou alfabetização cibernética.

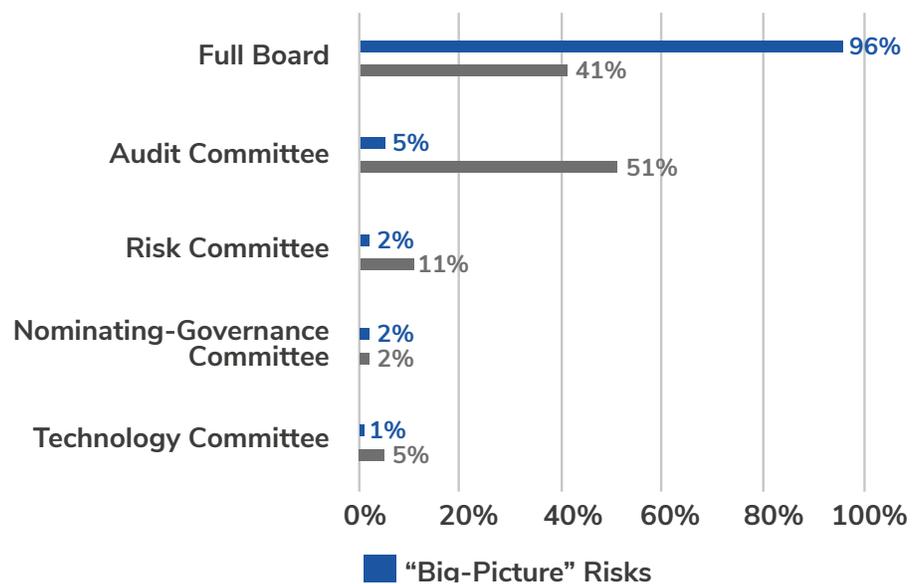
A fim de encorajar o compartilhamento de conhecimentos e o diálogo, alguns conselhos convidam todos os diretores a participarem de discussões em nível de comitê sobre questões de risco cibernético, ou a participarem de múltiplos comitês. Por exemplo,

um comitê de tecnologia de nível de diretoria de uma empresa global inclui diretores que são especialistas em privacidade e segurança do ponto de vista do cliente. Os presidentes de comitês de auditoria e tecnologia são membros dos comitês uns dos outros e os dois comitês se reúnem uma vez por ano para uma discussão que inclui um “mergulho profundo” na segurança cibernética³³. Alguns conselhos estão até estabelecendo um comitê de segurança cibernética para abordar melhor essas questões.

Figura 2

Para qual grupo o conselho tem alocado a maioria das tarefas relacionadas com as seguintes áreas de supervisão de risco?

(Lista parcial de respostas de múltiplas escolhas permitidas)



Fonte: (2016-2017 NACD Public Company Governance Survey)

PRINCÍPIO 2

Os conselhos devem entender as implicações legais dos riscos cibernéticos, já que se relacionam com as circunstâncias específicas da empresa.

O panorama legal e regulamentar em relação à segurança cibernética, incluindo divulgações necessárias, privacidade e proteção de dados, compartilhamento de informações, proteção de infraestrutura e muito mais, é complexo e está em constante evolução. Os conselhos devem estar cientes das atuais questões de responsabilidade enfrentadas por suas organizações - e, potencialmente, pelos diretores e proprietários familiares e acionistas controladores individualmente. Por exemplo, ataques de alto perfil podem gerar ações judiciais, incluindo ações de classe de acionistas e clientes, e podem levar a ações de fiscalização regulatória. Os requerentes também podem alegar que o conselho de diretores negligenciou seu dever fiduciário ao não tomar medidas suficientes para confirmar a adequação das proteções da empresa contra violações de dados e suas consequências. As exposições podem variar consideravelmente dependendo do setor e dos locais de operação da organização. Independentemente dos méritos legais ou do resultado final de qualquer desafio, danos à reputação causados a uma empresa por uma violação cibernética podem ser graves e duradouros. Não é somente importante que o conselho tome as seguintes medidas, mas também que documente sua diligência.

Conselhos devem considerar como:

- Manter registros de discussões sobre segurança cibernética e riscos cibernéticos;
- Manterem-se informados sobre os requisitos específicos da indústria, da região e do setor que se aplicam à organização, incluindo quaisquer leis e requisitos que possam ser estabelecidos em nível regional, estadual e local;
- Analisar os riscos em evolução relativos a resiliência de negócios e planos de resposta;
- Determinar antecipadamente o que divulgar caso um ataque cibernético ocorra.

A cultura de uma empresa tende a fluir de cima para baixo e, portanto, os conselhos devem adotar uma abordagem vigorosa para segurança cibernética, responsabilizando a administração com rigor, para mostrar aos funcionários que o risco cibernético deve ser sempre uma consideração importante. Estruturas de governança eficazes devem ser implementadas para sustentar essa cultura e garantir que a empresa esteja adequadamente focada no gerenciamento desses riscos. Também é aconselhável que diretores participem de simulações de violação cibernética para ganhar exposição aos procedimentos de resposta da empresa em caso de um incidente grave, para atenuar o seu impacto potencial, e para praticar em um cenário potencial que possa requerer uma importante decisão por parte do conselho de administração.

Entre os tópicos sobre os quais os conselhos devem estar atentos estão:

Agenda e Atas das Reuniões do Conselho de Administração

As atas do conselho devem refletir as ocasiões em que a segurança cibernética esteve presente na agenda em reuniões do plenário e/ou dos principais comitês, bem como quando questões cibernéticas foram inseridas em questões específicas de negócios perante o conselho, como treinamento de funcionários ou parcerias estratégicas. Deliberações destas reuniões podem incluir atualizações sobre riscos específicos e estratégias de mitigação, bem como relatórios sobre o programa de segurança cibernética global da empresa e da integração da tecnologia com a estratégia organizacional, políticas e atividades de negócios.

Cenário Jurídico

Como em grande parte do mundo, os governos da América Latina estão considerando uma onda de novas regulamentações relacionadas à segurança cibernética e privacidade. Embora seja importante que os conselhos exijam que sua administração cumpra a regulamentação cibernética e de privacidade, é fundamental que os conselhos também compreendam que estar em conformidade com os padrões e regulamentações governamentais não é o mesmo que estar seguro. Muitas regulamentações governamentais fornecem apenas as medidas mínimas de segurança que podem ser insuficientes para proteger dados valiosos dos métodos de ataques cibernéticos cada vez mais sofisticados.

Muitas organizações precisarão gerenciar a sobreposição e até mesmo o conflito entre regras e requisitos decorrentes da falta de coordenação entre as autoridades normativas e legislativas, e das diferentes prioridades que impulsionam o desenvolvimento de novas regulamentações. Embora os diretores não necessitem ter um conhecimento profundo sobre essa área cada vez mais complexa da lei, eles devem ser informados periodicamente por conselhos internos ou externos sobre os requisitos que se aplicam à empresa. Os relatórios da administração permitem que o conselho avalie se a organização está endereçando adequadamente tanto com os riscos de segurança quanto potenciais riscos legais.

Os requisitos de divulgação e reporte de uma empresa dependem do tipo de negócio que ela executa e do setor em que ela opera. Portanto, todos os membros do conselho devem ter em mente o seu dever primordial como diretores em exercer cuidado, habilidade e diligência razoáveis³⁴.

Um relatório preparado pelo Programa de Segurança Cibernética da OAS³⁵ recomendou a definição e aplicação de modelos regulatórios de privacidade e proteção de dados, criando plataformas multiclientes nacionais e sustentáveis, e fortalecendo a cooperação internacional. Nos últimos anos, o interesse dos elaboradores de políticas em segurança cibernética e privacidade têm aumentado, e enquanto muitas leis e regulamentos de segurança cibernética permanecem em estágio inicial, há várias tendências emergindo em todo o panorama jurídico na América Latina³⁶:

1. Desenvolvimento de regulamentações focadas em privacidade e proteção de dados alinhadas com os requisitos da União Europeia;
2. Integração da regulamentação da segurança cibernética nas leis de tecnologia financeira;
3. Introdução de requisitos para notificar as autoridades reguladoras sobre violações de dados.

Outra questão legal que deve ser levada em conta é a atividade criminosa relacionada à economia clandestina (underground economy), já que a lavagem de ativos (como, por exemplo, as criptomoedas) representa uma grande ameaça e pode ter um impacto significativo na segurança cibernética de uma organização.

Regulamentações de privacidade e proteção de dados³⁷

Muitos elaboradores de políticas na América Latina estão considerando a abordagem da União Europeia para segurança cibernética como um modelo à medida que desenvolvem suas próprias regulamentações. Embora a maioria destas regulamentações ainda sejam prematuras, o desenvolvimento e implementação de regulamentações de segurança cibernética focadas em privacidade têm se tornado uma prioridade para governos latino-americanos. Países da América Latina estão começando a integrar o Regulamento de Proteção de Dados Geral da União Europeia (GDPR) e outras diretrizes da União Europeia sobre segurança cibernética em seus próprios regimes. A região também está usando a Convenção de Budapeste sobre a crime cibernético como modelo (Argentina, Chile, Costa Rica, República Dominicana, Panamá e Paraguai participaram da convenção, e Colômbia, México e Peru foram observadores), e o estabelecimento das diretrizes de segurança cibernética

da União Europeia já está em vigor. Como é mais provável que a região adote um modelo baseado na União Europeia, é provável que as empresas precisem aderir aos requisitos de segurança cibernética que exigem a implementação de medidas técnicas e organizacionais “apropriadas” para garantir um nível de segurança adequado ao risco.

Requisitos para tecnologia financeira (“fintech”)

A América Latina emergiu na vanguarda do desenvolvimento de novas tecnologias no setor financeiro. Os países da América Central e do Sul têm preservado um setor financeiro orientado a inovação, mas novas exigências estão surgindo através das políticas e requisitos de segurança cibernética para o processamento e armazenamento de dados. Muitas dessas regulamentações ainda estão em desenvolvimento, mas devem trazer mais certeza para a indústria sobre quais medidas de segurança cibernética precisam estar em vigor. No entanto, as instituições financeiras provavelmente enfrentarão obrigações mais severas relacionadas à segurança cibernética devido ao foco em segurança cibernética nos dispositivos e serviços das fintechs.

Requisitos de “Notificação à Autoridades”

Países latino-americanos tradicionalmente têm exigido o reporte de violações de dados para as partes afetadas, mas não para as autoridades regulatórias. No entanto, isto está começando a mudar à medida que as organizações latino-americanas começam a atender a GDPR e outras obrigações regulatórias europeias. Devido à implementação das regras da União Europeia, muitos países latino-americanos estão começando a criar autoridades de proteção de dados nacionais e a adotar “notificação à autoridades”, estabelecendo requisitos não somente para notificar os consumidores afetados, mas também as autoridades reguladoras relevantes.

Papel do Conselho Jurídico

As equipes jurídicas e de conformidade internas, juntamente com o conselho externo, desempenham um papel fundamental na luta contra os ataques cibernéticos, especialmente à medida que os reguladores da região se fortalecem e se tornam mais ativos em áreas como segurança cibernética e governança corporativa³⁸. Os diretores devem pedir à administração que solicite as opiniões do conselho jurídico sobre:

- Implementar um modelo de trabalho para mitigar riscos legais e regulatórios;
- O plano de resposta a incidentes cibernéticos da organização, incluindo interação com reguladores e gestão documental;
- Possíveis considerações de divulgação relacionadas a fatores de risco prospectivos em geral.

Como os padrões de divulgação, instruções regulamentares, requerimentos formais e circunstâncias organizacionais continuam a evoluir, administradores e diretores devem ser atualizados periodicamente pelo conselho jurídico.

Litígio

As diretorias podem enfrentar litígios, por exemplo, se uma ação for tomada contra a empresa por clientes ou funcionários afetados por uma violação de dados ou por acionistas alegando que a diretoria não tomou as medidas apropriadas para proteger ativos ou que gerenciou mal a resposta a uma violação.

As organizações também podem ser obrigadas a apresentar litígios, por exemplo, na forma de injunções que congelem dinheiro ou informações roubadas por criminosos cibernéticos, ou em reclamações contra fornecedores terceirizados responsáveis. Em cada caso, o conselho será obrigado a tomar decisões estratégicas com base em diversos fatores, como custos, publicidade, perspectivas de sucesso e deveres para os acionistas.

PRINCÍPIO 3

Conselhos de Administração devem ter acesso adequado à conhecimentos especializados sobre segurança cibernética, e discussões sobre gestão de riscos cibernéticos devem receber tempo regular e adequado como parte das agendas de reuniões dos conselhos.

Em uma pesquisa recente, cerca de apenas 14 por cento dos diretores acreditam que seu conselho tem um “alto” nível de conhecimento dos riscos de segurança cibernética³⁹. Um estudo da OAS revelou que a maioria dos conselhos de administração na América Latina têm um conhecimento preliminar ou em formação sobre segurança cibernética, o que significa que eles têm mínimo ou nenhum entendimento sobre segurança cibernética e as responsabilidades fiduciárias afins, ou possuem alguma consciência sobre problemas cibernéticos, mas não sobre como os riscos podem afetar suas organizações. Mesmo entre os conselhos de administração da América Latina que possuem conhecimento mais avançado sobre segurança cibernética, o gerenciamento de questões cibernéticas tende a ser reativo e orientado ao perímetro, ao invés de proativo. Como o Fórum Econômico Mundial apontou, “Ser resiliente exige que aqueles que estão nos níveis mais altos de uma empresa, organização ou governo reconheçam a importância de evitar e mitigar riscos de maneira proativa”.

A menos que incidentes cibernéticos tenham sido descobertos, os conselhos não tem estado cientes sobre o que fazer para tratar a segurança cibernética dentro de suas empresas. O estudo da OAS enfatiza a importância de usar as melhores práticas de segurança cibernética em sua estrutura de governança, convidando os conselhos de administração a entender os riscos que enfrentam, os principais métodos de ataque e os protocolos da empresa para lidar com ameaças cibernéticas.

Receber instruções periódicas ou uma única vez também pode ser inadequado. Um diretor observou: “Segurança cibernética é um alvo em movimento. As ameaças e vulnerabilidades estão mudando quase diariamente, e os padrões de como gerenciar e supervisionar o risco cibernético estão apenas começando a tomar forma”⁴⁰. Em outra sessão de intercâmbio entre pares, outro diretor sugeriu essa analogia útil: “A alfabetização cibernética pode ser considerada semelhante à alfabetização financeira. Nem todos no conselho são auditores, mas todos devem ser capazes de ler uma demonstração financeira e entender a linguagem financeira dos negócios.”⁴¹. (Veja o apêndice para mais detalhes sobre alfabetização cibernética)

Melhorando o acesso ao conhecimento sobre segurança cibernética

À medida que a ameaça cibernética tem crescido, a responsabilidade (e expectativas) dos membros do conselho tem crescido. Os diretores precisam fazer mais do que simplesmente entender que as ameaças existem e receber relatórios da administração. Eles precisam empregar os mesmos princípios de investigação e desafio construtivo que são características padrão nas discussões de gestão do conselho sobre estratégia e desempenho da empresa.

Como resultado, algumas empresas estão considerando a possibilidade de adicionar a segurança cibernética e / ou a experiência em segurança de TI diretamente ao conselho por meio do recrutamento de novos diretores. Embora isso possa ser apropriado para algumas empresas ou organizações, não há uma abordagem única para todas as situações que seja aplicável a todos os lugares.

Comitês de Nomeação e Governança devem equilibrar muitos fatores ao preencher posições em aberto no conselho administrativo, incluindo a necessidade de experiência no setor, conhecimento financeiro, a experiência global, os desejos da família proprietária e dos controladores, e outros conjuntos de habilidades desejadas, dependendo das necessidades estratégicas e circunstâncias da empresa. Na América Latina, muitas vezes os donos de negócios e os acionistas controladores exercem influência significativa sobre a tomada de decisões e a participação em conselhos corporativos e, portanto, desempenham um papel significativo na determinação de adicionar conhecimento cibernético à diretoria. Se eles escolherem ou não adicionar um membro do conselho com conhecimento específico na área de segurança cibernética, os conselhos podem utilizar outras maneiras para trazer perspectivas de conhecimento sobre questões de segurança cibernética para a sala de reuniões, incluindo:

- Agendar instruções ou exames de aprofundamento com especialistas terceirizados independentes, de forma a validar se o programa de segurança cibernética está atingindo os objetivos pretendidos;
- Aproveitando os assessores independentes do conselho já existentes, tais como auditores externos e advogados externos, que terão uma perspectiva multicliente e de toda a indústria sobre as tendências de risco cibernético;
- Participar em relevantes programas educacionais para diretores, independente se fornecidos interna ou externamente.
- Proporcionar oportunidades para que os diretores compartilhem materiais de programas externos sobre segurança cibernética com outros membros do conselho.
- Criar oportunidades educacionais sobre segurança cibernética para os membros do conselho, famílias empresárias, e/ou controladores que tenham maior influência nas decisões do conselho.

Acessando Conhecimento Adequado sobre Segurança Cibernética

A maioria dos diretores é especialista em temas específicos ou áreas de especialização. Enquanto eles podem ter certa experiência sobre o assunto derivado de suas carreiras anteriores, diretores deve trazer uma visão mais ampla de gestão e resposta à riscos corporativos.

Uma organização não precisa necessariamente adicionar um especialista cibernético ao seu conselho de administração. Essa é uma decisão melhor atribuída a cada negócio. No entanto, os conselhos precisam ter clareza sobre até onde a responsabilidade cibernética pode recair, por exemplo, sobre comitê do conselho, uma administração específica ou todo o conselho. Isto se refere à responsabilidade da supervisão, não execução, da segurança cibernética e das questões de gestão de risco que a acompanham e transmitir a importância da segurança cibernética para os controladores e proprietários da família

Além disso, os riscos cibernéticos apresentam algumas diferenças importantes em relação aos riscos tradicionais. Por exemplo, as organizações não podem se proteger completamente em um mundo interconectado e em rápida evolução. Adversários cibernéticos, incluindo Estado-nação, podem ter até mais recursos do que as maiores corporações, e as dificuldades práticas associadas à captura e rastreamento de criminosos cibernéticos geralmente são maiores do que àquelas associadas a criminosos mais convencionais, algo que o(s) membro(s) do conselho devem compreender.

Existem várias maneiras pelas quais os conselhos podem considerar o aumento de seu acesso a especialistas em segurança. Conselhos podem criar um sistema de verificação e equilíbrio, buscando aconselhamento de várias fontes. Por exemplo, algumas organizações sofisticadas desenvolveram estruturas de relatórios a partir de três fontes independentes (não necessariamente externas), que poderiam incluir a perspectiva da pessoa responsável pelo risco cibernético, a perspectiva da pessoa que avalia o risco cibernético e a perspectiva do gerente operacional. Isso permite que uma organização desafie as funções e abordagens e veja o risco

cibernético de perspectivas variadas. O Princípio 4, abaixo, oferece um esboço de uma estrutura organizacional que pode, ao longo do tempo, melhorar a base de conhecimento geral sobre segurança cibernética dentro de uma empresa.

Aprimorando os relatórios da administração para o conselho

Quando solicitados a avaliar a qualidade das informações fornecidas para o conselho de administração pela alta gestão, informações sobre segurança cibernética obteve a pontuação mais baixa. Quase um quarto dos diretores de empresas públicas dos Estados Unidos reportaram estar insatisfeitos ou muito insatisfeitos com a qualidade das informações fornecidas pela administração sobre segurança cibernética. Menos de 15% disseram que estavam muito satisfeitos com a qualidade das informações recebidas, em comparação com um índice de alta satisfação de aproximadamente 64% para informações sobre desempenho financeiro⁴².

Os entrevistados da pesquisa identificaram várias razões para a sua insatisfação com o relatório de segurança cibernética da administração, incluindo:

- Dificuldade em usar as informações para avaliar o desempenho, tanto internamente (entre as unidades de negócios dentro da organização) quanto externamente (com pares do setor);
- Transparência insuficiente sobre desempenho; e
- Dificuldade em interpretar a informação⁴³.

A segurança cibernética e a análise de risco cibernético são disciplinas relativamente novas (certamente, menos maduras do que as análises financeiras) e levará tempo para as práticas de relatórios amadurecerem. No entanto, os membros do conselho devem definir expectativas claras com a administração sobre o formato, a frequência e o nível de detalhes das informações relacionadas à segurança cibernética e os principais indicadores de desempenho que desejam receber, e os relatórios devem ser escritos em termos de negócios. Ao revisar os relatórios da administração, os diretores também devem ter em mente que pode haver um viés inerente da parte da administração em minimizar o verdadeiro estado do ambiente de risco. Um estudo descobriu que 60% da equipe de TI não reporta riscos de segurança cibernética até que eles sejam urgentes (e mais difíceis de mitigar) - e reconhecem que tentam filtrar os resultados negativos⁴⁴. Os conselhos de administração devem procurar criar uma cultura de comunicação aberta, direta e transparente sobre a gestão e a comunicação de riscos cibernéticos

Consulte o Anexo D para obter detalhes sobre que tipos de métricas de relatórios sobre riscos cibernéticos os conselhos podem e devem esperar receber da gerência.

Fonte: 2016-2017 NACD Public Company Governance Survey

PRINCÍPIO 4

Os conselhos devem estabelecer a expectativa de que a administração estabelecerá uma estrutura de gerenciamento de riscos cibernéticos para toda a empresa, com pessoal e orçamento adequados.

A tecnologia integra organizações modernas, estejam os trabalhadores do outro lado do corredor ou do outro lado do mundo. Mas, como observado anteriormente, as estruturas de relatórios e os processos de tomada de decisão em muitas empresas são legados de um passado, onde cada departamento e unidade de negócios toma decisões de forma relativamente independente, sem levar em conta a interdependência digital que é um fato dos negócios modernos. Diretores devem buscar garantias de que a administração está adotando uma abordagem apropriada em toda a empresa para a segurança cibernética. O Fórum Econômico Mundial (WEF) observa que a função de governança dos conselhos é vital em relação à segurança cibernética.

Apêndice J contém considerações para construir um relacionamento com o CISO e a equipe de segurança.

Criando uma Abordagem Geral de Gestão do Risco Cibernético

Uma organização deve iniciar com uma avaliação de seu perfil único de risco e ambiente de ameaças. Talvez o maior risco para uma organização moderna é operar sob um mecanismo de avaliação de ameaças mal construída. A habilidade de uma organização para implementar um framework efetivo de segurança cibernética começa com um entendimento claro do ambiente de risco, seu apetite de risco único, e a disponibilidade de recursos necessários para mitigar os potenciais riscos cibernéticos. De fato, isto tem início com um sistema de gestão de risco empresarial (ERM) apropriadamente desenvolvido e relevante disponível onde os principais riscos estratégicos e outros riscos da companhia possam ser adequadamente coletados, avaliados, priorizados, mitigados e reportados.

Estrutura de Controles Técnicos para Gerenciamento de Riscos

É essencial que a administração seja capaz de articular claramente ao conselho a existência e implementação de uma estrutura técnica ponderada e coerente para gerenciar e proteger os dados das organizações. Nos Estados Unidos, o NIST Cybersecurity Framework é usado para delinear um conjunto de padrões, metodologias, procedimentos e processos que alinham políticas, negócios e questões tecnológicas para abordar os riscos cibernéticos. A estrutura do NIST procura fornecer uma linguagem comum para o gerenciamento corporativo sênior usar dentro da organização no desenvolvimento de uma abordagem corporativa para o gerenciamento de riscos cibernéticos.

Muitos governos latino-americanos começaram a avançar com seus próprios padrões e modelos de trabalho para segurança cibernética. Por exemplo, o Governo do Peru solicitou nos últimos anos assistência técnica da OAS para o desenvolvimento de sua própria estrutura nacional de segurança cibernética. O Peru também implementou a norma ISO 27001:2013, que também está sendo cada vez mais utilizada em toda a América Latina.

Em uma escala mais ampla, a Iberoamericana Red publicou padrões de proteção de dados para a Organização dos Estados Ibero-Americanos, em Junho de 2017. Estas normas são em grande parte baseadas na regulamentação e padrões de segurança para proteção de dados da Europa. Deve-se notar que também podem existir modelos de segurança cibernética específicos por indústria que são relevantes para as organizações. Por exemplo, os regimes regulatórios para fintechs - tais como aqueles sendo desenvolvidos pela Comisión Nacional Bancaria y de Valores, reguladora dos bancos e valores mobiliários do México - pode designar requisitos específicos para segurança de dados e privacidade para entidades do setor financeiro.

Muitas organizações adaptarão uma ou mais dessas estruturas a seus planos exclusivos de setor, cultura e negócios. O que é importante do ponto de vista do conselho não é entender os detalhes técnicos do quadro, mas que a gestão tenha um plano coerente para garantir a segurança cibernética técnica e que seja capaz de articular claramente isso para o conselho.

Enquanto a existência de um modelo técnico coerente - impulsionado por objetivos de negócio - é crítica, e, possivelmente, necessária para vários requisitos de conformidade, os conselhos precisam estar cientes de que conformidade com os modelos técnicos não corresponde necessariamente a dados organizacionais sendo adequadamente protegidos. Na verdade, as verificações operacionais de requisitos normalmente baseadas nestes modelos têm sido amplamente criticadas por não fornecerem uma imagem real da segurança organizacional. Felizmente, o campo do gerenciamento de riscos cibernéticos está evoluindo e novos métodos de avaliação de risco cibernético estão agora disponíveis, o que fornece uma forma mais contextualizada, empírica e baseada em economia para uma organização entender sua relativa segurança cibernética. Veja o apêndice sobre métricas para exemplos desses métodos mais novos de avaliação de risco.

Uma Estrutura de Gerenciamento para Segurança Cibernética

Diretores também devem definir a expectativa de que a administração considere se as estruturas corporativas tradicionais, que geralmente isolam vários departamentos, são apropriadas para um sistema muito mais integrado e consistente com a era digital. Pelo menos no que diz respeito à segurança cibernética, líderes de organizações em todo o mundo estão adotando estruturas de gerenciamento que criam uma equipe de gerenciamento de riscos cibernéticos para toda a empresa - não dominada pela TI, mas sob a supervisão de um executivo com ampla visão corporativa, como Diretor de Operações e Diretor Financeiro, ou um Chief Risk Officer. A equipe de gerenciamento de risco cibernético também deve operar com um orçamento separado e adequado para avaliar e gerenciar o risco cibernético. Um desses quadros desenvolvidos pelo ISA em conjunto com o Instituto Nacional Americano de Padrões (ANSI) é descrito abaixo.

Uma abordagem integrada para a governança de risco cibernético

- 1.** Estabeleça a propriedade do risco cibernético em uma base interdepartamental. Uma gerência sênior com autoridade interdepartamental, como o Chief Information Security Officer, o Chief Financial Officer, o Chief Risk Officer, ou o Chief Operational Officer (não o Chief Information Officer), deve liderar a equipe.
- 2.** Nomeie uma equipe de gerenciamento de riscos cibernéticos interorganizacional. Todos os departamentos relevantes das partes interessadas devem ser representados, incluindo os líderes das unidades de negócios, jurídico, auditoria interna e conformidade, finanças, RH, TI e gerenciamento de riscos. (Veja o trecho abaixo sobre “Papéis e Responsabilidades de Gestores-Chave”). Um objetivo-chave de tal esforço organizacional é garantir que não haja elos fracos ou exceções na segurança cibernética dentro da organização.

3. A equipe de risco cibernético precisa realizar uma avaliação de riscos para toda a empresa e voltada para o futuro, usando uma estrutura sistemática que responda pela complexidade do risco cibernético; incluindo, mas não limitado à conformidade regulatória. Isso incluiria a avaliação do panorama atual de ameaças e do quadro de riscos da organização. Então, estabelecendo claramente o seu apetite pelo risco. Identificar o risco potencial para a organização, bem como seu limite de risco, ajudará a equipe de risco cibernético a avaliar qual estrutura sistemática se alinha mais apropriadamente com sua missão e objetivos.

4. Esteja ciente de que as leis e regulações de segurança cibernética diferem significativamente entre as jurisdições e setores. Conforme observado no Princípio 2, a gestão deve dedicar recursos para rastrear os padrões e requisitos que se aplicam à organização, especialmente porque alguns países expandem agressivamente o escopo do envolvimento do governo na área da segurança cibernética.

5. Adote uma abordagem colaborativa para desenvolver relatórios para o conselho. Espera-se que os executivos acompanhem e informem as métricas que quantificam o impacto nos negócios de ameaças cibernéticas e os esforços de gerenciamento de riscos associados. A avaliação da eficácia do gerenciamento de riscos cibernéticos e a resiliência cibernética da empresa devem ser conduzidas como parte de auditorias internas trimestrais e outras avaliações de desempenho. Estes relatórios devem encontrar o equilíbrio certo entre muitos detalhes e o que é estrategicamente importante para relatar ao Conselho de Supervisão.

6. Desenvolva e adote um plano de garantia da gestão de riscos cibernéticos para toda a organização, incluindo estratégia de comunicação interna em todos os departamentos e unidades de negócios, e a auditoria interna. Embora a segurança cibernética obviamente tenha um componente substancial de TI (tecnologia da informação), todas as partes interessadas precisam estar envolvidas no desenvolvimento do plano corporativo e devem se sentir “compradas” por ele, incluindo as funções legais, de auditoria, risco e conformidade. O teste do plano deve ser feito rotineiramente.

7. Desenvolver e adotar um orçamento total de risco cibernético com recursos suficientes para atender às necessidades da organização e ao apetite de risco. As decisões sobre recursos devem levar em conta a grave escassez de talentos com experiência em segurança cibernética e identificar quais necessidades podem ser atendidas internamente em comparação ao que pode ou deve ser terceirizado para terceiros. Porque a segurança cibernética é mais do que Segurança de TI (ou tecnologia da informação), o orçamento para segurança cibernética não deve estar vinculado exclusivamente a um departamento: os exemplos incluem alocações em áreas como treinamento de funcionários, rastreamento de regulamentações legais, relações públicas, desenvolvimento de produtos e gerenciamento de fornecedores. O orçamento também pode incluir um plano de análise e sucessão de talentos para gerenciamento crítico, como COO, CTO, CISO, etc. Avaliando a prontidão dos sucessores e determinando se é necessário treinamento adicional para os funcionários atuais a fim de cumprir essas funções no futuro ou se o recrutamento externo de talentos é necessário aumenta a preparação cibernética da organização. Ao conduzir uma avaliação de talentos, uma organização pode minimizar a interrupção causada pela rotatividade de funcionários.

Fonte: Internet Security Alliance¹

¹ Adaptado de Internet Security Alliance y American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs* (Washington, DC: ANSI, 2010). Véase también Internet Security Alliance, *Sophisticated Management of Cyber Risk* (Arlington, VA: ISA, 2013).

PRINCÍPIO 5

A discussão sobre o risco cibernético pelo conselho administrativo deve incluir a identificação de quais riscos evitar, quais aceitar e quais mitigar ou transferir através de seguro, bem como planos específicos associados a cada abordagem.

Segurança cibernética integral é um objetivo não realista. Segurança cibernética é algo contínuo, não um estado final, e segurança não é o mesmo que conformidade. As equipes de gerenciamento precisam determinar onde, em um espectro de risco, eles acreditam que as operações e controles da empresa podem ser otimizados, em outras palavras, qual é o apetite de risco cibernético das organizações (e não pode ser zero - isso não é realista)

Definindo Apetite ao Risco

“Apetite por risco é a quantidade de risco que uma organização está disposta a aceitar em busca de objetivos estratégicos, ou o que a organização não está disposta a aceitar de forma alguma. O apetite de risco precisa estar no topo da agenda de qualquer conselho administrativo e é uma questão central de uma abordagem de gerenciamento de risco corporativo. Portanto, deve definir o nível de risco a partir do qual ações são necessárias para reduzir o risco a um nível aceitável. Quando adequadamente definido e comunicado, impulsiona o comportamento, definindo os limites para a execução do negócio e aproveitando as oportunidades.

“Uma discussão sobre o apetite ao risco deve abordar as seguintes questões:

- Valores corporativos - Que riscos não aceitaremos?
- Estratégia - Quais são os riscos que precisamos correr?
- Stakeholders - Que riscos eles estão dispostos a suportar e em que nível?
- Capacidade - Quais recursos são necessários para gerenciar esses riscos?

“O apetite ao risco é uma questão de julgamento baseada nas circunstâncias e objetivos específicos de cada empresa. Não existe uma solução única para todos.”

Fonte: PwC, *Board oversight of risk: Defining risk appetite in plain English* (New York, NY: PwC, 2014), p. 3.

Assim como ocorre com outras áreas de risco, a tolerância ao risco cibernético de uma organização deve ser consistente com sua estratégia e objetivos de negócios. Quando uma organização analisa seu risco cibernético, ela deve fazê-lo como parte de sua avaliação global do risco, colocando-o corretamente no contexto de outros riscos. A alocação de recursos de segurança é uma função do balanceamento de metas de negócios com os riscos inerentes em sistemas digitais (consulte “Definindo apetite a riscos”, página 19). Existem vários riscos cibernéticos e vários métodos para resolvê-los. A administração precisa apresentar ao conselho um quadro claro do cenário de risco e um plano para abordá-lo. Para conseguir isso, diretores e equipes de gerenciamento precisarão lidar com as seguintes questões:

• **Quais dados, sistemas e operações comerciais estamos dispostos a perder ou a que estamos comprometidos?** As discussões sobre a tolerância ao risco ajudarão a identificar o nível de risco cibernético que a organização está disposta a aceitar como uma consideração comercial possível. Neste contexto, distinguir entre missão crítica ou dados altamente confidenciais (veja “Identificar as ‘Joias da Coroa’ da Companhia, e categorias de dados altamente sensíveis” página 9) e outros dados ou sistemas que são tão importantes, mas menos essenciais ou sensíveis, é um primeiro passo fundamental. No entanto, o comprometimento de dados não é o único componente do risco cibernético. Implicações jurídicas, incluindo sanções regulatórias para violações de dados, podem existir muito além do valor real dos dados, e o risco de reputação de má publicidade pode corresponder mais a fatores externos do que o valor real dos sistemas comprometidos.

• **Como os investimentos em mitigação de risco cibernético devem ser alocados entre as defesas básica e avançada?** Ao analisar como lidar com ameaças mais sofisticadas, a gestão deve colocar o maior foco em defesas sofisticadas projetadas para proteger os dados e sistemas mais críticos da empresa. Enquanto a maioria das organizações concordaria com isso em princípio, na realidade, muitas organizações aplicam medidas de segurança de forma equivalente a todos os dados e funções. Os conselhos devem incentivar a administração a estruturar os investimentos em segurança cibernética da empresa em termos econômicos de ROI, e reavaliar o ROI regularmente. Novas ferramentas analíticas surgiram recentemente no mercado que podem ajudar a definir melhor o risco cibernético em termos econômicos e a gestão deve considerar se essas ferramentas são apropriadas para seus cálculos de risco cibernético. (Veja o Apêndice sobre Economia de Métricas Cibernéticas)

• **Quais opções estão disponíveis para nos ajudar a mitigar certos riscos cibernéticos?** Organizações de todos os setores e tamanhos têm acesso a soluções ponta-a-ponta que podem ajudar a reduzir parte do risco cibernético. Elas incluem uma bateria de medidas preventivas, como revisões de estruturas de segurança cibernética e práticas de governança, treinamento de funcionários, segurança de TI, serviços de resposta especializada e serviços gerenciados de segurança. Além da cobertura para perdas financeiras, essas ferramentas podem ajudar a mitigar o risco de uma organização sofrer danos à propriedade e danos pessoais resultantes de uma violação cibernética. Algumas soluções também incluem acesso a ferramentas proativas, treinamento de funcionários, segurança de TI e serviços de resposta especializada, para adicionar outra camada de proteção e especialização. A inclusão desses serviços de valor agregado prova ainda mais a importância de tratar a segurança cibernética além do departamento de TI, considerando-a em discussões de risco e estratégia corporativos tanto no nível do Conselho ou da administração. No entanto, a gerência precisa manter a diretoria informada sobre o cenário de risco cibernético em rápida mutação e ser ágil o suficiente para se adaptar às tecnologias em rápida mudança e aos cenários de ataques cibernéticos, como roubo de dados, corrupção de dados e até mesmo o uso de mecanismos de segurança (por exemplo, criptografia) como métodos de ataque (por exemplo, ransomware).

• **Quais opções estão disponíveis para nos ajudar na transferência de certos riscos cibernéticos?** O seguro cibernético existe para fornecer reembolso financeiro por perdas inesperadas relacionadas a incidentes de segurança cibernética. Isso pode incluir a divulgação acidental de dados, como a perda de um laptop não criptografado, ou ataques externos mal-intencionados, como esquemas de phishing, infecções por malware ou ataques de negação de serviço. Ao escolher um parceiro de seguro cibernético, é importante para uma organização escolher uma operadora com a amplitude de inovação global que melhor se adapte às necessidades da organização. As seguradoras frequentemente conduzem revisões detalhadas das estruturas de segurança cibernética da empresa durante o processo de subscrição e a precificação de políticas pode ser um sinal forte que ajuda as empresas a entender seus pontos fortes e fracos de segurança cibernética. Muitas seguradoras, em parceria com empresas de tecnologia, escritórios de advocacia, empresas de relações públicas e outras, também oferecem acesso às medidas preventivas discutidas acima. É importante notar, no entanto, que nem

todos os países latino-americanos têm mercados de seguros maduros que permitirão a transferência de riscos cibernéticos por meio de seguros, portanto as organizações devem avaliar se o seguro de segurança cibernética é uma opção viável na transferência de riscos cibernéticos.

• **Como devemos avaliar o impacto dos incidentes de segurança cibernética?** A realização de uma avaliação de impacto adequada pode ser um desafio, considerando o número de fatores envolvidos. Em um mundo interconectado, pode haver riscos cibernéticos para a organização que existam fora da capacidade da organização de mitigá-los diretamente de maneira eficaz. Por exemplo, a publicidade sobre violações de dados pode complicar substancialmente o processo de avaliação de risco. Partes interessadas (incluindo funcionários, clientes, fornecedores, investidores, imprensa, público e agências governamentais) podem ver pouca diferença entre uma violação comparativamente pequena e uma grande e perigosa. Como resultado, danos à reputação e impacto associado (incluindo reações da mídia, investidores e outras partes interessadas) podem não corresponder diretamente ao tamanho ou gravidade do evento. De fato, nesta era de hiper-transparência, mídia social e notícias imprecisas, o impacto do risco de reputação resultante de um incidente cibernético pode ser severo e desproporcional, e cabe ao conselho e aos executivos de primeira linha pensarem e serem preparados para o possível risco de reputação associado a um incidente cibernético. O conselho deve buscar garantias de que a administração refletiu cuidadosamente sobre essas implicações na elaboração de estratégias organizacionais para gerenciamento de riscos cibernéticos que incluam gerenciamento operacional de TI, mas também inclua estratégias como acordos legais com parceiros e fornecedores para ajudar a garantir segurança apropriada e relações públicas ou plano de comunicação para abordar o risco de reputação quando um evento ocorre.

APÊNDICE A

Avaliando a cultura de segurança cibernética do conselho

Um relatório da NACD Blue Ribbon Commission on Board Evaluation definiu a cultura da sala do conselho administrativo como “os valores compartilhados que fundamentam e impulsionam as comunicações, as interações e a tomada de decisões do conselho”. É a essência de como as coisas realmente são feitas.”⁴⁶. Em palavras de um participante:

Conselhos precisam mudar suas mentalidades. Devemos deixar de perguntar: “Qual é a probabilidade de sermos atacados?”, Dizendo: “É provável que tenhamos sido atacados”; de encarar a segurança cibernética como um custo e passar a visualizá-la como um investimento que nos ajuda a permanecer competitivos; de esperar que a gestão evite ou se defenda contra ameaças cibernéticas, perguntando com que rapidez eles podem detectar e responder a elas⁴⁷. Além disso, os conselhos precisam considerar quais vulnerabilidades existem em sua organização que poderiam ser exploradas por um invasor, identificando os ativos de valor e que benefício seria obtido com o ataque a esses ativos.

Diretores que desejem incorporar um componente de segurança cibernética nas autoavaliações de seus conselhos podem usar as perguntas da tabela abaixo como ponto de partida. Uma classificação de um é baixa, uma classificação de cinco é excelente.

Use a escala numérica para indicar onde a cultura da diretoria geralmente cai no espectro mostrado abaixo. ←----->			Item de ação
Nosso Conselho pensa na segurança cibernética principalmente como uma questão de TI / Tecnologia.	<p>1 2 3 4 5</p> <p><input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/></p>	Nossa Diretoria entende a segurança cibernética como uma questão de gerenciamento de risco de toda a empresa.	
Nosso Conselho confia no ambiente legal para a segurança cibernética como amplamente estável e geralmente aplicável à maioria das empresas da mesma maneira.	<p>1 2 3 4 5</p> <p><input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/></p>	O nosso Conselho aprecia a necessidade de procurar regularmente aconselhamento jurídico sobre um panorama jurídico cibernético emergente adaptado aos nossos planos e ambientes de negócios em evolução.	
Nosso Conselho não precisa de atualizações regulares sobre segurança cibernética de especialistas do setor na área.	<p>1 2 3 4 5</p> <p><input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/></p>	Nossa Diretoria procura regularmente conhecimento cibernético com relação às nossas necessidades e panorama de ameaças emergentes.	
Nossa Diretoria não sente a necessidade de que a administração forneça um plano específico para gerenciar o risco cibernético.	<p>1 2 3 4 5</p> <p><input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/></p>	Nosso Conselho espera que a administração forneça uma estrutura operacional e de gerenciamento que reflita o impacto moderno da tecnologia digital e como devemos gerenciar essa tecnologia, de acordo com nossas necessidades e riscos de negócios.	
Nossa Diretoria não espera que a administração avalie e gerencie exclusivamente riscos cibernéticos.	<p>1 2 3 4 5</p> <p><input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/></p>	Nossa diretoria espera que a administração forneça uma análise clara de quais são nossos riscos cibernéticos, quais aceitar, o que podemos mitigar e o que podemos transferir de forma consistente com nossas metas de negócios.	

APÊNDICE B

Perguntas Fundamentais que Administração deve se fazer sobre Segurança Cibernética

Mesmo antes de uma reunião do conselho, seria bom que os diretores pudessem fazer uma autoavaliação sobre se, além dos aspectos técnicos e operacionais, consideraram os vários aspectos da segurança cibernética. Em particular, os conselhos devem pensar em segurança cibernética em termos de negócios e considerar se estão preparando sua organização em um nível estratégico. Entre as perguntas que os diretores podem querer fazer, estão as seguintes:

- 1.** O CEO incentiva o diálogo aberto entre o conselho, as fontes externas e a administração sobre ameaças cibernéticas emergentes?
- 2.** Existem mecanismos para informar adequadamente os proprietários de empresas familiares e acionistas controladores que têm poder de decisão no conselho sobre a segurança cibernética da organização?
- 3.** Quem está gerenciando nossa segurança cibernética? Temos o talento certo e linhas claras de comunicação / prestação de contas / responsabilidade pela segurança cibernética? O tópico “cibernético” está incluído no nosso registro de riscos?⁴⁸ O que consideramos nossos ativos de negócios mais valiosos? Como o nosso sistema de TI interage com esses ativos?
- 4.** Estamos considerando, em tempo hábil, os aspectos de segurança cibernética em nossas principais decisões de negócios, como Fusões & Aquisições, parcerias, lançamentos de novos produtos, etc.?
- 5.** Acreditamos que existe proteção adequada se alguém quiser atingir ou danificar nossas “jóias da coroa” corporativas ou outros dados altamente confidenciais? O que seria necessário para se sentir confiante de que esses ativos / dados estavam protegidos?
- 6.** Estamos gastando sabiamente em ferramentas de segurança cibernética e treinamento? Sabemos se nossos gastos são rentáveis? Estamos realmente melhorando a segurança ou apenas cumprindo os requisitos de conformidade? Quais mecanismos estão sendo implantados para treinar funcionários em tópicos básicos de segurança cibernética em toda a empresa?
- 7.** Já consideramos como administrar nossas comunicações no caso de um evento, incluindo a comunicação com o público, nossos acionistas, nossos reguladores, nossas agências de classificação? Temos estratégias segmentadas para cada um desses públicos?
- 8.** A nossa organização participa de alguma das organizações de segurança cibernética e de compartilhamento de informações de todo o setor público ou privado? Nós deveríamos?
- 9.** A organização está monitorando adequadamente a legislação e a regulamentação atuais e potenciais relacionadas à segurança cibernética e o desenvolvimento de políticas e estruturas nacionais de segurança cibernética?⁴⁹

10. A organização está alavancando recursos dos CSIRTs nacionais (Computer Security Incident Response Teams) para analisar riscos e prevenir ataques?

11. A organização está trabalhando com colegas para compartilhar informações sobre ameaças à segurança cibernética?

12. A empresa possui seguro adequado, incluindo diretores e executivos, que cubra eventos cibernéticos? O que exatamente está coberto?⁵⁰ Existem benefícios além da transferência de risco para o seguro cibernético?⁵¹

APÊNDICE C

Perguntas para a Diretoria fazer à Administração sobre Segurança Cibernética na Consciência Situacional

Os Princípios 4 e 5 deste manual dizem respeito à responsabilidade do conselho de que a gerência forneça informações adequadas para gerenciar o risco cibernético no nível estratégico. Ao implementar esses princípios, os membros do Conselho podem optar por fazer algumas das seguintes perguntas de gestão. As questões de segurança cibernética não devem ser levantadas apenas no contexto de uma violação existente, mas em vários pontos do processo de desenvolvimento de negócios. Para facilitar o uso, o Manual divide as perguntas em tópicos relevantes que têm implicações de segurança cibernética.

- 1.** Quais são os nossos serviços críticos de negócios? Como eles mapeiam para entidades legais, perspectivas dos reguladores, departamentos de TI e fornecedores?
- 2.** Como estamos usando as operações de TI para avançar nossas metas de negócios e quais são os pontos fracos em nossa abordagem?
- 3.** Quais são os riscos de segurança cibernética da empresa e como a empresa gerencia esses riscos?⁵²
 - a. Temos um inventário de sistemas de TI e uma lista dos sistemas de TI mais críticos?
 - b. Onde está o maior risco? Onde estamos na substituição de programas desatualizados?
 - c. Qual é o nosso mapa do conselho para aprová-los para entender a idade dos sistemas e quando é hora de substituir / atualizar?
- 4.** Fomos informados de ataques cibernéticos que já ocorreram e quão severos eles eram?
- 5.** O que é importante proteger e quantas vezes observamos esses ativos comprometidos?
- 6.** Quem são nossos prováveis adversários? Eles são hackers privados ou de nação-estados?
- 7.** Na opinião da gerência, qual é a vulnerabilidade mais grave relacionada à segurança cibernética (incluindo sistemas de TI (e tecnologia), pessoal ou processos)?

8. Se um adversário quisesse infligir o maior dano à nossa empresa, como ele faria isso?
9. Quando foi a última vez que realizamos um teste de penetração ou uma avaliação externa independente de nossas defesas cibernéticas? Quais foram as principais descobertas e como as abordamos? Qual é o nosso nível de maturidade?
10. Respondemos a reguladores ou auditores externos? Quando uma auditoria provavelmente ocorreria? O que uma auditoria significa para conformidade e gerenciamento de risco?
11. Nosso auditor externo indica que temos deficiências relacionadas à segurança cibernética nos controles internos da empresa sobre relatórios financeiros? Se sim, quais são e o que estamos fazendo para remediar essas deficiências?
12. Consideramos a obtenção de uma avaliação independente e terceirizada de nosso programa de gerenciamento de riscos de segurança cibernética?
13. Somos membros de comunidades de compartilhamento de informações? Se sim, quais são as lições aprendidas de nossos colegas que sofreram violações?

APÊNDICE D

Perguntas para o Conselho fazer à Administração sobre Estratégia e Operações

1. Quais são os quadros regulamentares aos quais nos alinhamos? Fizemos uma análise de lacunas (gap analysis)?
2. Temos estratégias diferenciadas para a segurança cibernética em geral, e para proteger nossos ativos de missão crítica?
3. Nós temos uma equipe de gerenciamento de risco cibernético, orçada de forma independente, e para toda a empresa? O orçamento é adequado? Como ela está integrada ao processo geral de gerenciamento de riscos corporativos? Que tipo de decisões estratégicas têm impacto no risco cibernético?
4. Temos uma estrutura sistemática, como a Estrutura de Segurança Cibernética do NIST, as diretrizes de Padrões para Proteção de Dados em vigor para abordar a segurança cibernética e assegurar a higiene adequada da segurança cibernética?
5. Onde a gerência e nossas equipes de TI / Tecnologia discordam sobre segurança cibernética?
6. Os provedores e contratados terceirizados da empresa possuem controles e políticas de segurança cibernética? Esses controles são monitorados? Essas políticas estão alinhadas com as expectativas da nossa empresa?

7. Qual é a nossa cobertura de seguro para cyber? É adequada e qual tipo temos? Por que temos esse tipo de seguro?
8. Existe um programa de conscientização e treinamento em toda a empresa, estabelecido em torno da segurança cibernética?
9. Qual é a nossa estratégia para lidar com ameaças na nuvem, BYOD e cadeia de suprimentos?
10. Como estamos lidando com as vulnerabilidades de segurança apresentadas por uma força de trabalho cada vez mais móvel?
11. Estamos crescendo organicamente ou comprando empresas? Elas são empresas maduras ou start-ups? Onde estamos geograficamente?
12. Como o conselho deve ser estruturado para supervisionar a segurança cibernética em toda a empresa?

APÊNDICE E

Perguntas para o conselho fazer à Administração sobre Segurança Cibernética relativas a Ameaças Internas

1. Como nossos controles operacionais, incluindo restrições de acesso, criptografia, backups de dados, monitoramento do tráfego de rede, etc., ajudam a nos proteger contra ameaças internas?
2. Como adaptamos nossas políticas de pessoal, como verificação de antecedentes, orientação de novos funcionários, treinamento relacionado a mudanças de departamento / função, saídas de funcionários e afins, para incorporar a segurança cibernética?
3. Temos um plano de atividade de incidente interno que explique como e quando entrar em contato com o advogado, a força pública e / ou outras autoridades e explorar os recursos legais?
4. Temos recursos de investigação forense?
5. Quais são as principais práticas para combater ameaças internas e como elas diferem?
6. Como as principais funções (TI, RH, Jurídico e Compliance) funcionam juntas e com as unidades de negócios para estabelecer uma cultura de conscientização sobre riscos cibernéticos e responsabilidade pessoal pela segurança cibernética? Considerações incluem o seguinte:
 - a. Políticas escritas que abrangem dados, sistemas e dispositivos móveis devem ser exigidas e devem abranger todos os funcionários.

- b. Estabelecimento de um ambiente seguro para relatar incidentes cibernéticos (incluindo auto-relatos de problemas acidentais).
 - c. Treinamento regular sobre como implementar políticas de segurança cibernética da empresa e reconhecer ameaças.
7. O que estamos tentando evitar através da proteção contra ameaças internas?
8. Quais conflitos de interesse podem existir dentro das organizações que podem contribuir para uma ameaça interna relacionada à segurança cibernética?

APÊNDICE F

Perguntas para o Conselho fazer à Administração sobre Segurança Cibernética na Cadeia de Suprimentos

1. O que fazemos atualmente e o que será necessário para incluir totalmente a segurança cibernética em nosso atual gerenciamento de riscos da cadeia de suprimentos?
2. Quanto sabemos sobre nossa cadeia de fornecimento em relação à exposição e controles de risco cibernético? Que processos de due diligence usamos para avaliar a adequação das práticas de segurança cibernética de nossos fornecedores (durante o processo de integração e durante a vida útil de cada contrato)? Quais departamentos / unidades de negócios estão envolvidos? Existem arranjos de contingência apropriados em vigor no caso de um grande problema com fornecedores críticos de terceiros?
3. A empresa realiza o monitoramento estratégico adequado de fornecedores terceirizados?
4. Quais provedores usamos para a nuvem? Quais funções críticas de negócios terceirizamos, tal como segurança na nuvem, por exemplo?
5. Como podemos equilibrar as oportunidades financeiras (custos mais baixos, maior eficiência, etc.) criadas pela maior flexibilidade da cadeia de suprimentos com riscos cibernéticos potencialmente mais altos?
6. Como os requisitos de segurança cibernética são incorporados nos contratos de fornecedores? Como eles são monitorados e como estamos fazendo a devida diligência para fazer cumprir os contratos? Os contratos podem ser escritos para incluir requisitos mínimos de segurança cibernética, incluindo, por exemplo:
 - a. Políticas escritas de segurança cibernética.
 - b. Políticas de pessoal, como verificação de antecedentes, treinamento, etc.
 - c. Controles de acesso.
 - d. Políticas de criptografia, backup e recuperação.
 - e. Requisitos detalhados sobre dados detidos pelo terceiro.

- i. Requisitos de retenção e exclusão de dados retidos.
 - ii. Inventários claros de tipos de dados mantidos.
 - iii. Clareza sobre o que é armazenado, movido, processado, etc.
-
- f. Acesso secundário aos dados
 - g. Países onde os dados serão armazenados.
 - h. Notificação de violações de dados ou outros incidentes cibernéticos.
 - i. Planos de comunicação para relatórios e respostas a incidentes.
 - j. Planos de resposta a incidentes.
 - k. Auditorias de práticas de segurança cibernética e / ou certificações regulares de conformidade.

7. Permitimos que nossos fornecedores subcontratem a entrega de qualquer parte do contrato? Se sim, qual o nível de controle / vistoria que exercemos sobre os arranjos de subcontratação? Como monitoramos as mudanças nos acordos de subcontratação durante a vigência do contrato?

8. Temos tecnologia para mapear o perfil, do ponto de vista de segurança cibernética, de fornecedores e parceiros, visando identificar vulnerabilidades potenciais e gerenciar ativamente o risco de terceiros?

9. Somos indenizados contra incidentes de segurança em nossa cadeia de fornecimento? Qual é a robustez financeira da indenização?

10. Quão difícil / dispendioso será estabelecer e manter um sistema viável de teste de vulnerabilidade cibernética e penetração para nossa cadeia de suprimentos?

11. Quão difícil / dispendioso será melhorar o monitoramento de pontos de acesso nas redes de fornecedores?

12. Nossos contratos com fornecedores trazem riscos legais adicionais ou geram requisitos adicionais de conformidade (por exemplo, GDPR, FCA, etc.)?

APÊNDICE G

Perguntas para o Conselho fazer à Administração sobre Planejamento em caso de um Potencial Incidente, Gerenciamento de Crises e Resposta

- 1.** Qual é a nossa capacidade de proteger, detectar e responder a incidentes? Como a mesma se compara com os outros do nosso setor?
- 2.** No contexto de nossos negócios, o que constitui uma violação material de segurança cibernética? Como isso se compara à definição (se houver) incluída nas leis e regulamentações aplicáveis aos nossos negócios?
- 3.** Em que ponto o conselho é informado de um incidente? Quais são os critérios para relatar?
- 4.** O que se sabe sobre a intenção e capacidade do atacante? O que sabemos sobre como o invasor pode usar os dados?

5. Temos clareza sobre quem deve ser notificado e quando? A lei exige uma notificação aos órgãos reguladores ou apenas às partes afetadas? Em caso afirmativo, quais são os cronogramas e considerações estratégicas para relatar incidentes aos clientes? Reguladores / entidades governamentais relevantes? Aplicação da lei? Fornecedores / parceiros? Internamente? Pares? Investidores? Quais horários são obrigatórios por leis e regulamentos e quais são os critérios da empresa?
6. Como a administração responderá a um ataque cibernético?⁵⁴ A empresa tem um plano de resposta a incidentes validado?⁵⁵ Estamos exercendo adequadamente nosso plano de prontidão e resposta?
7. Temos um plano de gerenciamento de crise? Para violações significativas, quão bom é o nosso plano de comunicação (interna e externamente) à medida que são obtidas informações sobre a natureza e o tipo de violação, os dados afetados e as ramificações para a empresa e o plano de resposta?⁵⁶
8. O que estamos fazendo para evitar piorar o problema para nossa organização? Como podemos garantir que temos aconselhamento legal apropriado nas equipes de gerenciamento de incidentes e crises? As equipes jurídicas estão integradas nos planos de incidentes e crises

Após um incidente de segurança cibernética

1. Como aprendemos sobre o incidente? Fomos notificados por terceiros ou o incidente foi descoberto internamente?
2. O que acreditamos ser o motivo do incidente? Qual foi o impacto e como medimos isso? Alguma de nossas operações foi comprometida?
3. O nosso plano de resposta a incidentes cibernéticos / crises está em ação e está funcionando como planejado?
4. O que a equipe de resposta está fazendo para garantir que o incidente esteja sob controle e que o invasor não tenha mais acesso à nossa rede interna?
5. A equipe de resposta está coordenando as CSIRTs nacionais para gerenciar o incidente? Que mecanismos existem para colaborar e compartilhar informações com colegas de confiança do setor privado e / ou do governo?
6. Quais foram os pontos fracos em nosso sistema que permitiram que o incidente ocorresse e por que eles não foram identificados ou remediados?
7. A equipe de segurança verificou vulnerabilidades associadas em todos os sistemas / redes da empresa, não apenas nos sistemas ou serviços afetados? Verificaram o que aconteceu com a estrutura de controles e fizeram as mudanças necessárias nos controles de segurança e nos controles de negócios?
8. Que medidas podemos tomar para garantir que esse tipo de evento não aconteça novamente? Como podemos garantir que as lições sejam aprendidas e as ações de correção sejam rastreadas?
9. O que podemos fazer para mitigar as perdas causadas pelo incidente?

10. O incidente altera a tolerância ao risco do negócio? Isso foi discutido e as alterações foram capturadas?

Fonte: NACD, et al., *Cybersecurity: Boardroom Implications* (Washington, DC: NACD, 2014) (an NACD white paper).

APÊNDICE H

Considerações sobre segurança cibernética durante as fases de Fusões & Aquisições

As empresas envolvidas em transações geralmente são alvos primários de hackers e criminosos cibernéticos, porque o valor das informações confidenciais relacionadas a transações é alto, e os prazos curtos, ambiente de alta pressão e cargas de trabalho significativas associadas a transações podem fazer com que os principais agentes atuem de maneira descuidada e potencialmente cometer erros. As vulnerabilidades de segurança cibernética exploradas durante uma transação podem representar riscos para o valor da transação e retorno do investimento:

Riscos a curto prazo

- Operações paralisadas como resultado de ransomware ou malware.
- O período de transação pode ser usado por agentes de ameaças para obter reconhecimento de entrada e conduta, um evento que muitas vezes não é detectado até bem depois do fechamento do negócio.
- Roubo de informação privilegiada, incluindo avaliações, ofertas, etc.
- Reivindicações de garantia, alteração de termos de transação ou redução do valor da transação.
- Investigações forenses relacionadas a uma violação de dados.

Riscos a longo prazo

- Exposição ao risco de ações judiciais regulatórias e outras.
- Investigação regulatória e penalidades.
- Perda de clientes e impactos associados nas vendas e no lucro.
- Dano à reputação.
- Perda de participação de mercado para concorrentes sem uma violação de dados conhecida.

Diretores devem solicitar que a administração conduza uma avaliação de risco cibernético para cada fase do ciclo de vida da transação para confirmar que sistemas e processos estão seguros, e para quantificar os riscos que podem impactar a empresa após o fechamento do negócio, incluindo receitas, lucros, valor de mercado, participação de mercado e reputação da marca.

Estratégia e Fase de Identificação do Alvo

O risco de ataque começa antes mesmo de uma oferta oficial ou anúncio de fusão ser feito. Escritórios de advocacia, assessores financeiros, consultores e outras empresas associadas são atrativos para hackers porque possuem segredos comerciais e outras informações confidenciais sobre clientes corporativos, incluindo detalhes sobre exploração de transações em estágio inicial que podem ser roubadas para repassar informações privilegiadas ou obter vantagem competitiva nas negociações comerciais. Ataques cibernéticos em escritórios de advocacia estão aumentando globalmente, levando os advogados a rotular o cyber como uma “ameaça existencial” para as empresas⁵⁷. Uma empresa precisa, portanto, ter uma compreensão dos controles e da segurança em vigor em todos os terceiros que a assistem durante o processo de fusões e aquisições, e uma compreensão completa de como os dados confidenciais devem ser compartilhados entre as partes.

Os invasores buscam dicas de que uma empresa está considerando uma fusão, aquisição ou alienação. Eles podem ser informados por fofocas da indústria, uma desaceleração no ciclo de lançamento de uma empresa, reduções de pessoal ou vazamento de dados por meio de canais de mídia social. Existem quatro formas principais de a informação estar em risco:

- Um hacker entra na rede por meio de falhas em suas defesas, começando pelos computadores voltados para a Internet de uma empresa.
- Um hacker lança um ataque de engenharia social contra um funcionário da empresa.
- Os funcionários da empresa (funcionários, contratados, fornecedores) divulgam dados e informações confidenciais, intencionalmente ou como resultado de negligência. O risco de ameaças internas aumenta significativamente em uma Fusão & Aquisição.
- As informações são expostas através de vulnerabilidades em fornecedores terceirizados ou provedores de serviços.

Durante essa fase, a administração deve compreender os riscos cibernéticos associados à empresa-alvo e modelar o impacto desses riscos na postura de conformidade, nas previsões financeiras e nas possíveis avaliações. A administração pode executar a análise a seguir mesmo antes de começar o envolvimento direto com a empresa-alvo:

- Realizando pesquisas na “dark web”⁵⁸ (sites de difícil acesso favorecidos por hackers) sobre o alvo, seus sistemas, dados e propriedade intelectual. Isso ajuda a identificar se a empresa já está no radar dos hackers, se os sistemas ou credenciais já estão comprometidos e se há dados confidenciais para venda ou solicitação. A administração precisará considerar a legalidade de tais pesquisas com referência às informações que estão sendo acessadas.
- Mapeando o perfil da empresa-alvo do ponto de vista de segurança cibernética, enquanto implementa tecnologia relevante.
- Pesquisando infecções por malware na empresa-alvo e lacunas em suas defesas visíveis do lado de fora. Essas informações estão disponíveis ao público e podem ser usadas para comparar uma empresa a outra, permitindo que a administração economize tempo e energia ao não buscar empresas cujo perfil de risco é inaceitavelmente alto.

- Modelar o impacto financeiro dos riscos cibernéticos identificados. Esses riscos podem não apenas impactar o retorno de uma empresa sobre o capital investido, mas também resultar em perda de vantagens competitivas, remediação onerosa, multas e possivelmente anos de litígio, dependendo do que foi roubado. Uma estimativa inicial do impacto pode ser material o suficiente para encorajar as equipes de estratégia a alterar a trajetória do negócio. A estimativa pode ser refinada à medida que o processo de transação continua e os riscos são mitigados.

Investigação Prévia (Due Diligence) e Fases de Execução do Negócio

Durante essas fases, a empresa deve ser diligente quanto à avaliação da segurança cibernética. Problemas significativos exigiriam a negociação de uma redução no preço de compra para cobrir os custos de remediação necessária. Dependendo dos riscos identificados, a Diretoria pode adiar a aprovação da transação até que a correção seja concluída ou decidir se retirar de uma transação se os riscos identificados justificarem tal ação. A identificação dos riscos de segurança cibernética durante a fase de diligência pode ser realizada através da realização de diligências de segurança cibernética que são adaptadas para descobrir esses riscos:

- Identificar investimentos insuficientes na infraestrutura de segurança cibernética, bem como deficiências em recursos humanos, políticas, etc.
- Identificar atitudes culturais negligentes em relação ao risco cibernético.
- Determinar termos e condições relacionados à segurança cibernética (ou a falta deles) em contratos com clientes e fornecedores que tenham um impacto financeiro potencial ou resultem em litígios por não conformidade.
- Descobrir a não conformidade com as leis de privacidade de dados relacionadas a ciberespaço ou outros regulamentos e requisitos aplicáveis.
- Identificar violações recentes de dados ou outros incidentes de segurança cibernética.

Uma investigação prévia eficaz sobre questões de segurança cibernética demonstra aos investidores, reguladores e outras partes interessadas que a administração está buscando ativamente proteger o valor e os direcionadores estratégicos da transação, e que eles estão tentando reduzir o risco de um ataque cibernético antes da integração. Esses riscos e vantagens podem ser incluídos no preço inicial pago e em investimentos de melhoria de desempenho que elevarão o valor da transação, permitindo que uma proposta de transação robusta seja apresentada aos acionistas para aprovação.

Fase de Integração

A integração pós-negociação coloca uma série de desafios relacionados a pessoas, processos, sistemas e cultura. Os riscos cibernéticos acrescentam outra dimensão de complexidade e risco a essa fase da transação. Os hackers aproveitam as inconsistências existentes entre as plataformas e as operações de tecnologia da empresa e a entidade recém-incorporada ou adquirida nessa fase.

As equipes de integração precisam ter o conhecimento necessário para explorar e aprofundar os menores detalhes para identificar e mitigar riscos cibernéticos, tais como:

- Lacunas de segurança identificadas durante as fases anteriores.
- Priorização de atividades de remediação com base no impacto potencial de lacunas identificadas.
- Priorização de atividades de integração.
- Treinamento de funcionários em sistemas recém-integrados.

Fase de criação de valor pós-transação

Após a conclusão de uma transação, o monitoramento contínuo dos riscos cibernéticos pela administração criará inúmeras oportunidades para melhoria e crescimento do portfólio.

A administração deve continuar a avaliar a maturidade cibernética da entidade incorporada ou adquirida comparando-a com os padrões e a concorrência do setor, assim como fazem com o negócio principal. A baixa maturidade pode afetar as projeções de crescimento e a reputação da marca devido a incidentes cibernéticos e possíveis multas. Uma violação ou problema de conformidade pode levar os reguladores a investigar, levando a uma perda financeira ou à paralisação dos planos de saída pós-transação. Questões cibernéticas também podem levar a ações legais de clientes e fornecedores, causando perda de valor e menores retornos.

Uma visão do lado da venda

Muitos dos mesmos riscos que impactam a empresa compradora que são descritos aqui, naturalmente, aplicam-se igualmente ao lado do vendedor. Na fase de criação de avaliação pós-transação, o vendedor está particularmente exposto a violações de divulgações que podem afetar o preço / tempo do negócio e até mesmo as operações contínuas da entidade vendedora se a transação falhar. Conseqüentemente, um entendimento completo dos vetores de risco existentes antes da execução do negócio informará melhor a natureza das garantias feitas pela empresa de vendas e reduzirá a exposição.

O fluxo de informações para diretores de empresas vendedoras pode ser mais limitado em sua natureza e frequência à medida que o tempo passa após o anúncio do negócio e os diretores devem estabelecer os limites e a natureza de qualquer comunicação de violação no período pós-anúncio.

Conclusão

A diligência da segurança cibernética durante as fusões e aquisições exige uma dupla abordagem. As empresas devem conduzir uma investigação prévia rigorosa sobre os riscos cibernéticos da empresa-alvo e avaliar seu impacto nos negócios relacionados ao longo do ciclo de negócios para proteger o retorno sobre o investimento da transação e o valor da entidade após a transação. Além disso, todas as partes envolvidas no processo de negociação precisam estar cientes do aumento do potencial de um ataque cibernético durante o processo de transação em si e devem diligentemente manter seus esforços de segurança cibernética. A aplicação dessa abordagem em duas frentes durante as fusões e aquisições servirá para proteger o valor das partes interessadas.

APÊNDICE I

Métricas de Segurança Cibernética para o Conselho Administrativo

Quais métricas de segurança cibernética devem ser incluídas em um resumo para o conselho? Esta questão é enganosamente simples. Semelhante a praticamente todas as outras divisões e funções dentro da organização, a função de segurança cibernética coleta e analisa um enorme volume de dados e há pouco consenso sobre quais são os poucos dados críticos que devem ser compartilhados com o público da diretoria. Somando-se ao desafio está o fato de que a segurança cibernética é um domínio relativamente novo, com padrões e benchmarks que ainda estão se desenvolvendo ou evoluindo.

Em última análise, os diretores precisarão trabalhar com os membros da administração para definir as informações, métricas e outros dados de segurança cibernética que são mais relevantes para eles, considerando o ambiente operacional da organização - incluindo indústria ou setor, requisitos regulamentares, presença geográfica e assim por diante. Na maioria das vezes, os conselhos veem um grande volume de métricas operacionais que fornecem muito pouca visão estratégica sobre o estado do programa de segurança cibernética da organização. As métricas normalmente apresentadas incluem estatísticas como “número de ataques bloqueados”, “número de vulnerabilidades não corrigidas” e outras medidas autônomas e orientadas à conformidade, que fornecem pouco contexto estratégico sobre o desempenho e a posição de risco da organização.

Como ponto de partida, os diretores podem aplicar os mesmos princípios gerais usados para outros tipos de métricas para o conselho nos relatórios relacionados à segurança cibernética (consulte na barra lateral, “Princípios Orientadores para Métricas do Conselho”).

Além disso, as recomendações a seguir fornecem um ponto de partida para os tipos de métricas de segurança cibernética que os membros do conselho devem considerar solicitar à administração.

- 1.** Qual é o nosso apetite ao risco cibernético? Esta é uma questão fundamental na qual o Chief Information Security Officer (CISO) deve trabalhar com o Chief Risk Officer (CRO) para resolver. Esse tipo de colaboração pode produzir pontos de dados qualitativos e quantitativos para apresentação ao conselho, o qual proverá contexto sobre o apetite ao risco cibernético.
- 2.** Quais métricas nós temos que indicam risco para a empresa? Uma organização implementou um “índice” de risco de segurança cibernética que incorpora várias métricas individuais para riscos corporativos, para a cadeia de suprimentos e para os que atingem consumidores.
- 3.** Quanto do nosso orçamento de TI / tecnologia está sendo gasto em atividades relacionadas à segurança cibernética? Como isso se compara aos nossos concorrentes/pares e/ou a outros benchmarks externos? Essas métricas apoiarão as conversas sobre como a administração determina “quanto é suficiente o gasto” e se o aumento dos investimentos reduzirá o risco residual da organização? Outras perguntas adicionais incluem:
 - Quais iniciativas não foram financiadas no orçamento deste ano? Por quê?
 - Quais trade-offs foram feitos?
 - Temos os recursos certos, incluindo funcionários e sistemas, e eles estão sendo implantados de forma eficaz?

- 4.** Como medimos a eficácia do programa de segurança cibernética de nossa organização e como ele se compara aos de outras empresas? As métricas para o conselho devem destacar mudanças, tendências e padrões ao longo do tempo, mostrar o respectivo desempenho e indicar impacto. Empresas de teste de penetração externas e especialistas de terceiros podem fornecer uma comparação entre setores da indústria.
- 5.** Quantos incidentes de dados (por exemplo, dados confidenciais expostos) a organização experimentou no último período do relatório? Essas métricas informarão conversas sobre tendências, padrões e causas principais.
- 6.** Os relacionamentos da cadeia de valor geralmente representam um risco maior para as empresas, dado o grau de interconectividade do sistema e o compartilhamento de dados que agora fazem parte das operações diárias do negócio. Como avaliamos a posição de risco cibernético de nossos fornecedores, fornecedores, parceiros de Joint Ventures e clientes? Como conduzimos o monitoramento contínuo de sua postura de risco? Quantos fornecedores externos se conectam à nossa rede ou recebem dados confidenciais de nós? Esta é uma métrica operacional limítrofe, mas pode ajudar a apoiar discussões com a gerência sobre risco residual de terceiros. Existem prestadores de serviços no mercado de segurança cibernética que fornecem monitoramento passivo e contínuo das posturas de segurança cibernética das empresas. Um número crescente de empresas utiliza esses serviços para avaliar seus relacionamentos de terceiros de alto risco, bem como seu próprio estado de segurança cibernética.
- 7.** Quais métricas operacionais são rastreadas e monitoradas rotineiramente por nossa equipe de segurança? Embora as métricas operacionais sejam o domínio da equipe de TI/Segurança, seria benéfico para os diretores compreenderem a abrangência e a profundidade das atividades de monitoramento da segurança cibernética da empresa para fins de conscientização situacional.
- 8.** Quais métricas usamos para avaliar a conscientização sobre segurança cibernética em toda a organização? Os dados sobre conformidade com as políticas, a implementação e a conclusão de programas de treinamento, entre outros, ajudarão a informar conversas sobre riscos internos em vários níveis de senioridade e em várias regiões e divisões.
- 9.** Como rastreamos os indivíduos ou grupos que estão isentos das principais políticas de segurança, monitoramento de atividades, etc.? Essas medidas indicarão áreas em que a empresa está exposta a riscos adicionais, abrindo caminho para discussões sobre trade-offs de risco/retorno nessa área.

Desenvolvendo Métricas Econômicas Cibernéticas

O risco cibernético agora é aceito como uma conversa no conselho de administração. O desafio, no entanto, é como comunicar de forma eficaz e precisa o impacto financeiro dos incidentes cibernéticos ao Conselho. Antes que os conselhos possam tomar decisões fundamentadas sobre como gerenciar o risco cibernético, eles devem primeiro ter a capacidade de traduzir dados de segurança cibernética em métricas financeiras. Os diretores do conselho precisarão trabalhar com a gerência para delinear as informações de segurança cibernética mais relevantes, considerando o ambiente operacional da organização, incluindo indústria ou setor, requisitos regulamentares, presença geográfica e assim por diante. Para começar, as seguintes recomendações de risco cibernético para o Conselho de Administração fornecem um ponto de partida que os mesmos devem considerar solicitar à administração:

- Quais são as nossas métricas trimestrais de perda esperada relacionadas à nossa condição de risco cibernético em nossas várias unidades de negócios e ambientes operacionais?
- Qual é o impacto financeiro relacionado ao pior cenário de risco cibernético?
- Que processos estabelecemos relacionados à aceitação de riscos cibernéticos, correção de riscos cibernéticos e decisões de transferência de riscos cibernéticos? Como medimos como essas decisões reduzem nossa exposição financeira ao risco cibernético?
- Como estamos medindo e priorizando nossas atividades de implementação de controle e orçamentos de segurança cibernética contra nossa exposição financeira ao risco cibernético? Conectamos nossa estratégia de implementação de controle e programas de segurança cibernética, incluindo orçamentos, com nossa estratégia de transferência de risco cibernético?
- Com base em nossas metas de desempenho financeiro, como o risco cibernético pode afetar o mesmo? Qual é o nosso valor de perda esperada anual de risco cibernético?
- Qual é o nosso plano de remediação de risco cibernético para atingir nosso nível de tolerância a perda esperado? O nosso plano produz um retorno financeiro líquido positivo?
- Como o nosso programa de segurança cibernética alinha a análise da taxa de perda esperada baseada no risco cibernético e as metas de tolerância à perda esperada? Como estamos medindo, rastreando e demonstrando como nossos investimentos em segurança cibernética estão reduzindo nossa exposição financeira a incidentes cibernéticos e entregando retorno sobre o investimento em segurança cibernética?
- Como estamos medindo e alinhando nossa “análise de taxa de perda esperada baseada em risco cibernético” e nosso “planejamento de segurança cibernética” com nosso “plano de seguro para transferência de risco cibernético”?
- Como medimos a eficácia do programa de segurança cibernética de nossa organização e como ele se compara aos de outras empresas?

Fonte: Secure Systems Innovation Corporation (SSIC) and X-Analytics

APÊNDICE J

Construindo um relacionamento com a Gestão de Segurança Cibernética e o time de Segurança

Até recentemente, a noção de um executivo sênior cujos esforços eram dedicados a garantir a segurança cibernética da empresa era um conceito estranho para empresas fora da área de tecnologia. Os tempos mudaram; executivos da alta gestão (C-Suite) responsáveis pelo controle do risco digital estão em ascensão em empresas de médio e grande porte em muitos setores diferentes, uma consequência da realização de negócios no mundo sempre conectado de hoje.

De acordo com um estudo, 54% das empresas em todo o mundo empregam um Chief Information Security Officer (CISO)⁵⁹. Outra pesquisa constatou que as organizações com CISOs estavam mais propensas a ter equipes e planos de resposta a incidentes dedicados e estavam mais confiantes sobre a força das defesas de sua empresa contra ameaças como *malware*⁶⁰. Na América Latina, as organizações estão apenas começando a estabelecer CISOs dentro de suas organizações. Onde não há CISO, no entanto, haverá uma equipe de segurança que assume as responsabilidades pela segurança cibernética. A chave é que o conselho desenvolva um relacionamento com aqueles que lideram a segurança cibernética dentro da organização. É importante esclarecer que o papel de um CISO e da equipe de segurança tradicionalmente não é o mesmo. Os CISOs são geralmente associados à função de segurança da informação como uma segunda linha de defesa no gerenciamento e avaliação de riscos de informações, enquanto as equipes de segurança cibernética geralmente são a primeira linha de defesa no gerenciamento de sistemas de TI diretamente.

Construir as relações corretas entre o CISO (ou equivalente) e o conselho é essencial. À medida que as funções corporativas de segurança da informação se tornam mais maduras, surge uma nova questão: como a diretoria se comunica com a função de segurança? O CISO ou equivalente é responsável por gerenciar riscos operacionais, de reputação e monetários significativos, portanto, é essencial uma relação de confiança com a diretoria. Muitos membros do conselho agora buscam estabelecer um relacionamento contínuo com o CISO e incluem o executivo de segurança em discussões sobre questões de segurança cibernética em reuniões do Conselho e/ou comitês-chave. Durante essas sessões informativas (briefings) entre o CISO e a diretoria, é importante que a equipe de gerenciamento de riscos cibernéticos seja totalmente representada perante a diretoria para reduzir os temores de punição individual por vulnerabilidades de segurança cibernética.

As perguntas e diretrizes abaixo foram elaboradas para auxiliar os diretores a estabelecer ou aprimorar um relacionamento com o CISO ou equivalente. Eles também podem ajudar os membros do conselho a melhorar suas comunicações com a equipe de segurança e ajudá-los a obter um melhor entendimento da abordagem geral da empresa para a segurança cibernética. Como nem todas as questões terão relevância para todas as empresas, os diretores devem selecionar as mais adequadas aos problemas e circunstâncias em questão.

1. Entenda o papel e o mandato da equipe de segurança.

- Qual é o estatuto e o escopo de autoridade da equipe de segurança em termos de recursos, decisões, orçamento, recursos humanos e acesso à informação? Como isso se compara à prática líder em nosso setor e em geral? ⁶¹
- Como o orçamento de segurança cibernética da organização é determinado? Comparar esse número com as tendências de gastos da indústria é provavelmente a melhor maneira de obter contexto sobre a adequação do financiamento. Qual é o seu tamanho (por exemplo, porcentagem do total de gastos em TI / Tecnologia), e como esse número se compara com as principais práticas em nosso setor e em geral? Qual o papel da equipe de segurança na alocação do orçamento de segurança cibernética e nas decisões de investimento? Quais ferramentas de segurança ou outros investimentos estavam abaixo da linha de corte no orçamento?
- Qual é o relacionamento de subordinação administrativa da equipe de segurança (por exemplo, CIO, CTO, COO, chefe de segurança corporativa, outros)? Diferencia-se da relação de subordinação funcional? Que protocolos existem para garantir que a equipe de segurança tenha um canal independente para encaminhar os problemas e fornecer uma divulgação imediata e completa das deficiências de segurança cibernética? ⁶²
- Qual papel a equipe de segurança desempenha na estrutura de gerenciamento de riscos corporativos (ERM) da organização e na implementação de processos de ERM?
- Que papel a equipe de segurança desempenha, caso exista, além de definir e impor políticas de segurança cibernética e sistemas de controle relacionados?
 - Por exemplo, a equipe de segurança fornece informações sobre o processo de desenvolvimento de novos produtos, serviços e sistemas ou sobre o design de contratos de parceria e aliança, etc., de modo que a segurança cibernética seja “incorporada” ao invés de “adicionada” após o fato?
- A equipe de segurança possui as habilidades necessárias e a empresa é capaz de atrair e reter o nível necessário para ser eficaz?
- Como a divisão de risco é decidida? Como a postura de segurança da empresa é determinada, como ela é assinada e com que frequência ela é revisada?
- Quais são os arranjos para poder escalar a equipe de segurança em caso de crise? Temos as relações certas com terceiros adequados?

2. Passar tempo com a equipe de segurança antes de um incidente gera dividendos.

- Uma crise é o momento errado para os diretores se familiarizarem com a equipe de segurança e com o pessoal-chave. Os membros da diretoria podem marcar uma visita à equipe de segurança e receber orientações em primeira mão do pessoal situado nas linhas de frente da segurança cibernética, talvez agendado em conjunto com uma reunião regular da diretoria ou visita ao local. Essas sessões fornecerão informações valiosas e oportunidades de aprendizado para os membros do conselho. A equipe de segurança também apreciará isso, já que visitas como essa podem aumentar sua visibilidade, aumentar a moral e reforçar a necessidade de se concentrar nessa área.
- Os diretores também podem solicitar ao executivo de segurança uma avaliação de sua situação pessoal de segurança cibernética, incluindo a segurança de seus dispositivos, redes domésticas, etc.

Essas discussões não são apenas informativas para diretores individuais, mas também ajudam a proteger informações confidenciais ao longo do seu serviço.

- Muitas equipes de segurança rotineiramente produzem relatórios internos para a administração e liderança sênior sobre tendências e incidentes de ataques cibernéticos. Os diretores podem discutir com a equipe de segurança, o secretário corporativo e os líderes do Conselho se essas informações podem ser relevantes e úteis para incluir nos materiais do Conselho.
- Os conselhos podem sugerir uma reunião trimestral ou mensal com o pessoal-chave de segurança para acessar o estado atual de segurança e exposição ao risco. Os conselhos devem entender que a segurança está continuamente evoluindo e mudando e, portanto, reuniões regulares para avaliar o estado atual do perfil de risco de uma organização fornecem informações sobre quais recursos são necessários e onde a atenção precisa ser revertida. Os conselhos também devem solicitar que uma simulação ou um “exercício de mesa” de planos de resposta a incidentes seja realizado pelo menos anualmente.

3. Obtenha informações sobre a rede de relacionamento da equipe de segurança.

Dentro da organização

- Como a equipe de segurança da informação colabora com outros departamentos e funções corporativas em questões relacionadas à segurança cibernética? Por exemplo, a equipe de segurança trabalha de maneira coordena com:
 - Desenvolvimento de negócios em due diligence sobre metas de aquisição e contratos de parceria;
 - Auditoria interna referente à avaliação e teste de sistemas e políticas de controle;
 - Recursos humanos em treinamento de funcionários e protocolos de acesso;
 - Compras e cadeia de suprimentos em protocolos de segurança cibernética com fornecedores, clientes e fornecedores; e/ou
 - Jurídico em relação à conformidade com os padrões regulamentares e de relatórios relacionados à segurança cibernética, bem como à privacidade de dados?

A equipe de segurança deve ser capaz de articular para que a segurança cibernética não seja apenas um problema de tecnologia; ela é sobre habilitar a empresa para que a mesma implemente sua estratégia da maneira mais segura possível.

- Qual suporte a equipe de segurança recebe do CEO, CIO e equipe de gerenciamento sênior?
- Como a equipe de segurança da informação desenvolve e mantém o conhecimento dos objetivos estratégicos, modelo de negócios e atividades operacionais da organização?
 - Por exemplo, em empresas que estão ativamente buscando uma estratégia de “big data” para melhorar a análise de produtos e clientes, até que ponto a equipe de segurança entende a estratégia e contribui para sua execução segura?
- Quais atividades de educação continuada são realizadas pela equipe de segurança da informação para se manterem atualizados em questões de segurança cibernética?

Fora da organização

- A equipe de segurança da informação participa de iniciativas de compartilhamento de informações de segurança cibernética (por exemplo, com foco na indústria, com foco em TI / Tecnologia ou parcerias público-privadas)? Como as informações obtidas da participação em tais iniciativas são usadas e compartilhadas dentro da organização?
- A equipe de segurança da informação tem relacionamento com partes interessadas do setor público, como agências de segurança pública e divisões de segurança cibernética de agências reguladoras?

4. Avalie o desempenho.

- Como o desempenho da equipe de segurança é avaliado? Como o desempenho da equipe de segurança da informação é avaliado? Quem realiza essas avaliações e quais métricas são usadas?
- Quais medidas e marcos de desempenho de segurança cibernética foram estabelecidos para a organização como um todo? Utilizamos uma abordagem baseada em risco que fornece um nível mais alto de proteção para os ativos mais valiosos e críticos da organização?
- Até que ponto as atividades de avaliação e gerenciamento de riscos cibernéticos são integradas aos processos de gerenciamento de riscos da empresa em toda a organização? Estamos usando a segurança cibernética apropriada para avaliar a higiene da segurança cibernética a partir de uma perspectiva ampla da organização?

5. Envolve a infraestrutura de segurança em discussões sobre o “estado da organização.”

- Qual foi o incidente de segurança cibernética mais significativo da organização durante o último trimestre? Como foi descoberto? Qual foi a nossa resposta? Como a velocidade de detecção e recuperação se comparou com a de incidentes anteriores? Que lições aprendemos e como elas são incorporadas nos esforços de melhoria contínua da organização?
- Qual foi o nosso mais significativo ponto de falha na segurança cibernética no trimestre passado? Como foi descoberto? Qual foi a nossa resposta? Que lições aprendemos e como elas são incorporadas nos esforços de melhoria contínua da organização?
- Onde fizemos o maior progresso em segurança cibernética nos últimos seis meses, e a que fator(es) esse progresso é atribuível? Onde nossas lacunas mais significativas permanecem e qual é o nosso plano para preencher essas lacunas?

Princípios orientadores para apresentar ao Conselho sobre segurança cibernética

Como a administração trabalha com os conselhos de administração em segurança cibernética, é fundamental que a segurança cibernética seja adequadamente comunicada ao conselho. Para utilizar eficazmente os seguintes apêndices, a administração deve manter essas características em mente ao apresentar a segurança cibernética ao conselho:

- Relevante para o público (full-board; comitê chave);
- De fácil leitura: utilize resumos, textos explicativos, gráficos e outros recursos visuais; evitar o jargão técnico;
- Transmitir significado: comunicar percepções, não apenas informação;
 - Realce mudanças, tendências, padrões ao longo do tempo;
 - Mostrar o desempenho relativo em relação aos pares, em relação às médias do setor, em relação a outros indicadores externos relevantes, etc. (por exemplo, avaliações de maturidade);
 - Indicar impacto nas operações de negócios, custos, participação de mercado, etc.;
- Ser conciso: evite sobrecarga de informação.

Acima de tudo, permita a discussão e o diálogo.

Sobre os Colaboradores

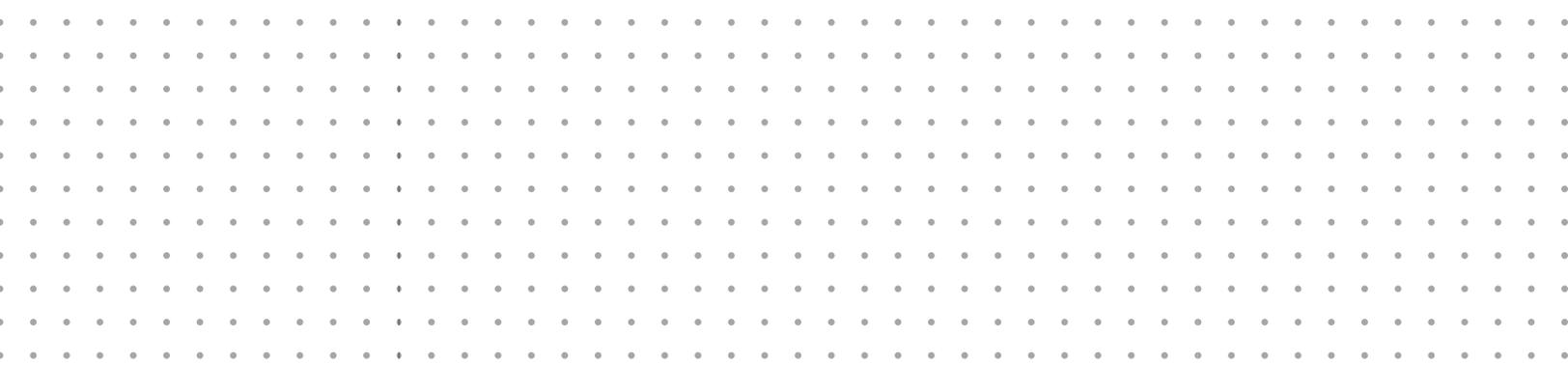
A Internet Security Alliance

A Internet Security Alliance (ISA) é uma associação comercial internacional, fundada em 2000, que se concentra exclusivamente na segurança cibernética. O Conselho da ISA é constituído pelas principais pessoas de segurança cibernética de empresas internacionais, representando praticamente todos os setores da economia. A missão da ISA é integrar economia com tecnologia avançada e política governamental para criar sistemas cibernéticos sustentáveis. Em 2014, a ISA produziu o primeiro Manual de Supervisão de Risco Cibernético, abordando especificamente o papel exclusivo que os conselhos corporativos desempenham no gerenciamento do risco cibernético. Em sua pesquisa anual Global Information Security, a PricewaterhouseCoopers (PwC) informou que o handbook estava sendo amplamente adotado pelas diretorias corporativas e seu uso resultou em melhor orçamento de segurança cibernética, melhor gerenciamento de riscos cibernéticos, alinhamento mais próximo da segurança cibernética com metas gerais de negócios e ajuda a criar uma cultura de segurança nas organizações que o utilizam. Para mais informações sobre o ISA, visite www.isalliance.org.

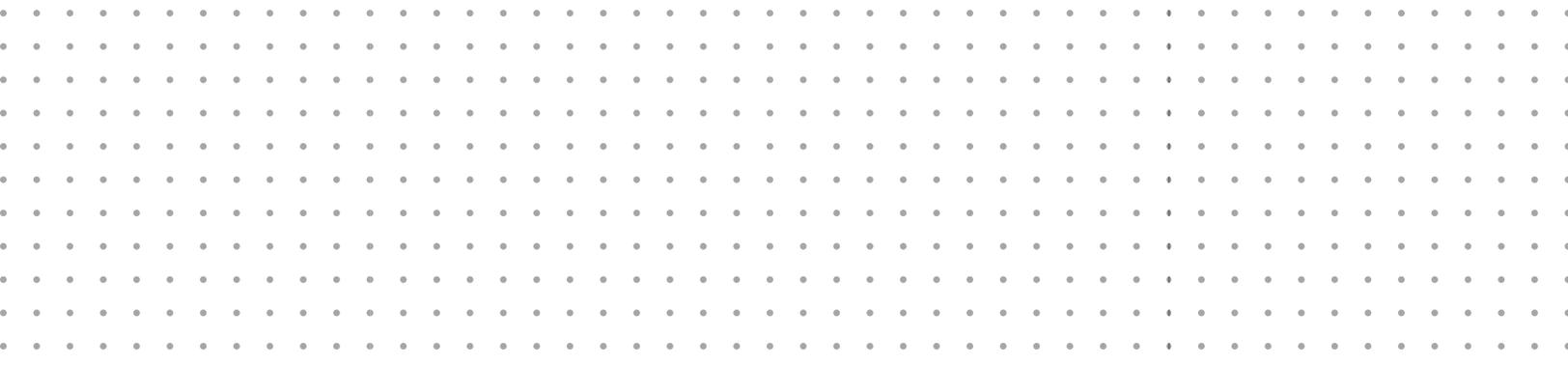
Notas de rodapé

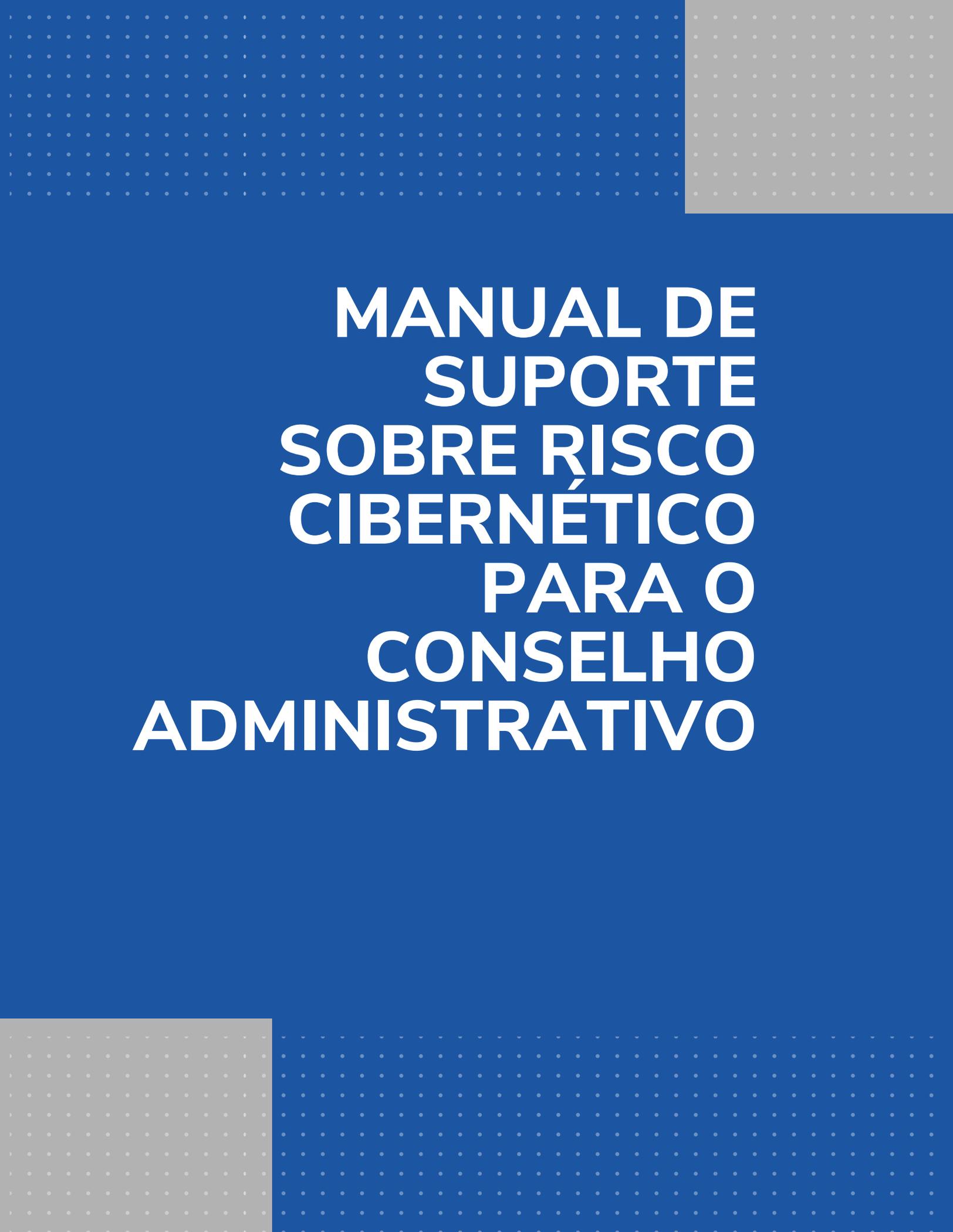
1. <https://www.swiftinstitute.org/wp-content/uploads/2017/10/SIWP-2016-004-Cyber-Threat-Landscape-Carter-Final.pdf>
2. <https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean>
3. https://www.sites.oas.org/cyber/Certs_Web/OAS-Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf
4. https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Cyber_Threat_Landscape%20_Carter.pdf?UWwqJEbDm.dBKSLEIFTyYs1IxJaExh9Y7
5. World Economic Forum, “**Advancing Cyber Resilience Principles and Tools for Boards**”
6. <https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean>
7. <https://www.oas.org/es/sms/cicte/cipreport.pdf>
8. Verizon RISK Team, et al., **2013 Data Breach Investigations Report**, March 2013.
9. <https://www.cyberscoop.com/apt-c-36-blind-eagle-colombia/>
10. Nicole Perlroth, “**Hackers Lurking in Vents and Soda Machines**,” *the New York Times*, Apr. 7, 2014.
11. Steve Morgan, “**Cyber Crime Costs Projected to Reach \$2 Trillion by 2019**,” *Forbes*, Jan. 17, 2016.
12. Ibid.
13. <http://aldianews.com/articles/culture/unknown-consequence-latin-americas-tech-boom/55104>
14. <http://www.seguridadinternacional.es/?q=es/content/cybersecurity-challenges-latin-america>
15. https://www.trendmicro.com/en_ae/about/newsroom/press-releases/2015/trend-micro-partners-with-rmeducation-to-bring-worry-free-secur21221111111212.html
16. <https://www.symantec.com/security-center/threat-report>
17. <https://www.threatmetrix.com/info/q1-2018-cybercrime-report/>
18. Limor Kessem, “**2016 Cybercrime Reloaded: Our Predictions for the Year Ahead**,” Jan. 15, 2016.
19. FireEye Inc, **Mandiant M-Trends 2016**, p. 4.
20. Kessem, “**2016 Cybercrime Reloaded**.”
21. Jeff Goldman, “**48 Percent of Companies Don’t Inspect the Cloud for Malware**,” *eSecurity Planet (blog)*, Oct. 12, 2016.
22. Thor Olavsrud, “**Companies complacent about data breach preparedness**,” *CIO*, Oct. 28, 2016. Eset, *Latin American Security Report (2017)*
23. http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf
24. Mark Smith, “**Huge rise in hack attacks as cyber-criminals target small business**,” *The Guardian*, Feb. 8, 2016.
25. Estudio del BID
26. AFCEA Cyber Committee, **The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment**, 27. October 2013. See also: Internet Security Alliance, **Sophisticated Management of Cyber Risk** (Arlington, VA: Internet Security Alliance, 2013).
27. AFCEA Cyber Committee, **The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment**, October 2013.
28. <https://www.oas.org/es/sms/cicte/cipreport.pdf>
29. Internet Security Alliance and American National Standards Institute, **The Financial Management of Cyber Risk: An Implementation Framework for CFOs**, 2010.
30. NACD, et al., **Cybersecurity: Boardroom Implication** (Washington, DC: NACD, 2014) (an NACD white paper).
31. Ibid. See also: KPMG Audit Committee Institute, **Global Boardroom Insights: The Cyber Security Challenge**, Mar. 26, 2014.
32. NACD, **Report of the Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward** (Washington, DC: NACD, 2009).
33. Adaptado de Robyn Bew, “**Cyber-Risk Oversight: 3 Questions for Directors**,” *Ethical Boardroom*, Spring 2015.
34. Section 174 Companies Act 2006
35. <https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean>
36. <https://www.lexology.com/library/detail.aspx?g=c0701531-2665-4e4b-a87b-00434e25d55f>
37. Regulation (EU) 2016/679 [NB: This paragraph has been written as if the GDPR is effective. The effective date is May 2018.]

38. <https://www.atkearney.com/documents/783760/869855/Governance+practices+of+Corporate+Boards+in+Latin+America.pdf/f5ae6de9-86e6-9999-8e9d-2fa4cc8e913d?version=1.0>
39. NACD, **2016-2017 NACD Public Company Governance Survey** (Washington, DC: NACD, 2016), p. 26.
40. NACD Audit Committee Chair and Risk Oversight Advisory Councils, **Emerging Trends in Cyber-Risk Oversight**, July 17, 2015, p. 1.
41. NACD, et al., **Cybersecurity: Boardrooms Implications** (Washington, DC: NACD, 2014) (an NACD white paper), p. 3.
42. NACD, **2016-2017 NACD Public Company Governance Survey** (Washington, DC: NACD, 2016), p. 28.
43. *Ibid.*
44. Sean Martin, “**Cyber Security: 60% of Techies Don’t Tell Bosses About Breaches Unless It’s Serious,**” *International Business Times*, April 16, 2014.
45. Andrea Bonime-Blanc. “**Cyber-Reputation: Risk Turbocharged**”. *Ethical Corporation Magazine*. March 2016.
46. **Report of the NACD Blue Ribbon Commission on Board Evaluation: Improving Director Effectiveness** (Washington, DC: NACD, 2010), p. 7.
47. Italicized quotations are from participants in the Global Cyber Summit, held Apr. 15-16, 2015, in Washington, DC. Discussions were conducted under the Chatham House Rule.
48. Lexology.com, Ed Batts, DLA Piper LLP, “**Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members,**” Jan. 23, 2014.
49. *Ibid.*
50. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, “**Board Oversight.**”
51. *Ibid.*
52. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, “**Board Oversight.**”
53. Lexology.com, Ed Batts, DLA Piper LLP, “**Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members,**” Jan. 23, 2014.
54. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, “**Board Oversight.**”
55. *Ibid.*
56. StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, “**Board Oversight.**”
57. <https://www.law.com/international/2018/04/27/cyberattacks-geopolitical-shocks-and-global-competition-what-keeps-law-firm-leaders-up-at-night-396-2954/?sreturn=20180728162144>
58. “The Dark Web” é um termo geral que descreve sites da Internet ocultos que os usuários não podem acessar sem usar um software especial como o TOR (“The Onion Router”). Embora o conteúdo desses sites possa ser acessado, os editores desses sites são ocultados. Os usuários acessam a “Dark Web” com a expectativa de poder compartilhar informações e / ou arquivos com pouco risco de detecção.
59. PwC, **Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016** (New York, NY: PwC, 2015), p. 26, and see Paul Solman, “**Chief information security officers come out from the basement,**” *Financial Times*, Apr. 29, 2014.
60. Kris Monroe, “**Why are CISOs in such high demand?**” *Cyber Experts Blog*, Feb. 8, 2016.
61. See, for example, Marc van Zadelhoff, Kristin Lovejoy, and David Jarvis, *Fortifying for the Future: Insights from the 2014 IBM Chief Information Security Officer Assessment* (Armonk, NY: IBM Center for Applied Insights, 2014).
62. A 2014 study of global information security issues found that organizations with CISOs reporting outside the CIO’s office have less downtime and lower financial losses related to cybersecurity incidents as compared with those who report directly to the CIO. See Bob Bragdon “**Maybe it really does matter who the CISO reports to,**” *The Business Side of Security (blog)*, June 20, 2014.



**MANUAL DE
SUPORTE
SOBRE RISCO
CIBERNÉTICO
PARA O
CONSELHO
ADMINISTRATIVO**





**MANUAL DE
SUPORTE
SOBRE RISCO
CIBERNÉTICO
PARA O
CONSELHO
ADMINISTRATIVO**