GLOBAL PERSPECTIVES & INSIGHTS

Cibersegurança em 2022

PARTE 1: Como as novas propostas da SEC podem mudar o jogo

PARTE 2: Parceiros Críticos – Auditoria Interna e CISO

PARTE 3: Resposta e Recuperação de Incidentes Cibernéticos

TRADUZIDO POR • INSTITUTO DOS AUDITORES INTERNOS DO BRASIL •
IIA Brasil

The Institute of Internal Auditors

CONTEÚDO

Parte 1:

Como as novas propostas da SEC podem mudar o jogo

Sobre os Especialistas

Andy Watkin-Child

Watkin-Child é um veterano de 20 anos em cibersegurança, gerenciamento de riscos e tecnologia, e cofundador do The Augusta Group, um fornecedor de soluções para gestão, supervisão e avaliação de cibersegurança e risco cibernético. Ocupou cargos de liderança internacional na 1ª e 2ª Linhas de Defesa de cibersegurança, gerenciamento de risco cibernético, risco operacional e tecnologia, trabalhando com equipes de liderança de empresas com balanços superiores a €1 trilhão nas indústrias de engenharia e fabricação, serviços financeiros, e publicação e mídia. É membro experiente de conselhos de administração, equipes de liderança de risco global e comitês de cibersegurança, risco operacional e GDPR.

Manoj Satnaliwala

Satnaliwala é chefe executivo de auditoria e vice-presidente sênior de auditoria interna da Caliber Home Loans, e é responsável por todas as atividades de auditoria, trabalhando diretamente com o comitê de auditoria. Antes de seu cargo atual, liderou a função de auditoria do Radian Group Inc., a terceira maior seguradora de hipotecas de capital aberto dos Estados Unidos, e foi diretor de auditoria interna da PwC, onde gerenciou a validação de controles para auditoria interna como parte do projeto CCAR para uma grande holding bancária.

Introdução

Novas propostas regulatórias podem ter grandes consequências

O ciclo de notícias em 2022, e, na verdade, dos últimos anos, tem visto pouca positividade, e as ciberameaças têm sido fonte de preocupação em conjunto com a crise da Ucrânia, ameaças persistentes do COVID-19 e as crescentes tensões entre EUA e China. Juntas, essas variáveis e muitas outras se combinaram para dar à cibersegurança um lugar significativo — e até de liderança — nos mapas de riscos do auditor interno.

No entanto, 2022 também teve avanços relacionados à cibersegurança que prometem impactar um amplo espectro de organizações, que exigirão maior esforço para entender e cujas implicações levarão tempo para compreender totalmente. Entre elas, estão duas propostas regulatórias da Comissão de Valores Mobiliários dos EUA (*Securities and Exchange Commission* – SEC). A segunda proposta é especialmente digna de destaque, porque exigiria que empresas de capital aberto que operem nos EUA divulgassem suas políticas de cibersegurança, procedimentos e estratégias de governança, bem como o conhecimento e experiência do conselho - se houver - no domínio da cibersegurança. Se implantadas (como provavelmente serão de alguma forma), organizações de capital aberto, independentemente da indústria ou tamanho, estarão sujeitas a essas novas regras. Sem exagero algum, esses avanços representam um novo capítulo para a cibersegurança e um tópico novo — talvez, familiar — para a comunidade de auditoria interna, que desempenhará um papel fundamental na navegação de suas organizações através deste desafio.

Embora este não seja um desafio a ser levado despreocupadamente, a auditoria interna felizmente entende as ferramentas e habilidades necessárias para prestar avaliação sobre essa área de risco em evolução. A Parte 1 da série Brief de Conhecimento Global de três Partes do IIA sobre cibersegurança apresenta uma visão geral das novas propostas da SEC, incluindo as consequências que terão quanto à regulamentação de relatórios de cibersegurança nos EUA e no exterior. Também explora como os auditores internos podem desempenhar um papel importante para ajudar suas organizações a gerenciar o cenário de conformidade alterado que pode vir a ser criado por novas regulamentações em breve.

Preparando o Palco

Cibersegurança domina o cenário de risco

O maior risco do nosso tempo

A cibersegurança permanece em primeiro lugar em todos os níveis de todas as organizações em todas as indústrias em 2022, e essa preocupação é claramente refletida nos dados do *2022 North American Pulse of Internal Audit (Pulse)*[1] do IIA. Ao classificar o nível de risco dos 13 principais riscos para suas organizações, os líderes de auditoria interna que responderam à pesquisa Pulse classificaram os riscos relacionados à tecnologia entre os três principais – cibersegurança, TI e relacionamentos com terceiros (que geralmente incluem serviços de TI). Mesmo entre esses três primeiros, a cibersegurança conquistou facilmente o primeiro lugar, com 85% dos entrevistados classificando-a como risco alto ou muito alto, 24 pontos percentuais acima das classificações de TI, o segundo risco mais bem avaliado.

Tal preocupação é justificada. Em 2021, ciberataques de quase todos os tipos aumentaram em margens alarmantes. De acordo com o *2022 SonicWall Cyber Threat Report*[2], o número de ameaças criptografadas em 2021 aumentou 167% (10,4 milhões de ataques), o ransomware aumentou 105% (623,3 milhões de ataques), o cryptojacking (ataques em computadores para minerar criptomoedas) aumentou 19% (97,1 milhões de ataques), as tentativas de intrusão aumentaram 11% (5,3 trilhões de ataques) e o malware direcionado à Internet das Coisas (IoT) aumentou 6% (60,1 milhões de ataques).

Além disso, todos esses ataques têm um custo significativo pelo dano que causam. Os custos anuais totais de ciberataques devem chegar a US$ 10,5 trilhões até 2025, um crescimento médio de 15% ano a ano, de acordo com a versão mais recente do Cybersecurity Almanac de 2022[3] da Cisco/Cybersecurity Ventures.

E isso nem leva em consideração as mudanças dramáticas no cenário geopolítico que afetam a cibersegurança. Mesmo antes da invasão da Ucrânia pela Rússia, havia amplas evidências de que suspeitas de ciberataques patrocinados pelo Estado, com altos níveis de sofisticação, estavam aumentando em impacto e frequência. A violação de 2020 dos sistemas da SolarWind sediada no Texas, conduzida por um grupo de hackers supostamente[4] dirigido pelo Serviço de Inteligência Estrangeira da Rússia, comprometeu a infraestrutura digital de até 18.000 clientes[5] — incluindo a Microsoft, Cisco, Intel, Deloitte, partes do Pentágono, Departamento de Segurança Interna dos EUA, Departamento de Energia e a Administração Nacional de Segurança Nuclear —, passando sem detecção por meses.

Em 2021, outro grande ataque patrocinado pelo Estado contra uma empresa dos EUA foi visto na Colonial Pipeline Co.[6] O ataque interrompeu temporariamente o fluxo de quase metade dos suprimentos de gasolina e combustível de aviação para a Costa Leste. Por fim, a Colonial pagou um resgate de quase US$ 5 milhões ao grupo de hackers DarkSide para restaurar a rede e recuperar os dados.

---

[1] The IIA, *2022 North American Pulse of Internal Audit*, março de 2022, https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of-internal-audit/

[2] SonicWall, *2022 SonicWall Cyber Threat Report*, 2022, https://www.sonicwall.com/2022-cyber-threat-report/.

[3] Steve Morgan, "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics," Cybersecurity Ventures, Cisco, 19 de janeiro de 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/.

[4] Joe Hernandez, "The Russian Hacker Group Behind the SolarWinds Attack Is At It Again, Microsoft Says," NPR, atualizado em 25 de outubro de 2021, https://www.npr.org/2021/10/25/1048982477/russian-hacker-solarwinds-attack-microsoft.

[5] Isabella Jibilian e Katie Canales, "The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal," Business Insider, atualizado em 15 de abril de 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[6] Andrew Marquardt, "As Biden Warns of a Russian Cyberattack, What Are the Precedents? Here's What Happened When a Major Oil Pipeline Was Hacked Last Year," Fortune, 22 de março de 2022, https://fortune.com/2022/03/22/biden-warns-russian-cyber-attack-pipeline/.

Ponto de Ruptura Geopolítico

Desde esses ataques, as preocupações com a Rússia só aumentaram, atingindo um pico com a invasão da Ucrânia. De fato, a agressão da Rússia contra a Ucrânia inclui guerra cibernética – um ataque em larga escala à rede de energia elétrica[7] da Ucrânia — além da guerra tradicional, e há uma preocupação crescente de que a Rússia possa retaliar contra uma miríade de sanções econômicas impostas pela OTAN e pelos EUA. Antes da entrada formal da Rússia na Ucrânia, a *Cybersecurity and Infrastructure Security Agency* (CISA) emitiu um raro alerta "*Shields Up*"[8], alertando as empresas dos EUA de todos os tamanhos a adotar uma postura defensiva em relação à cibersegurança e à proteção de ativos críticos. "Recentes Orientações publicadas pela CISA e outras fontes não classificadas revelam que os agentes de ameaças patrocinados pelo Estado russo têm como alvo as seguintes indústrias e organizações, nos Estados Unidos e em outras nações ocidentais: pesquisa de COVID-19, governos, organizações eleitorais, saúde e farmacêutica, defesa, energia, videogames, instalações nucleares, instalações comerciais, água, aviação e manufatura crítica", escreveu a CISA em uma declaração[9] de março de 2022, avaliando as ciberameaças russas.

Em maio de 2021, o presidente Biden assinou uma ordem executiva[10] criada para melhorar o estado da segurança nacional nos EUA. A ordem abordava especificamente a necessidade de que agências governamentais revisem e desenvolvam novas diretrizes e normas para cibersegurança, e de que as organizações se concentrem em aprimorar a segurança da cadeia de suprimentos de software e do compartilhamento de informações sobre ameaças. Mais recentemente, o Presidente também emitiu uma declaração reiterando a ameaça russa à cibersegurança e destacando a evolução das orientações[11] da CISA sobre o assunto.

A Rússia não é o único estado a supostamente apoiar ciberataques desestabilizadores. De acordo com um relatório[12] de 2021 do The Evanina Group, a China tornou-se cada vez mais agressiva na frente cibernética, especialmente no que diz respeito à aquisição de dados pessoais e privacidade de dados.

"A capacidade da China de obter de forma holística nossa Propriedade Intelectual e Segredos Comerciais por meio de métodos híbridos ilegais, legais e sofisticados é diferente de tudo que já testemunhamos", disse William Evanina, ex-diretor do Centro Nacional de Contrainteligência e Segurança.

Evanina fez referência a vários incidentes cibernéticos ligados ao Partido Comunista Chinês, incluindo a violação cibernética da Equifax em 2017; uma campanha de 2011-2018 de quatro cidadãos chineses para invadir dezenas de empresas, universidades e entidades governamentais; e uma campanha cibernética patrocinada pelo Estado em 2011-2013, atacando empresas de oleodutos e gasodutos dos EUA (o Departamento de Justiça divulgou um relatório sobre esse incidente em julho de 2021). Evanina também se referiu a um relatório de julho de 2021 da *National Security Agency* (NSA), do *Federal Bureau of Investigation* (FBI) e da CISA que divulgou mais de 50 táticas e ferramentas cibernéticas usadas por hackers patrocinados pelo Estado chinês contra os EUA.

É nesse ambiente cibernético complexo e globalmente perigoso que a SEC tomou medidas históricas para abordar a saúde cibernética e a preparação em todo o cenário organizacional, particularmente no que diz respeito ao reporte à SEC e (em alguns casos) ao público. Essas medidas são as primeiras desse tipo e podem ter consequências significativas, não apenas para empresas americanas de capital aberto, mas também para empresas do mundo todo.

---

[7] IANS, "Ukraine Foils Russia-backed Cyber Attack on Power Grid," 14 de abril de 2022, https://www.nationalheraldindia.com/international/ukraine-foils-russia-backed-cyber-attack-on-power-grid.
[8] Cybersecurity and Infrastructure Security Agency (CISA), "Shields Up," acessado em 22 de abril de 2022, https://www.cisa.gov/shields-up.
[9] Cybersecurity and Infrastructure Security Agency (CISA), "Russia Cyber Threat Overview and Advisories," Department of Homeland Security, acessado em 22 de abril de 2022, https://www.cisa.gov/uscert/russia.
[10] U.S. General Services Administration (GSA), "Executive Order 14028: Improving the Nation's Cybersecurity," 12 de maio de 2021, https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity.
[11] Cybersecurity and Infrastructure Security Agency (CISA), "Shields Up."
[12] William Evanina, "Statement of William R. Evanina, CEO, The Evanina Group, Before the Senate Select Committee on Intelligence, at a Hearing Concerning the Comprehensive Threat to America Posed by the Communist Party of China (CCP), The Evanina Group, 4 de agosto de 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf.

A Grande Mudança

Um primeiro passo histórico quanto à divulgação de incidentes cibernéticos

As propostas

Em um período de dois meses, a SEC divulgou duas propostas sobre cibersegurança há muito esperadas no setor empresarial. A primeira proposta[13], revelada em fevereiro de 2022, concentra-se em consultores de investimento registrados, empresas de investimento registradas e empresas ou fundos de desenvolvimento de negócios. De acordo com as regras propostas, os consultores e fundos seriam obrigados a:

- Adotar e implantar políticas e procedimentos escritos de cibersegurança, projetados para lidar com riscos de cibersegurança que possam prejudicar clientes de consultoria e investidores de fundos.
- Reportar à SEC incidentes significativos de cibersegurança que afetem o consultor, ou seus clientes de fundos ou fundos privados, em um novo formulário confidencial.
- Divulgar publicamente, em seus folhetos e declarações de registro, os riscos de cibersegurança e incidentes significativos de cibersegurança ocorridos nos dois últimos exercícios fiscais.

Além disso, a proposta estabeleceria novos requisitos de manutenção de registros para consultores e fundos, criados para melhorar a disponibilidade de informações relacionadas à cibersegurança, bem como ajudar a facilitar os recursos de inspeção e fiscalização da SEC.

"O risco cibernético está relacionado a cada parte da missão de três partes da SEC e, em particular, aos nossos objetivos de proteger os investidores e manter os mercados ordenados", disse o presidente da SEC, Gary Gensler, em um comunicado à imprensa[14]. "As regras e alterações propostas foram criadas para aumentar a preparação para a cibersegurança e podem melhorar a confiança dos investidores na resiliência dos consultores e dos fundos contra ameaças e ataques à cibersegurança."

Embora essas regras reflitam – ainda que implicitamente – as expectativas da SEC sobre como entidades regulamentadas devem gerenciar os riscos de cibersegurança e reportar incidentes de cibersegurança, a segunda proposta torna essas expectativas explícitas. Dirigida a todas as empresas de capital aberto, a segunda proposta[15], emitida em março de 2022, busca "aprimorar e padronizar as divulgações sobre o gerenciamento de riscos de cibersegurança, estratégia, governança e reporte de incidentes de cibersegurança por empresas públicas sujeitas aos requisitos de reporte da Lei da Bolsa de Valores de 1934". Para isso, as novas regras exigiriam que as empresas públicas fornecessem divulgações sobre:

- As políticas e procedimentos da empresa para identificar e gerenciar riscos de cibersegurança. Incluída nas regras está uma lista extensa, mas não absoluta, de estratégias, políticas e procedimentos de gerenciamento de riscos que podem estar sujeitos a divulgação, incluindo:
    - Se o registrante possui um programa de avaliação de riscos de cibersegurança.

[13] U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," 9 de fevereiro de 2022, https://www.sec.gov/rules/proposed/2022/33-11028.pdf.
[14] U.S. Securities and Exchange Commission (SEC), "SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds," comunicado à imprensa, 9 de fevereiro de 2022, https://www.sec.gov/news/press-release/2022-20.
[15] U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," 9 de março de 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

- Se o registrante contrata assessores, consultores, auditores ou outros terceiros em conexão com qualquer programa de avaliação de riscos de cibersegurança.
- Se o registrante possui políticas e procedimentos para supervisionar e identificar os riscos de cibersegurança associados ao uso de qualquer prestador de serviços terceirizados.
- Se o registrante realiza atividades para prevenir, detectar e minimizar os efeitos de incidentes de cibersegurança.
- Se o registrante possui planos de continuidade de negócios, contingência e recuperação para o caso de um incidente de cibersegurança.
- Se incidentes anteriores de cibersegurança permitiram mudanças na governança, políticas e procedimentos ou tecnologias do registrante.
- Se os riscos e incidentes relacionados à cibersegurança afetaram ou têm probabilidade razoável de afetar os resultados operacionais ou a condição financeira do registrante.
- Se os riscos de cibersegurança são considerados como parte da estratégia de negócios, planejamento financeiro e alocação de capital do registrante.

- O papel da gestão na implantação de políticas e procedimentos de cibersegurança, incluindo:
  - Se determinados cargos de gestão ou comitês são responsáveis por mensurar e gerenciar os riscos de cibersegurança.
  - Se o registrante designou um diretor de segurança da informação ou alguém em cargo comparável.
  - Se os processos por meio dos quais essas pessoas ou comitês recebem informações e realizam o monitoramento da prevenção, mitigação, detecção e remediação de incidentes de cibersegurança.
  - Se essas pessoas ou comitês reportam ao conselho de administração ou a um comitê do conselho de administração sobre riscos de cibersegurança, bem como a frequência com que reportam.
  - Se todo o conselho, membros específicos do conselho ou um comitê do conselho são responsáveis pela supervisão dos riscos de cibersegurança.
  - Se o conselho é informado sobre os riscos de cibersegurança e a frequência de suas discussões sobre esse risco.
  - Se e como o conselho ou comitê do conselho considera os riscos de cibersegurança como parte de sua estratégia de negócios, gerenciamento de riscos e supervisão financeira.

- A experiência em cibersegurança do conselho de administração, se houver, e sua supervisão dos riscos de cibersegurança. Isso inclui informações sobre:
  - Se o conselho tem experiência de trabalho em cibersegurança.
  - Se o conselho obteve uma certificação ou diploma em cibersegurança.
  - Se o conselho tem conhecimento, habilidades ou outro histórico em cibersegurança.

Além disso, a proposta inclui uma emenda ao Formulário 8-K, que exigiria que empresas públicas divulgassem incidentes de cibersegurança em quatro dias úteis, assim como já são obrigados a fazer para qualquer outro evento material não programado. Tais divulgações incluiriam:

- Quando o incidente foi descoberto e se está em andamento.
- Uma breve descrição da natureza e escopo do incidente.
- Se algum dado foi roubado, alterado, acessado ou usado para qualquer outra finalidade não autorizada.

- O efeito do incidente nas operações da empresa.
- Se a empresa corrigiu ou está corrigindo o incidente.

Essas divulgações, de acordo com a SEC, forneceriam aos investidores informações "consistentes, comparáveis e úteis para decisões". "Hoje, a cibersegurança é um risco emergente que os emissores públicos devem enfrentar cada vez mais", disse Gensler[16]. "A interconexão de nossas redes, o uso da análise preditiva de dados e o desejo insaciável por dados estão apenas acelerando, colocando em risco nossas contas financeiras, investimentos e informações privadas. Os investidores querem saber mais sobre como os emissores estão gerenciando esses riscos crescentes."

A importância histórica

De muitas formas, a estrutura dessas regras descritas reflete outras regras de divulgação da SEC, como aquelas relacionadas a condições financeiras e resultados operacionais (Sarbanes-Oxley), informações privilegiadas e forças, fraquezas, oportunidades e ameaças organizacionais. No entanto, dar o passo adicional de elevar os riscos de cibersegurança a ponto de exigir tais divulgações é algo sem precedentes.

"Os EUA são provavelmente o primeiro país, e eu diria o único país do mundo, a regular a cibersegurança", diz Andy Watkin-Child, sócio fundador do The Augusta Group e da Parava Security Solutions, e fundador da *Cybersecurity Maturity Model Certification Europe* (CMMC Europa). "As empresas nos EUA podem estar familiarizadas com o Regulamento Geral de Proteção de Dados (GDPR) da UE e podem ser rápidas em combinar essas propostas, mas a proteção de dados e a cibersegurança são dois paradigmas diferentes. Há uma grande diferença e, além do Regulamento de Gestão Financeira do Departamento de Defesa (DoD) – que poderia resultar na investigação até de empreiteiros estrangeiros pelo Departamento de Justiça por vulnerabilidades de cibersegurança –, não há nada parecido no universo da cibersegurança."

Watkin-Child também explica como o significado das novas regras pode ter fortes efeitos em cascata no exterior. "A crise da Ucrânia provou que a cibersegurança é uma arma e, de fato, a OTAN a considera um grau de operação desde 2016", diz ele. "A cibersegurança é uma ferramenta de ataque, assim como as armas nucleares. O problema é que, por ser um domínio de operação, representa uma grave ameaça às infraestruturas nacionais. A proposta da SEC está atingindo os grandes players primeiro – as firmas de trade –, mas minha crença é que isso se espalhará para organizações além da alçada da SEC, porque o cenário de negócios, bem como o cenário federal, está tão entrelaçado em nível global."

Na guerra, diz Watkin-Child, não se pode considerar a cibersegurança como parte de apenas um único exército; se um aliado está vulnerável, isso tem um efeito direto sobre toda a operação conjunta. A proteção da cibersegurança para empresas públicas – e privadas – não é diferente. "Se os sistemas de armas americanos não podem ser hackeados, mas os sistemas britânicos podem, não faz sentido ter proteção alguma", diz ele. "Há uma razão pela qual o presidente [dos EUA] falou com a OTAN sobre, entre outras coisas, normas comuns de cibersegurança. É a coisa certa a se fazer, porque, se uma entidade como a Rússia usar o setor comercial para atacar geradores de energia, por exemplo, sua água, sua eletricidade, sua gasolina, sua saúde – tudo vai embora."

Essas consequências potenciais são obviamente de natureza macro, mas também é importante não desconsiderar as consequências no nível da organização. E, apesar do que se possa sentir ao ver as extensas listas de elementos que podem ter sua inclusão justificada nas divulgações de cibersegurança, nem todas as consequências são negativas.

"Claro, há o lado legal das divulgações", diz Watkin-Child, "mas, como citado nas propostas, você não está apenas reportando à SEC. Você está reportando a todos os participantes do mercado que possam ter impacto sobre seus negócios. A comunidade de investimentos, agências de classificação de crédito, companhias de seguros – todos verão, juntamente com a SEC, o quão bom você é em cibersegurança, ou não, conforme o caso. Essa transparência traz riscos, mas também representa uma oportunidade."

[16] Gary Gensler, "Statement on Proposal for Mandatory Cybersecurity Disclosures," U.S. Securities and Exchange Commission (SEC), 9 de março de 2022, https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

O Papel da Auditoria Interna Segue Consistente

Identificar, avaliar, comunicar

As ferramentas estão em prática

A Lei Sarbanes-Oxley de 2002 (SOX) forneceu responsabilidades adicionais e abriu novas oportunidades para as funções de auditoria interna agregarem valor às suas organizações. De fato, conforme as organizações navegavam pela nova legislação, a auditoria interna, para muitos, tornou-se sinônimo de conformidade com a SOX. Devido à natureza das novas propostas da SEC, há motivos para acreditar que o mesmo possa acontecer no domínio da cibersegurança.

À primeira vista, isso pode parecer uma impossibilidade pelo menos no curto prazo, devido à natureza complexa do campo da cibersegurança. De acordo com os entrevistados da pesquisa Pulse[17], a cibersegurança representa, em média, apenas 9% da alocação do plano de auditoria em organizações de capital aberto, o que representa um aumento de 7% em relação aos três anos anteriores, mas ainda fica muito abaixo dos 35% alocados para o reporte financeiro. Há várias razões pelas quais isso pode acontecer, como limitações orçamentárias, falta de recursos suficientes e falta de conhecimento ou experiência.

O valor real que a auditoria interna pode fornecer, no entanto, não é necessariamente através do conhecimento de cibersegurança, mas do conhecimento da identificação de riscos, comunicação de riscos e avaliação de controles para lidar com os riscos. De fato, essas são exatamente as coisas que as propostas da SEC desejam enfatizar para um risco específico.

"É importante perceber que essas propostas não são realmente sobre cibersegurança, são sobre o gerenciamento de riscos de cibersegurança", diz Watkin-Child. "Quando as pessoas pensam em cibersegurança, todas pensam em implantar controles e consertar coisas. O que a SEC está buscando é algo completamente diferente; está buscando que as organizações avaliem seus riscos de cibersegurança. Eles querem que os conselhos das organizações tenham estruturas de governança para avaliar e garantir a supervisão de seu programa de gerenciamento de riscos de cibersegurança, seja qual for a forma que ele assuma".

"O que a SEC quer é que os conselhos assumam a responsabilidade pela supervisão e avaliem o resto", diz Manoj Satnaliwala, chefe executivo de auditoria da Caliber Home Loans, Inc. "A lacuna não está realmente nas normas de cibersegurança – há frameworks para orientar organizações, como o *NIST Cybersecurity Framework*. A verdadeira lacuna está na prestação de contas, que pode rapidamente se tornar uma gangorra de responsabilidade."

O papel da auditoria interna pode ajudar a trazer equilíbrio a essa gangorra. "Os conselhos e a gestão precisam de ajuda. A auditoria interna, por meio da avaliação, garante a prestação de contas e, por meio da maior visibilidade em toda a organização, promove a propriedade compartilhada do risco", diz Satnaliwala. "O risco é diferente, mas o papel da auditoria interna realmente segue consistente. As funções de auditoria não precisam começar do zero, e não é razoável esperar que cada departamento de auditoria interna já esteja mergulhado em um programa de cibersegurança, mas quanto a esse desafio, é buscar fazer um pouco mais do que apenas analisar as propostas da SEC, e perguntar: 'quais são as expectativas

[17] The IIA, "2022 North American Pulse of Internal Audit".

da SEC?' Desde que já existam pelo menos alguns recursos de cibersegurança, não acho que sejam necessárias mudanças na função média de auditoria interna, além de ajustar as abordagens para garantir a cobertura adequada dos riscos."

No entanto, o acesso a esses recursos de cibersegurança é geralmente mais fácil de falar do que de fazer. Desenvolver qualquer grau de especialização em cibersegurança por meio de treinamento e certificações não vai acontecer da noite para o dia e, especialmente para pequenas funções de auditoria interna com orçamentos limitados para recrutar talentos caros e de alta demanda, as opções para desempenhar qualquer tipo de função além da conformidade orientada a processos são limitadas. Nesses casos, a auditoria interna deve ter uma compreensão abrangente de onde o conhecimento pode ser acessado da melhor forma. Isso pode ser:

- **Dentro da própria base de talentos da organização.** Aqueles com experiência em uma natureza mais tradicional de auditoria de TI geralmente têm a base de conhecimento para concluir o treinamento técnico de cibersegurança com relativa rapidez. Além disso, certos fundamentos de cibersegurança podem ser incorporados em áreas como gestão de mudanças, controles de acesso, operações de TI e recuperação de desastres, o que pode reduzir a necessidade de terceirização a longo prazo.
- **Por meio da colaboração com a segunda linha e com funções de auditoria externa confiáveis.** Embora a independência e a objetividade da auditoria interna devam ser mantidas em conformidade com as *Normas Internacionais para a Prática Profissional de Auditoria Interna* (IPPF), estabelecer uma relação de trabalho mais colaborativa com funções relevantes, como a TI, pode dar aos auditores acesso indireto a competências técnicas que, de outra forma, poderiam ser difíceis ou caras de obter.

Conclusão

Hora de se preparar

A cibersegurança, como tópico, está sempre evoluindo conforme maus feitores continuam inovando em suas abordagens e as empresas continuam inovando para frustrá-los. No entanto, conforme a história da cibersegurança continua sendo escrita, 2022 será lembrado pelos marcos alcançados em um esforço para neutralizar as terríveis tendências vistas no cenário de negócios. Embora as propostas da SEC devam completar um período de 60 dias para comentários antes que regras oficiais sejam emitidas, deve haver pouca surpresa para as empresas de capital aberto e suas funções de auditoria interna.

A auditoria interna pode e deve usar o tempo que tem, se ainda não o fez, para fazer um balanço de todo o escopo dos ativos de sua organização que devem ser contabilizados em uma estratégia de cibersegurança. Sem esse conhecimento, os auditores internos terão dificuldade em avaliar se os atuais controles, políticas e estratégias de governança relacionados à cibernética são suficientes. Essas avaliações não são importantes apenas para fins de segurança organizacional, mas também para toda a comunidade do mercado. O mundo está se tornando mais interconectado a cada dia, e isso significa que as responsabilidades em relação a riscos como a cibersegurança são amplamente compartilhadas. Afinal, como a história tem mostrado repetidas vezes, a violação de uma organização pode ter um impacto muito real na segurança de outra.

Uma corrente é tão forte quanto seu elo mais fraco.

PARTE 2

Parceiros Críticos — Auditoria Interna e CISO

Sobre os Especialistas

Jerry Perullo

Jerry Perullo é o fundador da *Adversarial Risk Management*, uma empresa de estratégia e governança de programas de cibersegurança que permite que empresas em crescimento estabeleçam rapidamente programas maduros de cibersegurança. Antes de fundar a *Adversarial*, Perullo se aposentou como Diretor de Segurança da Informação da *IntercontinentalExchange* (NYSE:ICE), depois de 20 anos construindo e liderando o programa de cibersegurança em uma família global de infraestrutura econômica crítica, incluindo a Bolsa de Valores de Nova York. Certificado pela NACD como *Directorship Certified*®, Perullo também atuou no Conselho de Administração do *Financial Services Information Sharing and Analysis Center* (FS-ISAC) por 6 anos, mais recentemente como Presidente. Perullo também dá palestras no Georgia Institute of Technology, onde é Professor da prática na *School of Cybersecurity and Privacy* e compartilha suas experiências com líderes de risco tecnológico por meio de seu podcast *lifeafterCISO.com*.

Hassan NK Khayal, CIA, CRMA, CFE

Hassan NK Khayal é Gerente de Auditoria Interna baseado em Dubai. Hassan foi apresentado pelo *Institute of Internal Auditors* (IIA) como um dos 15 líderes globais com menos de 30 anos. Hassan possui um BBA, um MBA e um certificado em Estudos do Oriente Médio. Também é CIA, CRMA e CFE. Possui certificações profissionais em *Robotic Process Automation* (RPA), *Data Analytics*, *Internet of Things* (IoT), Gestão da Qualidade, Saúde e Segurança, Gestão Ambiental e Gerenciamento de Riscos.

Alan Maran

Alan é o Chefe de Auditoria Interna (CAE) da Chewy, Inc. Está na empresa desde janeiro de 2019. Nessa função, é responsável por supervisionar as atividades gerais de Estratégia e Execução da Função de Auditoria Interna, incluindo a execução de avaliações Ágeis de riscos da empresa, fornecer suporte consultivo contínuo e tempestivo a várias atividades apoiadas pela Gestão; e avaliação sobre a adequação dos controles sobre os principais riscos identificados para a organização, alinhamento com operações, sistemas corporativos e governança de TI, risco e conformidade (GRC) em toda a empresa, foco contínuo no desenvolvimento dos membros da Equipe de Auditoria Interna, com maior foco em análise de dados, cibersegurança e privacidade de dados. Alan é um executivo de auditoria experiente, com mais de 22 anos de experiência em empresas de comércio eletrônico, *fintech*, tecnologia e manufatura, que continua apaixonado por aprender. Antes de ingressar na Chewy, ocupou cargos de liderança progressivos, iniciando sua carreira na Ernst & Young, LLC, e depois seguindo para outros cargos de Auditoria Interna em organizações multinacionais da Fortune 500. Ele tem um MBA; e mestrado em Finanças pela Washington State University; é um *Certified Fraud Examiner* (CFE), um *Certified Blockchain Expert* e afiliado a filiais locais do Institute of Internal Auditors.

Srini Srinivasan, PMP, CBIP

Srini Srinivasan é o *Chief Information Security and Data Officer* da Chewy, Inc. Está na empresa desde outubro de 2019, quando ingressou como Chefe de Segurança, Dados e Sistemas Corporativos. Nessa função, é responsável por supervisionar a segurança da informação, gerenciar plataformas de dados e análises, sistemas corporativos e governança de TI, risco e conformidade (GRC) em toda a empresa. Srini é um executivo de tecnologia experiente, com mais de 25 anos de experiência em comércio eletrônico, serviços bancários e financeiros, varejo e marketing. Antes de ingressar na Chewy, ocupou cargos de liderança no Citizens Financial Group. Possui mestrado em Ciência da Computação pela Bharathidasan University e MBA pela Bentley University.

Introdução

Parcerias de cibersegurança são essenciais para o sucesso

A cibersegurança permanece entre os principais riscos para todas as organizações. As pesquisas refletem consistentemente os esforços implacáveis e descarados de cibercriminosos para invadir dados confidenciais ou levar pessoas destreinadas e desavisadas a divulgar informações confidenciais ou permitir acesso a agentes mal-intencionados.

Por exemplo, o *Data Breach Investigations Report* de 2022, da Verizon, reflete um aumento surpreendente de 13% nas violações relacionadas a *ransomware* em 2021, maior do que nos últimos cinco anos combinados. No entanto, o relatório conclui que os métodos mais bem-sucedidos de ataques de *ransomware* permanecem consistentes – abuso de software de compartilhamento de desktop e acesso remoto (40%) e e-mail (35%), de acordo com o relatório da Verizon.[18]

A nova orientação do The IIA, *Auditing Cybersecurity Operations: Prevention and Detection* (GTAG), foi criada para ajudar as organizações a examinar e priorizar a avaliação sobre as operações de cibersegurança. Ela visa ajudar os auditores internos a definir operações de cibersegurança, identificar seus componentes, considerar orientações de controle relevantes em frameworks de controle de TI e entender as abordagens para auditar operações de cibersegurança.

Uma chave para melhorar a avaliação da cibersegurança não abordada na orientação é ter um relacionamento saudável entre os chefes de auditoria interna e os *chief information security officers* (CISOs). Essa relação potencialmente simbiótica pode ajudar a alinhar a auditoria interna e a segurança da informação em frameworks, riscos e controles, ao mesmo tempo em que dá suporte ao gerenciamento do perfil de risco crescente de cibersegurança.

Este *Global Knowledge Brief* examina os benefícios de um forte relacionamento entre os chefes de auditoria interna e suas contrapartes da segurança da informação, analisa os caminhos para estabelecer e nutrir tais relacionamentos garantindo a independência da auditoria interna, e avalia como essas parcerias podem agregar valor à organização.

[18] "3 Takeaways From the 2022 Verizon Data Breach Investigations Report," J. Mack, Rapid7, 31 de maio de 2022, https://www.rapid7.com/blog/post/2022/05/31/3-takeaways-from-the-2022-verizon-data-breach-investigations-report/.

O Argumento da Cibersegurança Coletiva

O risco cibernético exige abordagem que englobe toda a empresa

A cibersegurança continua sendo uma área de risco crescente e em evolução, com cada ano revelando esquemas mais sofisticados e abundantes dos cibercriminosos. Não faltam estatísticas para mostrar que as organizações continuam vulneráveis a ciberataques. Ao mesmo tempo, cresce a pressão para que organizações de toda a indústria adotem estratégias de negócios orientadas por dados que dependem muito da coleta, gerenciamento, análise e utilização de dados, ao mesmo tempo alavancando novas tecnologias para melhorar o desempenho e os resultados.

Assim como em outras áreas de risco significativo, o risco cibernético deve ser entendido e gerenciado em toda a organização. No entanto, poucas organizações adotam uma abordagem corporativa ao gerenciamento da cibersegurança, de acordo com o *"The State of Cyber Resilience"*, um relatório da Microsoft e da Marsh, firma corretora de seguros e de gerenciamento de riscos. Com base em uma pesquisa[19] com mais de 600 tomadores de decisões de risco cibernético, o relatório descobriu que apenas cerca de 4 em cada 10 organizações envolvem o jurídico, planejamento corporativo, finanças, operações ou a gestão da cadeia de suprimentos na elaboração de planos de risco cibernético.[20]

"Uma coisa que impede a confiança é que a maioria das empresas não adotou uma abordagem corporativa ao risco cibernético; uma que, em sua essência, seja sobre comunicação de base ampla e promova a colaboração e alinhamento entre os stakeholders durante os principais momentos de tomada de decisão em sua jornada de resiliência cibernética,"[21] de acordo com o relatório.

Entre as principais tendências de risco identificadas no relatório:

"As metas corporativas específicas da cibernética – incluindo medidas de cibersegurança, seguros, dados e análises e planos de resposta a incidentes – devem estar alinhadas para criar resiliência cibernética, em vez de simplesmente prevenir incidentes, pois toda organização pode esperar um ciberataque."[22]

Para apoiar uma abordagem eficaz que englobe toda a empresa, os chefes de auditoria interna podem contribuir significativamente ao estabelecer e nutrir relacionamentos com os CISOs. Tais relacionamentos devem ser baseados na compreensão mútua, em seus objetivos e no respeito.

O CISO veterano e fundador da Adversarial Risk Management, Jerry Perullo, antes da Intercontinental Exchange (NYSE:ICE), controladora da NYSE, disse que comunicações ruins ou entendimentos pouco claros sobre segurança da informação e funções de auditoria interna podem prejudicar o alinhamento na cibersegurança. Por outro lado, um bom relacionamento entre os chefes de auditoria interna e de segurança da informação abre as portas para uma compreensão mais profunda das metas, estratégia, operações e políticas que podem tornar a auditoria interna - e, consequentemente, suas descobertas e recomendações - mais relevante para os líderes de risco cibernético, a gestão executiva e o conselho, disse ele. Além disso, um forte relacionamento entre as equipes de auditoria interna e segurança da informação expande o conhecimento da missão crítica de cada área e de como ambas apoiam a cibersegurança geral.

"No final das contas, a auditoria interna quer se informar sobre a segurança da informação", disse Perullo. "Há muitas formas de fazer isso, mas não há forma melhor do que aprender com a própria equipe (de segurança da informação)."

Em seu trabalho de consultoria com startups, Perullo geralmente começa configurando programas de governança para cibersegurança. Isso normalmente envolve a criação de um comitê de governança de segurança cibernética multifuncional, que pode incluir a gestão executiva, finanças, jurídico e segurança da informação. Também costumam incluir executivos seniores de auditoria interna como observadores, disse ele.

[19] "2022 Marsh and Microsoft Cyber Risk Survey"
[20] "The state of cyber resilience," Marsh Microsoft, 2022, https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html?utm_source=forbes&utm_medium=referral-link&utm_campaign=gl-cyber-risk-2022-the-state-of-cyber-resilience.
[21] ibid.
[22] ibid.

Cinco Chaves para o Sucesso

Benefícios de uma relação sólida entre auditoria interna e CISO

A auditoria interna e os CISOs identificam vários benefícios de uma parceria bem elaborada. Os detalhes e a sofisticação dessas parcerias podem variar dependendo do tamanho da organização, do nível de regulamentação em cada indústria ou do perfil de risco de cibersegurança de uma organização. No entanto, surgem cinco áreas em que a colaboração e a cooperação podem criar benefícios claros, independentemente do tamanho da organização ou da indústria em que opera.

Entendendo e alinhando o perfil de risco cibernético da organização

Um perfil de risco é uma análise quantitativa dos tipos de ameaças que uma organização enfrenta. De uma perspectiva de cibersegurança, essa análise identifica ativos e riscos cibernéticos, examina políticas e práticas criadas para gerenciar esses riscos e se esforça para entender quaisquer vulnerabilidades que possam existir. O entendimento da auditoria interna sobre o perfil de risco cibernético fornece uma base para construir um plano de auditoria que não apenas apoie a abordagem geral da organização à cibersegurança, mas que também possa melhorar a relevância e o valor da auditoria interna nessa área crítica.

Alan Maran, chefe de auditoria interna da Chewy, Inc., desenvolveu um forte relacionamento com o CISO da organização, Srini Srinivasan, ao longo dos três anos desde que o varejista online de alimentos para animais de estimação e outros produtos relacionados a animais de estimação abriu seu capital. Srinivasan disse que a segurança da informação fez parceria com a auditoria interna, com o jurídico e outros stakeholders para avaliar e mensurar de forma abrangente o perfil de risco cibernético da empresa com base no Framework de Cibersegurança do NIST.

“Essa é nossa linha de base”, disse Srinivasan. “Depois, estabelecemos um roteiro de três anos para a cibersegurança e a governança, e o adaptamos e aprimoramos com base na avaliação do framework de cibersegurança que fizemos. Agora, fazemos uma avaliação anual para ver se estamos fazendo melhorias nessas áreas de oportunidade, e avaliamos como nossas pontuações gerais de risco se comparam.”

Essa abordagem colaborativa envolvendo a auditoria interna desde o início permitiu uma estratégia mútua que incorpora os serviços de avaliação e assessoria da auditoria interna, com o objetivo de melhorar consistentemente a postura geral de cibersegurança da Chewy.

“Não é uma perspectiva de 'tenho sempre que auditar a TI e a segurança'. Precisamos também apoiá-las", disse Maran. “Do lado da auditoria interna, vemos que somos um parceiro com uma forte mentalidade de apoiar Srini e sua equipe no desenvolvimento de toda uma estratégia.”

Um benefício adicional da colaboração é que a segurança da informação e a avaliação independente estão sendo incorporadas em novos projetos desde o início. Em outras palavras, a segurança da informação, a auditoria interna e os controles de governança não são mais considerações a posteriori, disse Srinivasan.

“O que fazemos é que, conforme as iniciativas do projeto estão em andamento, ambas as nossas equipes estão se envolvendo e fazendo parcerias com as equipes de engenharia, de produtos e de negócios... Quais são as considerações de segurança? Estamos seguindo as melhores práticas?” disse Srinivasan.

Essa abordagem ajuda a identificar, minimizar e, se possível, eliminar riscos cibernéticos, criando processos e controles apropriados conforme o projeto é desenvolvido, disse Srinivasan. “Então, quando o projeto vai ao ar, fica muito fácil para ambas as nossas equipes, porque temos um entendimento sólido. Quando seguimos com avaliações de controle de auditoria ou revisões de acesso ou controles de governança, temos muito mais insights.”

Entendendo os papéis

O relacionamento construído por Maran e Srinivasan foi muito auxiliado pelo fato de a Chewy ser uma empresa de capital aberto relativamente nova, o que proporcionou uma oportunidade de moldar o relacionamento desde o início. Isso também criou uma expectativa de comunicação aberta e frequente entre Maran, Srinivasan e suas equipes.

“Seria uma forma ideal de estabelecer essa transparência e confiança entre os principais stakeholders; por isso, não queríamos deixar essa oportunidade passar”, disse Srinivasan.

Isso não quer dizer que nunca haja divergências. Mas quando os conflitos surgem, o relacionamento torna mais fácil debatê-los e encontrar uma solução que sirva a ambos os lados, disse Srinivasan.

“Para mim, não há qualquer benefício em manter qualquer coisa longe da auditoria interna”, disse ele. “Quanto mais eles sabem sobre o que estamos fazendo. . . maior o nível de apreciação que eles têm. Da mesma forma, do ponto de vista da auditoria interna, posso dizer que acho que não há momentos 'te peguei' por aqui.”

Em última análise, a abordagem colaborativa permite operar de uma forma Ágil, na qual a auditoria interna é parte integrante de um processo em que as deficiências podem ser detectadas e tratadas mais cedo, disse Srinivasan.

Maran acrescenta que a interação franca afirma e reforça a compreensão mútua dos papéis.

“Srini não presume que sabemos tudo, mas, ao mesmo tempo, respeita nossas preocupações e nosso ponto de vista”, disse ele.

Relevância

Oferecer insights e descobertas de avaliação sobre questões críticas no momento certo é um dos maiores desafios da auditoria interna em qualquer área de risco, mas principalmente na cibersegurança. Esse risco em constante evolução e em ritmo acelerado exige que a avaliação seja relevante e tempestiva.

Perullo alertou que os trabalhos de auditoria interna e recomendações relacionadas que não estejam alinhados à missão de cibersegurança da organização podem causar mais danos do que benefícios. Podem criar confusão na segurança da informação sobre o que a auditoria interna deseja ver, principalmente se a auditoria interna não tiver certeza.

“A auditoria interna, inicialmente, pode não ter uma boa ideia do que quer ver”, disse ele. “É melhor colaborar pré-auditoria e observar o processo de governança cibernética, para garantir que as auditorias estejam alinhadas com a missão.”

Hassan Khayal, consultor de auditoria interna com experiência em cibernética, disse que esta é uma área em que a auditoria interna é especialmente vulnerável a críticas. Muito frequentemente, os auditores internos resistem em conhecer membros das equipes de TI ou de segurança da informação e aprender mais sobre o assunto, sob o pretexto de proteger a independência da auditoria interna.

“Eu assumi descaradamente minhas primeiras tarefas e disse à equipe de TI: 'olhe, estou aqui mais para aprender com vocês do que para qualquer outra coisa.' Eu levava a pessoa que tinha entendimento do processo, ou entendimento técnico, para uma conversa amigável no almoço, para que eu entendesse exatamente as partes essenciais do que estavam fazendo.”

Esse processo de educação também ajuda o auditor interno a entender a maturidade da cibersegurança da organização, o que é fundamental para fornecer recomendações relevantes, disse Khayal.

“Se você está falando sobre a empresa de pequeno a médio porte, ou mesmo sobre uma organização maior que não tem capital aberto, há muito que você pode ou deve fazer”, disse ele. “Em um certo ponto, as recomendações podem ser muito agressivas; então, as recomendações que você está fazendo não são realistas.”

Construir um forte relacionamento entre as equipes de auditoria interna e de segurança da informação reduz a probabilidade de trabalhos e recomendações de auditoria irrelevantes ou mal orientados. Esse benefício foi comprovado na Chewy.

“A equipe de Alan e o próprio Alan estão muito familiarizados com nossa estratégia geral de segurança, do ponto de vista tecnológico, o que estamos fazendo a respeito e quais são alguns dos nossos principais riscos”, disse Srinivasan. “Portanto, não temos a enorme lacuna entre as classificações de risco e nossas capacidades internas. Isso continuará nos ajudando a fazer um trabalho melhor, em termos de melhorar o conhecimento geral de nossa equipe ou dos membros de nossa equipe na Chewy, bem como da nossa equipe de liderança.”

Comunicando o conselho e a gestão executiva

A cultura organizacional da Chewy oferece uma visão de risco maior, apoiada por conversas abertas. Maran e Srinivasan assumiram o papel de educar os stakeholders – a gestão executiva e o conselho – sobre sua colaboração e sobre os benefícios que ela gerou.

“Em muitas organizações por aí, as pessoas estão adotando a abordagem em silos. Ela funciona tipo, 'ah, é segurança de TI, então, vamos conversar com o CISO e o CISO cuidará disso.' Mas, em uma perspectiva integrada de gerenciamento de riscos ou de riscos corporativos, qualquer risco que vejamos à empresa pode atingir todo o empreendimento”, disse Maran. “Um ciberataque pode afetar suas operações, suas entregas e suas finanças. Srini também fez um bom trabalho educando a liderança sobre o que estamos fazendo e sobre os riscos que estamos mitigando. Então, dessa perspectiva, tem sido uma colaboração.”

Isso também se traduz em respostas tempestivas e ágeis às mudanças nos cenários cibernéticos regulatórios e de risco. Por exemplo, Maran e Srinivasan estão cada vez mais confiantes de que a organização pode responder às regras de reporte de cibersegurança propostas pela Comissão de Valores Mobiliários dos EUA, divulgadas no primeiro trimestre de 2022.

Essa colaboração também vai além da segurança da informação e da auditoria interna. “Não se limita à segurança da organização”, disse Srinivasan. “Temos outros stakeholders importantes com quem temos parcerias semelhantes, incluindo a equipe de contabilidade e a equipe jurídica. Acho que estabelecer esses relacionamentos transparentes nos prepara muito bem para quando esses regulamentos em evolução e requisitos adicionais entram em cena.”

Embora a liderança da Chewy se beneficie de mensagens consistentes e unificadas, Khayal alerta para perigos significativos de quando a liderança não é mantida atualizada sobre o status e as necessidades de cibersegurança da organização. Quando os líderes não são informados e educados sobre isso, a TI e a cibersegurança podem rapidamente ser vistas simplesmente como centros de custo, disse ele. Quando a auditoria interna evita entender a segurança da informação, é menos provável que preste uma avaliação valiosa e relevante nessa área, disse Khayal. Isso afeta as visões sobre cibersegurança a partir da perspectiva da gestão executiva e do conselho.

Protegendo e respeitando a independência

Khayal, que está se dedicando a se tornar um auditor certificado de sistemas de informação (*certified information systems auditor*– CISA), disse que seu compromisso com a certificação já aumentou sua credibilidade entre os profissionais de TI e de segurança da informação. Também permitiu que interagisse com esses colegas de trabalho em seu nível, tornando mais provável que oferecessem informações que possam ser consideradas muito avançadas ou complexas para um auditor que participa apenas quando realiza um trabalho de auditoria. Além disso, ele não vê essa interação como uma ameaça à sua capacidade de conduzir um trabalho de auditoria independente e objetivo.

“No final das contas, você está no local de trabalho”, disse ele. “Quando dizemos aos auditores que sejam independentes, não acredito, pessoalmente, que estejamos dizendo a eles: ‘você não pode ter amigos no trabalho; você deve sempre almoçar sozinho.'”

Khayal disse que adota essa abordagem em todas as áreas da organização. Ele falará de Linux com a equipe de informática ou de mídias sociais com a equipe de marketing.

“É uma boa oportunidade para se desenvolver profissionalmente, ao mesmo tempo em que mantém relacionamentos”, disse ele. “É como quando dizemos aos nossos clientes de auditoria ou auditados: ‘estamos analisando o processo e as transações; não estamos caçando pessoas'. Então, quando você leva as pessoas para almoçar, você não está assumindo controle do processo ou da transação.”

Na Chewy, a estreita relação de trabalho entre Maran e Srinivasan apoia o entendimento mútuo da necessidade de verificação independente, disse Maran.

“A natureza da nossa profissão é confiar, mas verificar. Do ponto de vista da objetividade, tenho o dever de fazer isso”, disse. “Então, sim, confiamos até um certo nível, especialmente nas coisas incrementais que testamos. Na maioria dos casos, validamos que as coisas não mudaram. Mas continuo testando também a integridade das informações fornecidas pela gestão. Não olhamos para um relatório apenas pelo valor de face; voltamos à fonte, para garantir que estamos obtendo os mesmos resultados que eles, para garantir que seja completo e preciso.”

Em última análise, entender o papel de cada um na organização facilita o processo, disse Maran.

“Há um acordo aqui. Aqui está o que eu preciso fazer. Aqui está a avaliação que preciso fornecer à alta liderança – o conselho, os stakeholders e o comitê de auditoria”, disse ele. “Estamos nos alinhando quanto às auditorias que vamos fazer para o ano. Alinhamos o escopo. Sim, às vezes, conversamos sobre nosso ponto de vista e como o outro o vê, mas raramente discordamos quanto às áreas de risco sobre as quais precisamos prestar avaliação.”

Srinivasan acrescenta que o foco em uma abordagem de cibersegurança baseada em dados pressupõe que haverá um acordo sobre os fatos entre a segurança da informação e a auditoria interna.

“Se houver algum desacordo, precisamos trabalhar e chegar ao mesmo conjunto de fatos”, disse ele. “Então, você pode ter algum nível de subjetividade que, individualmente, podemos dizer: ‘ok, eu sinto que isso é criticidade média, ou criticidade alta, ou criticidade baixa’. Acho que isso leva a uma discussão e a um resultado saudável, em vez de bater de frente sem ter um quadro de referência comum.”

Agregando Valor

Aumentando a resiliência da cibersegurança

Srinivasan disse que sua abordagem desde o início era permanecer fiel à missão de Chewy. Isso significava realizar três coisas: praticar os princípios operacionais internos da empresa, garantir o alinhamento entre a segurança da informação e a auditoria interna e construir confiança por meio da transparência.

“Acho que percorremos um longo caminho, e isso realmente está valendo muito, em termos do que é preciso dos membros da equipe e da liderança para manter uns aos outros atualizados”, disse ele.

Conforme observado anteriormente, o alto grau de comunicação, colaboração e cooperação apoia uma abordagem Ágil que incorpora continuamente a auditoria interna no processo de cibersegurança. Srinivasan observa que as principais forças, como o foco crescente na sustentabilidade, considerações da cadeia de suprimentos, condições de mercado, acontecimentos geopolíticos e mais, exigem abordagens resilientes à cibersegurança e à avaliação relacionada.

“Acho que isso nos obriga a sermos atentos, ágeis, receptivos e relevantes”, disse ele. “Se usarmos uma abordagem clássica de cachoeira, com prazos de entrega mais longos, perderemos o barco. Então, estou feliz pelo nível de engajamento que temos.”

Expandindo o conhecimento

Outro benefício intrínseco da parceria é como ambas as equipes evoluíram e cresceram em sua compreensão e apreciação das abordagens uma da outra para atingir o mesmo objetivo – manter a organização cibernética.

“Estamos sempre verificando o conhecimento técnico um do outro em termos de ‘nós olhamos para isso? Você está pensando nisso? Aqui está o meu ponto de vista sobre esta análise de risco — está alinhado com o seu também?'”, disse Maran. “Então, desde o início, já pensamos no que vamos examinar, e Srini participa das reuniões iniciais. Ele faz parte da conversa antes de começarmos a auditoria. De fato, não há surpresas.”

Mas o verdadeiro valor agregado vem da colaboração, uma vez que os trabalhos de auditoria são executados e a auditoria interna lida diretamente com a equipe de TI e de segurança.

“Do ponto de vista do desenvolvimento de carreira, especialmente com uma mentalidade de TI e de cibersegurança, é realmente muito gratificante, porque você enxerga muito mais do que simplesmente riscar tarefas em um checklist e dizer: 'você fez isso?'”, disse Maran. “Há muito mais. Há interpretação; há expertise técnica que precisa ser bem aplicada, então, acho que é aí que minha equipe aprende muito.”

Conclusão

Um relacionamento saudável entre a auditoria interna e a segurança da informação oferece vários benefícios para a organização, principalmente no alinhamento e compreensão do perfil de risco cibernético da organização – desde vulnerabilidades e oportunidades até maturidade e testes de penetração.

Além disso, um relacionamento sólido pode aumentar a resiliência e a agilidade, caso a organização precise responder a incidentes cibernéticos, mudanças em fatores que influenciam a cibersegurança ou o cenário regulatório em evolução. Ele ajuda a transmitir mensagens consistentes e unificadas à alta administração e ao conselho sobre riscos, necessidades, prioridades e saúde da cibersegurança. A independência da auditoria interna pode ser protegida com sucesso, até mesmo aprimorada, quando ambos os lados desenvolvem uma compreensão e uma apreciação mais profundas das funções, abordagens e deveres. Em última análise, um relacionamento sólido entre os chefes de auditoria e os CISOs pode fortalecer a segurança de TI, apoiando uma abordagem de cibersegurança que englobe toda a empresa.

"A mentalidade está mudando, indo de simplesmente auditar – 'preciso chegar, avaliar e agregar observações significativas' – para realmente dizer: 'esta é minha empresa; é com isso que eu realmente me importo; e é assim que vou ajudar essa equipe a ter sucesso'", disse Maran.

PARTE 3

Resposta e Recuperação de Incidentes Cibernéticos

Sobre os Especialistas

Brian Tremblay

Brian Tremblay lidera o departamento de Conformidade na Onapsis, onde é responsável por ajudar os clientes a entender e navegar pelos desafios e oportunidades criados pela crescente sobreposição de conformidade, cibersegurança e continuidade de negócios, em relação aos controles gerais de TI e questões regulatórias e de conformidade, como Sarbanes- Oxley (SOX) e o Regulamento Geral de Proteção de Dados (GDPR). Antes da Onapsis, foi CAE da empresa de semicondutores de alta tecnologia Acacia Communications. Além de fundar e liderar todas as atividades da função de auditoria interna, ajudou a preparar a organização para abrir capital (incluindo a implantação da SOX) e facilitou a implantação do gerenciamento de riscos corporativos (ERM). Anteriormente, Tremblay foi Diretor de Auditoria Interna da Iron Mountain, supervisionando todas as auditorias e projetos na América do Norte, bem como fazendo contato com gerentes de qualidade globais. Antes, como gerente sênior da Houghton Mifflin Harcourt, criou um departamento de auditoria interna e realizou uma implantação de SOX. No início de sua carreira, trabalhou na Raytheon e na Deloitte.

DaMon Ross Sr.

Em 2020, DaMon Ross Sr. fundou a Cyber Defense International, onde ele e sua equipe alavancam operações de cibersegurança de elite e recursos de inteligência de ciberameaças para fornecer soluções e serviços de cibersegurança acessíveis para organizações que não possuem meios para desenvolver seus próprios recursos. Antes de abrir a Cyber Defense International, Ross atuou como vice-presidente sênior de operações de cibersegurança no SunTrust Bank. Nessa função, foi encarregado de criar o centro de operações de cibersegurança 24/7/365 da SunTrust. Como tal, Ross construiu equipes especializadas em inteligência cibernética, monitoramento de ciberameaças, resposta a incidentes cibernéticos e crimes cibernéticos. Notavelmente, também fez uma parceria bem-sucedida com parceiros jurídicos, de recursos humanos, segurança corporativa, e ética e riscos empresariais, para estabelecer o primeiro programa de monitoramento de ameaças internas do banco. Ross também facilitou o estabelecimento de várias parcerias de compartilhamento de informações, inclusive com a Força-Tarefa de Crimes Eletrônicos do Serviço Secreto dos Estados Unidos e com o Departamento de Segurança Interna.

Introdução

De volta ao básico

A cibersegurança tem sido um ponto focal proeminente das organizações e de suas funções de auditoria interna, e com a introdução das novas propostas da *Securities and Exchange Commission* (SEC) sobre gerenciamento de riscos de cibersegurança, estratégia, governança e divulgações de incidentes, 2022 não foi exceção. O ímpeto por essas e outras propostas regulatórias está garantido. De acordo com um relatório do *Identity Theft Resource Center*, houve 1.862 violações de dados de alto perfil registradas em 2021, um número que superou o total de 2020 em 68%, bem como o recorde histórico estabelecido em 2017. Nenhum setor foi poupado da tendência.[23]

Nesse ambiente, as organizações desejam - na verdade, exigem - controles e processos de cibersegurança claros e robustos, baseados em fundamentos básicos, incluindo o aprendizado contínuo sobre o risco e seus regulamentos relacionados, bem como comunicação e alinhamento entre o conselho, a gestão e a auditoria interna. A Parte 1 da série de três partes do The IIA, Cibersegurança em 2022, concentra-se nos possíveis impactos regulatórios, enquanto a Parte 2 examina os benefícios de uma relação simbiótica entre os *chief information security officers* (CISOs) e suas contrapartes da auditoria interna. Esta parte final enfatiza o desenvolvimento e a implantação da estratégia de resposta a incidentes cibernéticos de uma organização e, mais especificamente, onde a auditoria interna pode fornecer valor organizacional na avaliação dos controles críticos para a rápida recuperação de uma violação de cibersegurança.

[23] Identify Theft Resource Center, "Identify Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," 24 de janeiro de 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

Principais Controles

Dando à auditoria interna um papel a desempenhar na resposta cibernética

A falácia da resposta a incidentes

Embora os termos "resposta a incidentes cibernéticos" e "resposta e recuperação da cibersegurança" sejam precisos e úteis, também implicam uma visão um tanto incompleta do que esses planos exigem para que sejam eficazes.

A auditoria interna em sua função mais essencial oferece às organizações uma avaliação independente sobre o gerenciamento de riscos. Isso inclui não apenas a avaliação para uma resposta adequada a incidentes cibernéticos, mas também a análise adequada dos controles, para garantir que o risco e seus efeitos sejam mitigados ou, idealmente, evitados. Para atingir um padrão tão elevado sobre qualquer risco, a atenção não deve ser reservada apenas a simplesmente responder a um risco. Em vez disso, é mais eficaz visualizar a resposta a incidentes cibernéticos de uma forma holística e cíclica, que priorize controles preventivos e medidas de resposta ativa.

"O gerenciamento de riscos é como uma roda", disse Brian Tremblay, líder do setor de conformidade da Onapsis, Inc. "No início do giro da roda, temos os controles certos e os processos são o que achamos que deveriam ser. Então, quando algo acontece, a conversa imediatamente se torna: 'os controles funcionaram conforme o esperado e conforme o que pensamos que aconteceria?' A partir daí, aprendemos o que precisa mudar e o ciclo recomeça. Se a única vez que você está respondendo a um evento é após o fato, você provavelmente está sendo ineficiente com seu tempo e recursos. O presente e o futuro devem ter o mesmo peso, porque não estamos apenas construindo o negócio de hoje, estamos construindo o negócio do futuro. Como as organizações, muitas vezes, têm dificuldade com isso, esse é um lugar realmente importante para a auditoria interna se concentrar."

Fundamentos imutáveis

Os riscos raramente se tornam menos complexos e, como a cibersegurança é inerentemente altamente técnica, a curva de aprendizado para entender o risco em si e os sistemas necessários para mitigá-lo só aumentou a cada avanço tecnológico subsequente. No entanto, isso não significa necessariamente que a estrutura fundamental de um plano de resposta a incidentes cibernéticos e os controles dentro dela mudem drasticamente.

Esses controles estão descritos na Orientação Suplementar mais recente do The IIA, *Auditing Cyber Incident Response and Recovery*, e podem ser agrupados em quatro objetivos de negócios de alto nível:

- **Planejamento de Resposta a Incidentes.** Políticas e procedimentos devem ser estabelecidos para orientar a determinação da ocorrência de um incidente e o que fazer a respeito. O planejamento deve envolver os principais stakeholders, definir funções e responsabilidades, e deve ser testado conforme apropriado, para promover a conscientização e a execução.
- **Identificação de Incidentes.** Os processos de análise de dados de controles de detecção levam à determinação da existência de um incidente cibernético, que normalmente é o gatilho para a execução de um ou mais planos de resposta.

- **Comunicações.** Há muitos stakeholders em potencial em incidentes cibernéticos, portanto, cada plano de resposta deve incorporar uma estratégia de comunicação para notificação apropriada e tempestiva sobre impactos e esforços de resolução.
- **Resposta e Recuperação Técnicas.** A natureza do incidente determina, em grande parte, os controles técnicos de remediação e restauração necessários, muitas vezes envolvendo a coordenação de esforços interna e externamente.[24]

Cumprir com esses objetivos de negócios e aderir a um framework de resposta a incidentes cibernéticos estabelecido, como o *Framework for Improving Critical Infrastructure Cybersecurity*, do National Institute of Standards and Technology (NIST), requer conhecimento técnico sobre a implantação, manutenção e melhoria que as equipes de segurança da informação e tecnologia da informação podem fornecer — conhecimento que as equipes de auditoria interna podem ou não possuir. No entanto, também há amplo espaço para outros com disciplinas menos técnicas, mas igualmente valiosas, agregarem valor significativo. A auditoria interna, com seu acesso exclusivo e compreensão das funções organizacionais em todos os departamentos, bem como sua perspectiva independente crítica para prestar avaliação objetiva, é exatamente uma dessas disciplinas.

"Do ponto de vista da auditoria interna, a abordagem da resposta a incidentes cibernéticos não é diferente de qualquer outro risco, pois o foco está no processo em si e no produto desse processo", disse DaMon Ross Sr., fundador da Cyber Defense International, LLC , e ex-vice-presidente sênior, chefe de operações de cibersegurança da SunTrust. "Mesmo com a natureza técnica dos materiais, qualquer auditor interno acostumado a operar em um espaço de processo perceberá rapidamente o que importa."

Esse processo tem mais do que uma semelhança passageira com o que a auditoria interna pode ver nos programas de conformidade da Sarbanes-Oxley (SOX), planos de resposta a crises ou qualquer estratégia de gerenciamento de riscos estabelecida. "Organizações diferentes têm terminologias diferentes, mas um plano de incidente cibernético é, essencialmente, uma política de governança que descreve quando ocorre um incidente cibernético, quais são as funções e responsabilidades de todas as partes aplicáveis e quem precisa estar à mesa para a tomada de decisões", disse Ross.

Tremblay expressou um sentimento semelhante. Os controles relevantes aos riscos cibernéticos também fazem parte dos frameworks usados para gerenciar os riscos de conformidade associados à Sarbanes-Oxley, disse ele.

Por exemplo, um dos primeiros passos dos hackers quando invadem qualquer tecnologia é acessar os direitos e privilégios necessários para atingir seu objetivo. No cenário geral dos riscos, isso cai sob o risco do acesso não autorizado. Não há diferença se isso se aplica à SOX ou a um risco cibernético, disse Tremblay. "Os riscos, quando resumidos em suas formas mais simples, e os controles para mitigar esses riscos, são essencialmente idênticos."

Controles de documentação

Como Tremblay mencionou, os controles contidos em tal política também têm uma sobreposição significativa com o que pode ser visto em outros riscos organizacionais. Um exemplo é ter um processo de documentação eficaz. Ross concorda. As organizações devem entender como são os fluxos de trabalho que documentam adequadamente os incidentes cibernéticos e como todas as peças executadas em paralelo se encaixam, disse ele.

"Isso não vale apenas para grandes incidentes. Toda organização deve ter uma função que lida com isso no dia-a-dia. Digamos que um computador tenha malware nele. São pequenos incidentes como esse que podem se transformar em incidentes maiores e, no caso do pior ocorrer, a documentação adequada ajuda a entender como ele escalou. Essa função é um controle em si."

[24] The IIA, *Auditing Cyber Incident Response and Recovery*, Orientação Suplementar, Guia Prático, https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/2022/gtag_auditing_cyber_incident_response_and_recovery_final.pdf.

Detecção e controles de infraestrutura física

Outro controle crítico, e que se enquadra na rubrica de riscos de acesso não autorizado, é a infraestrutura física. Embora esses controles possam não vir à mente imediatamente ao discutir a cibersegurança, o acesso não autorizado a discos rígidos ou servidores onde informações confidenciais são armazenadas foi responsável por 10% de todas as violações maliciosas em 2020, custando às organizações uma média de US$ 4,36 milhões por violação, de acordo com uma pesquisa do Ponemon Institute publicada pela IBM Security.

Essa infraestrutura pode incluir salas de servidores seguras com acesso restrito, bem como medidas de segurança mais básicas, como portas trancadas em todas as instalações. Embora a segurança da infraestrutura seja importante, ter controles para detectar e documentar atividades potencialmente suspeitas pode ser mais relevante.

“Quando falo de infraestrutura física, não estou falando de portas trancadas, mas de garantir que haja notificação e documentação da ação que cria o risco real. É como o prato principal de uma refeição, em vez de um aperitivo”, disse Tremblay.

Identificar e prestar avaliação para esses sistemas se enquadra perfeitamente nas habilidades estabelecidas da auditoria interna, disse Ross, acrescentando: “a auditoria interna tem a capacidade de identificar sistemas que são de alto risco ou críticos para a subsistência da organização. É provável, de fato, que a auditoria interna já tenha esses sistemas identificados como parte da avaliação de conformidade com leis e regulamentos federais relacionados a outros riscos. Tudo o que é necessário é expandir esse pensamento para incluir novos tipos de provisionamento que possam oferecer acesso elevado.”

Alinhamento das expectativas de recuperação

A documentação eficaz em todas as etapas de um plano de resposta a incidentes cibernéticos é fundamental. Igualmente crítica, no entanto, é a comunicação dos dados que tal documentação fornece e o alinhamento das expectativas organizacionais de detecção e recuperação.

De acordo com Tremblay, essa é uma das maiores lacunas que ele viu nos planos de resposta cibernética das organizações – e onde a auditoria interna pode agregar o maior valor. “O papel da auditoria interna na recuperação de desastres cibernéticos é duplo”, disse ele. “Primeiro, certifique-se de que o incidente existe e você pode provar que existe por meio da documentação ou de qualquer tecnologia ou processo que você use. A segunda coisa, e a coisa que eu não vejo sendo feita suficientemente, é sentar com todos os principais stakeholders para determinar qual será o cronograma realista de recuperação com base no apetite a risco da organização.”

O cronograma, disse Tremblay, será estabelecido pelo "proprietário" do aplicativo em questão na organização, que pode ser o CISO, o chefe da cadeia de suprimentos ou qualquer outro líder, dependendo de onde o incidente ocorrer. A chave para a auditoria interna é funcionar como o elo entre essa parte e todas as outras partes dependentes dessa solicitação para tarefas do dia-a-dia.

“Por exemplo, o CISO pode dizer que um tempo de recuperação de 48 horas é aceitável, mas se você não for ao CFO ou outros líderes ou funções que dependem de que a tecnologia esteja funcionando e recebendo suas contribuições, você está dando abertura para uma possível confusão”, disse Tremblay. “Por exemplo, o CFO pode dizer que o prazo de 48 horas está bom, mas apenas se não estivermos fechando os livros. Mas se estivermos fechando os livros, nenhum tempo de inatividade é aceitável, porque a organização teria que pedir uma extensão de prazo, o que causaria uma impressão péssima nos mercados públicos.”

Essas conversas não exigem necessariamente que uma parte se sobreponha à outra. Em vez disso, por meio dessa comunicação, a auditoria interna pode intermediar o consenso de acordo com o apetite a risco da organização. “Nos casos em que existe discrepância”, disse Tremblay, “o que a auditoria interna pode perguntar é: 'Vale a pena fazer isso acontecer?'

O CEO pode dizer 'Sim, vale, porque vai custar um milhão de dólares para resolver esse problema.' O que estamos realmente fazendo é garantindo que o plano tenha sido realmente desenvolvido em torno dos stakeholders em torno da tecnologia."

Ele continua: "Acho que esta é uma área em que, como profissão, não temos sido especialmente bons. Acho que tentamos riscar as tarefas no checklist de validação de certas coisas, sem realmente dizer: 'Ei, como parte da revisão dos controles sobre a resposta a incidentes, identificamos uma lacuna nos requisitos entre os stakeholders de certas tecnologias.' Isso é muito válido. Isso é identificar um risco de negócios não identificado anteriormente e que é valioso para a organização."

Interfuncionalidade

É um equívoco comum que a propriedade principal da resposta de cibersegurança seja do CISO e da equipe de segurança. Isso é apenas parcialmente verdadeiro. Embora a experiência e o conhecimento necessários para implantar os aspectos mais técnicos de uma estratégia cibernética provavelmente sejam encontrados nesse departamento, é perigoso supor que o departamento terá a largura de banda – ou o desejo – de arcar com o fardo por conta própria.

"A resposta a incidentes cibernéticos é, ou pelo menos deveria ser, um processo interfuncional", disse Ross. "A maior razão para o atraso nos tempos de resposta organizacionais que vejo não é o próprio departamento de segurança da informação em termos de conhecimento, mas sim estabelecer funções e responsabilidades de forma interfuncional, com departamentos cuja principal responsabilidade não seja a segurança. Eles têm outras coisas a fazer."

De acordo com Ross, corrigir esse equívoco e promover a ideia de responsabilidade compartilhada entre todos os stakeholders deve ser uma área principal do foco da auditoria interna. "A ênfase não precisa necessariamente estar na equipe de segurança e no que estão fazendo, mas sim em como seu processo está sendo apoiado por outras entidades em toda a empresa que têm participação nele. A equipe de segurança sabe o que fazer, mas não pode forçar as equipes de TI e os desenvolvedores de back-end a ajudar de formas críticas. Há muita política organizacional envolvida e, quando estava nessa posição, encontrei na auditoria interna uma parceria valiosa. As equipes de segurança não podem encarar essas batalhas sozinhas. Se você conseguir uma parte neutra para ajudar a identificar onde a organização tem falhas no processo, isso ajuda a todos."

Uma estratégia útil para destacar essas lacunas e esclarecer as funções, disse Ross, é a auditoria interna, geralmente em colaboração com um consultor externo, para facilitar simulações. "Depois de ter seu plano de resposta a incidentes cibernéticos em um local que possa ser testado, o simulado de mesa reúne o CIO, o CISO, os líderes de TI, o CEO, a auditoria interna – todos os stakeholders aplicáveis – em uma sala de conferência ou chamada de Zoom, para percorrer um cenário plausível. Mesmo sem conhecimento técnico, a auditoria interna pode facilitar a discussão, perguntando quem faz o quê e avaliando como essas responsabilidades se alinham com a realidade. Ela poderia dizer: 'Neste ponto, sua equipe deve estar executando X e Y de acordo com nosso plano, mas, na realidade, pode ser que você esteja fazendo Z.' É aí que você vai identificar os verdadeiros problemas. A maioria das organizações precisa fazer simulações pelo menos uma vez por ano, mas a auditoria interna deve realmente se encarregar disso."

Conclusão

Evoluindo com o ambiente de risco

A auditoria interna, por seu lugar único na organização, merece um lugar à mesa quando se trata dos planos de resposta a incidentes cibernéticos de uma organização. Mas esse sucesso não isenta a auditoria interna de buscar uma exploração e compreensão mais profundas da cibersegurança. De fato, em um futuro que está dispensando rapidamente a infraestrutura física em favor da tecnologia baseada na nuvem, uma maior especialização da auditoria interna inevitavelmente se tornará necessária e esperada.

"Quando comecei minha carreira em auditoria interna, um dos grandes pontos de venda era que era um papel muito generalista", disse Tremblay. "Você tem que ver e aprender muitas coisas sobre muitas coisas nas quais você não precisa ser um especialista. Mas houve uma mudança tão grande em torno da tecnologia que estou começando a me perguntar se os dias do auditor interno generalista estão contados. Em vez disso, talvez a auditoria interna um dia se torne mais especialista em coisas que são inerentemente críticas para as organizações. Portanto, em vez de ter equipes de auditoria compostas por 8 a 10 auditores operacionais e de conformidade e de demonstrações financeiras, as organizações terão um auditor de cibersegurança, um auditor de ESG, etc."

Ross concorda. "Em um certo ponto, com a tecnologia emergente, como realmente entender as lacunas no processo de resposta em um nível profundo, se você não pode ir tão fundo? Você nunca entenderia, na verdade."

Há muito que pode ser alcançado com o conhecimento e os recursos disponíveis, mas um futuro empolgante e radicalmente novo está chegando. A auditoria interna precisa fazer parte disso.

Edições Anteriores

Para acessar edições anteriores do *Global Perspectives and Insights*, visite www.theiia.org/GPI.

Feedback do Leitor

Envie perguntas ou comentários para globalperspectives@theiia.org.

Sobre o The IIA

The Institute of Internal Auditors (IIA) é uma associação profissional internacional que atende a mais de 215.000 membros globais e concedeu 180.000 certificações *Certified Internal Auditor* (CIA) no mundo todo. Fundado em 1941, o The IIA é reconhecido como líder global da profissão de auditoria interna em normas, certificação, educação, pesquisa e orientação técnica. Para mais informações, visite theiia.org.

Isenção de Responsabilidade

O The IIA publica este documento para fins informativos e educacionais. Este material não tem o objetivo de fornecer respostas definitivas a específicas circunstâncias individuais e, assim, deve ser usado apenas como guia. O The IIA recomenda que você sempre busque conselhos especializados independentes, relacionados diretamente a qualquer situação específica. O The IIA não aceita qualquer responsabilidade pela confiança depositada unicamente neste material.

Copyright

Agosto de 2022

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101