PERSPECTIVAS E PERCEPÇÕES GLOBAIS

Segurança cibernética

PARTE I: Contratação de pessoal e desenvolvimento para a próxima geração
PARTE II: Inteligência artificial - amiga e inimiga da segurança cibernética
PARTE III: Gestão do risco de terceiros em matéria de segurança cibernética

AUDITBOARD

The Institute of Internal Auditors

Conteúdo

PARTE 1

Equipe e Desenvolvimento para a Próxima Geração

SOBRE OS ESPECIALISTAS

ANETA WABERSKA, CISA

Aneta é diretora de produtos de segurança da informação e conformidade da AuditBoard. Ela tem mais de 15 anos de experiência em auditoria de TI e domínios de conformidade e ingressou na AuditBoard para se concentrar nos esforços de desenvolvimento de produtos que atendem aos usuários de risco e conformidade de TI, aproveitando sua experiência no setor. Aneta iniciou sua carreira na KPMG e na PwC, onde ajudou os clientes a implementar e avaliar estruturas como SOC 1 e SOC 2. Ela trabalhou com empresas de diferentes portes para implementar e gerenciar programas de conformidade de complexidade variada, incluindo o gerenciamento de políticas de toda a empresa, programas de gerenciamento de riscos de terceiros, trabalhou em estreita colaboração com a gerência para implementar controles para atender aos requisitos da estrutura de segurança e trabalhou com a gerência executiva para garantir que a conformidade apoie os objetivos estratégicos da empresa.

UDAY GULVADI, CIA, CPA, CAMS, CISA

Uday é diretor administrativo do grupo de disputas, conformidade e investigações da Stout e co-lidera sua prática de conformidade regulatória e crimes financeiros em nível nacional. Uday é líder em práticas de crimes financeiros, auditoria interna, auditoria de sistemas de informação e consultoria de riscos, com mais de 20 anos de experiência. Ele é especialista em orientar conselhos, comitês de auditoria e gerência sênior sobre os mais desafiadores riscos de conformidade com crimes financeiros,TI e cibernéticos, governança e questões de risco e conformidade, incluindo gerenciamento de riscos corporativos, governança de programas de AML e sanções, validações de modelos, auditorias internas baseadas em riscos, tecnologia da informação e auditoria e controles de segurança cibernética. Seus clientes vão desde alguns dos maiores bancos e instituições financeiras do mundo até empresas menores de serviços financeiros.

INTRODUCÃO

A segurança cibernética representa uma ameaça significativa para organizações de qualquer porte. Exemplos recentes refletem a rapidez com que as coisas podem dar errado. Um ataque cibernético interrompeu as remessas da Ace Hardware Corporation para seus revendedores e a forçou a desativar temporariamente os pedidos on-line dos clientes. Um ataque de ransomware em uma grande empresa de telecomunicações chilena interrompeu serviços como data centers, acesso à Internet e voz sobre IP. E, demonstrando que entidades menores também podem ser afetadas, o acesso público on-line a registros de terras e índices de nascimentos, mortes e casamentos foi interrompido por um ataque cibernético no Condado de Cabarrus, Carolina do Norte.

A auditoria interna é adequada para desempenhar um papel fundamental na ajuda ao gerenciamento dos riscos cibernéticos, mas deve ter os recursos necessários para cumpri-lo. Ela deve ter o conhecimento e as habilidades necessárias para identificar e aconselhar sobre as ameaças cibernéticas que a organização enfrenta. De acordo com a Deloitte[1], ao realizar uma avaliação de segurança cibernética, é fundamental envolver profissionais de auditoria com a profundidade adequada de habilidades técnicas e conhecimento do ambiente de risco atual.

Este resumo é o primeiro de uma série de três partes sobre segurança cibernética. Como os líderes de auditoria interna devem entender as ameaças antes de poderem se preparar para enfrentá-las, ele começa examinando os desafios da cibersegurança para os auditores internos e suas organizações. Também aborda as opções e estratégias que os líderes de auditoria interna podem seguir para garantir que tenham o talento necessário para lidar com os riscos cibernéticos contínuos.

[1] "Cybersecurity and the Role of Internal Audit—An Urgent Call to Action," Deloitte Development LLC, 2017.

Uma Ameaça Clara

Segurança cibernética continua sendo um dos principais riscos

Os esforços de segurança cibernética da auditoria interna estão crescendo

"Os auditores internos precisam examinar toda a organização e adotar uma abordagem baseada em riscos", disse Aneta Waberska, CISA, diretora de produtos de segurança da informação e conformidade da AuditBoard. "Os riscos cibernéticos estão no topo da lista para a maioria das organizações."

Os auditores internos parecem estar bem cientes da ameaça que os riscos cibernéticos representam. A segurança cibernética foi identificada como o principal risco para 2024, de acordo com uma pesquisa global de líderes de auditoria interna da The Internal Audit Foundation. A segurança cibernética, juntamente com o Capital Humano e a Continuidade dos Negócios, foram listados como os três principais riscos na pesquisa Risk in Focus 2024[2] de mais de 4.200 executivos-chefes de auditoria (CAEs), com 73% dos entrevistados listando a segurança cibernética como um dos cinco principais riscos.

Na América do Norte, 78% dos líderes de auditoria interna descreveram a segurança cibernética como um risco alto ou muito alto em suas organizações, de acordo com o The Institute of Internal Auditors 2023 North American Pulse of Internal Audit.[3] Os auditores pesquisados estavam dedicando 10% de seus planos de auditoria à segurança cibernética, com preocupações de TI representando outros 9%. Além disso, quase 70% das funções revisaram as áreas de alto risco que incluem segurança cibernética e TI anual ou continuamente, de acordo com os resultados da pesquisa Pulse.

Alguns perigos de segurança cibernética que devem ser lembrados incluem:

- Violações que permitem que criminosos roubem informações críticas ou que exponham dados de clientes ou parceiros de negócios.
- Ataques de ransomware que impossibilitam as organizações de executar funções importantes ou acessar informações necessárias sem antes pagar um resgate aos criminosos cibernéticos.
- Malware que pode causar estragos em um sistema.

Os ataques cibernéticos têm consequências que vão além das mais óbvias, como perdas financeiras quando as funções de negócios são prejudicadas ou se os clientes ou parceiros de negócios perdem a confiança em uma organização e deixam de fazer negócios com ela. Ademais, depois que um incidente cibernético é descoberto, as organizações precisam investir tempo e dinheiro em investigações forenses para entender o que aconteceu e quando realizar a correção para reparar qualquer dano e determinar se as

[2] "Risk in Focus 2024," The Internal Audit Foundation, 2023

[3] "2023 North American Pulse of Internal Audit," The Institute of Internal Auditors, 2023

consequências de tais ataques são relevantes do ponto de vista financeiro e operacional para atender aos requisitos de relatórios regulamentares.

Não é de surpreender, portanto, que os gastos com segurança cibernética estejam se expandindo rapidamente. No início de 2023, a Canalys esperava que os gastos globais com segurança cibernética aumentassem 13,2% durante o ano, com o potencial de atingir US$ 224 bilhões.[4]

"As empresas perceberam que essas ameaças trazem consequências comerciais e financeiras muito reais", disse Uday Gulvadi, CIA, CPA, CAMS, CISA, diretor administrativo do grupo de Disputas, Conformidade e Investigações da Stout. As ameaças certamente são as mais importantes para os comitês de auditoria, disse ele, e "a auditoria interna está sendo solicitada a intensificar e fornecer garantias nessas áreas".

Os Desafios

Abordagem de segurança cibernética, equipe de impacto de maturidade

É fundamental ter uma compreensão clara do ambiente cibernético

Para contratar as pessoas certas para ajudar a auditoria interna a apoiar o gerenciamento do risco cibernético e oferecer a elas as oportunidades de desenvolvimento adequadas, é importante entender completamente as circunstâncias e os riscos exclusivos de segurança cibernética da organização. Vários fatores e desafios devem ser considerados.

UMA MENTALIDADE MANUAL

Muitas equipes de auditoria interna estão tradicionalmente acostumadas a pensar sobre controles internos e vários processos a partir de uma perspectiva manual, disse Waberska. Entretanto, a transformação digital contínua dos negócios exige que as equipes estejam cientes de como as soluções digitais podem aprimorar e melhorar as auditorias internas e outros processos em toda a organização, incluindo a segurança cibernética. Ao mesmo tempo, os auditores internos também devem entender os riscos que a própria transformação digital representa para as organizações, já que criminosos cibernéticos, cada vez mais sofisticados, exploram as vulnerabilidades que os ambientes digitais podem criar.

[4]"Cybersecurity investment to grow by 13% in 2023", Canalys, Jan. 18, 2023, https://www.canalys.com/newsroom/cybersecurity-fore- cast-2023

Se, por exemplo, uma organização opera na nuvem ou usa ou planeja usar qualquer tecnologia avançada ou emergente, ela precisará de pessoas que tenham experiência com essas ferramentas. Não é necessário que os membros da equipe sejam especialistas em tecnologia, afirmou Waberska, mas a exposição ao ambiente de nuvem ou a outras soluções proporcionará maior familiaridade com os riscos relacionados. Além de contratar pessoas com essas habilidades, as equipes de auditoria também devem incluir novas tecnologias em seu treinamento e desenvolvimento do pessoal existente.

CONTROLES INTERNOS

Os auditores internos são treinados para garantir que a organização tenha os controles adequados para se protegercontra os riscos que enfrenta.Em relação aos riscos cibernéticos, os controles internos devem trabalhar para garantir que a tecnologia da informação da organização não seja comprometida e que as funções de negócios possam permanecer operacionais.

Para identificar e aconselhar sobre os riscos de segurança cibernética, as equipes de auditoria interna precisarão estar familiarizadas com os controles de segurança de TI para as tecnologias usadas por sua organização. Ao trabalhar com a nuvem, por exemplo, os controles serão diferentes daqueles usados com data centers internos, apontou Waberska. Elas também precisarão entender quais controles são apropriados, considerando a ameaça que o crime cibernético pode representar para a privacidade e as implicações para os planos de auditoria do programa de privacidade de sua organização.

REGULAMENTOS DE DIVULGAÇÃO E PROTEÇÃO DE DADOS

Agora, as organizações estão sendo solicitadas a serem mais abertas em relação aos relatórios sobre seus esforços de segurança cibernética. Os auditores internos terão de entender quais regras afetam suas empresas e serão capazes de avaliar as necessidades de conformidade. Em um exemplo significativo, em agosto, a U.S. Securities and Exchange Commission emitiu uma regra final sobre Gestão de Risco de Segurança Cibernética, Estratégia, Governança e Divulgação de Incidentes, que exige que as empresas públicas forneçam maior transparência quando sofrerem um ataque cibernético e divulguem informações específicas sobre seus esforços para mitigar os riscos cibernéticos. O IIA fez comentários sobre a regra quando ela estava na fase de proposta. Ele planeja continuar trabalhando com a SEC para desenvolver orientações de implementação, especialmente para determinar a materialidade de um incidente cibernético e definir melhor o termo“segurança cibernética”.

Devido à natureza cada vez mais multinacional dos negócios e ao crescente número de regulamentações de segurança cibernética em todo o mundo, os auditores internos devem se familiarizar com todas as leis de segurança e privacidade de dados que possam afetar suas organizações, como a Regulamentação Geral de Proteção de Dados da União Europeia. De fato, de acordo com a Conferência das Nações Unidas sobre Comércio e Desenvolvimento, 137 dos 194 países haviam implementado uma legislação para garantir a proteção dos dados e da privacidade.

SISTEMAS DE TI

Qualquer organização, mesmo com tecnologia básica, está envolvida em algum tipo de sistema de TI, e todos eles são vulneráveis ao risco cibernético. Dado o volume de sistemas e as possíveis fraquezas e ameaças envolvidas, é importante que as empresas e a auditoria interna entendam quais sistemas são mais importantes. "Nunca conseguiremos colocar o mesmo nível de controles em todos os sistemas", observou Waberska. Definir prioridades envolverá fazer perguntas como:

- Quais sistemas são essenciais para o funcionamento da organização? É possível responder a essa pergunta considerando se - e por quanto tempo - a organização seria capaz de continuar a conduzir os negócios ou atingir as principais metas sem eles.
- Quais deles processam os dados mais confidenciais? Isso pode incluir informações corporativas confidenciais ou informações de identificação pessoal (PII).
- Quais deles contêm dados exclusivos ou difíceis de substituir?[5]

TERCEIROS

Mesmo as organizações de pequeno e médio porte estão envolvidas com terceiros que lidam com seus dados. Isso pode ocorrer por meio de um aplicativo em nuvem ou, no caso de organizações maiores, talvez em um centro de processamento no exterior. Esses fornecedores podem lidar com dados organizacionais importantes e com as PII dos clientes, e os dados podem estar armazenados em qualquer lugar do mundo, observou Gulvadi. Por esse motivo, "é extremamente importante entender todo o cenário dos ativos de TI", inclusive onde eles estão e se os controles adequados estão em vigor em torno desses ativos, disse ele.

[5]"CISA Insights – Cyber, Secure High Value Assets (HVAs)," U.S. Department of Homeland Security, https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf

As organizações devem avaliar os processos de segurança cibernética de terceiros antes de compartilhar dados com eles e monitorar esses processos quando os terceiros começarem a usar os dados, em alguns casos mantendo o direito de auditar os terceiros. “Se você compartilha dados de clientes com terceiros, precisa garantir que eles os protegerão da mesma forma que sua empresa faria”, disse Waberska. As empresas devem analisar os relatórios de atestados de terceiros, como o SOC 2, que avalia seus controles internos para verificar se eles lidam bem com os riscos, ou outros tipos de atestados ou certificações relacionados à proteção de categorias relevantes de dados.

GARANTIA DE ACESSO SEGURO E DISPONIBILIDADE

Há um equilíbrio entre garantir que a organização possa proteger os dados e os sistemas e, ao mesmo tempo, garantir que as informações e os sistemas estejam disponíveis para uso conforme necessário para atingir os objetivos comerciais, observou Gulvadi. Para manter o equilíbrio, as organizações terão de escolher controles que protejam os dados sem dificultar o acesso às informações necessárias para o atendimento ao cliente ou outras funções comerciais importantes. Essa determinação deve ser mais fácil de ser feita depois que a organização tiver considerado quais sistemas exigem o mais alto nível de segurança. Alguns talvez precisem ser protegidos com autenticação multifatorial, protocolos de criptografia e software de prevenção de perda de dados, enquanto outros não exigirão esse nível de granularidade.

Fortalecimentos dos recursos de auditoria interna

A equipe de segurança cibernética continua sendo uma das principais prioridades

Contratação e desenvolvimento do talento cibernético da auditoria interna

Considerando esses riscos, como a auditoria interna pode criar e manter uma equipe que possa lidar com eles? As especificidades da resposta variarão de acordo com a organização, mas há algumas recomendações que se aplicam a todas.

BUSQUE UMA COMBINAÇÃO DE HABILIDADES

Para abordar o risco cibernético, as equipes de auditoria interna precisam de um profundo entendimento do lado técnico da segurança cibernética, bem como da capacidade de compreender as consequências que os problemas de segurança podem ter para os negócios, disse Gulvadi. No passado, os auditores de TI tendiam a ser fortes nos aspectos técnicos da segurança da informação, mas geralmente não se concentravam em como os riscos relacionados afetavam a capacidade da organização de cumprir seus objetivos comerciais. A capacidade de articular o impacto nos negócios pode ser particularmente valiosa se a auditoria interna precisar obter a adesão da gerência para os investimentos necessários em tecnologia ou controles aprimorados ou em pessoal adicional.

Gulvadi está vendo mais esforços para criar equipes que combinem conhecimento técnico com um entendimento dos objetivos, processos e cadeias de valor do negócio. Em alguns casos, as equipes de auditoria interna estão encontrando profissionais que têm ambas as habilidades, mas em outros, as equipes incluem profissionais cujas habilidades se complementam. A organização pode considerar oferecer treinamento para dar a cada tipo de profissional um conhecimento básico de trabalho da outra disciplina.

INTEGRAR HABILIDADES EM TECNOLOGIAS EMERGENTES

Muitas equipes de auditoria interna estão adicionando profissionais com experiência em análise de dados, inteligência artificial e aprendizado de máquina, à medida que se afastam dos testes baseados em amostras. “Você pode usar a inteligência artificial para testar toda a população e melhorar a detecção de anomalias”, declarou Gulvadi. Isso não apenas aumenta a eficiência e a confiabilidade, mas também ajuda os auditores internos a acompanhar o ritmo dos criminosos cibernéticos, que estão se tornando cada vez mais sofisticados no uso de novas tecnologias.

INVESTIGAR A TERCEIRIZAÇÃO

Algumas equipes de auditoria interna trazem uma equipe terceirizada para aprimorar as habilidades técnicas ou comerciais. Profissionais com conhecimento especializado em segurança cibernética ou de TI podem ser incorporados à equipe de auditoria interna em um projeto ou a longo prazo, conforme necessário. Quando os membros da equipe de auditoria interna trabalham ao lado desses especialistas, eles podem ajudar os contratados a aprimorar seus conhecimentos e a navegar melhor pelos processos e procedimentos da empresa. Ao mesmo tempo, a exposição a especialistas externos pode ajudar a expandir a base de conhecimento dos membros da equipe. Ao avaliar uma opção de terceirização, Gulvadi recomenda examinar as certificações e a experiência anterior dos membros da equipe para garantir que elas correspondam ou aprimorem as habilidades atuais da equipe.

CONSIDERAR A COLABORAÇÃO

Às vezes, a experiência de que a equipe de auditoria interna precisa pode estar disponível internamente em áreas como TI, segurança ou conformidade. Uma boa parceria, ao mesmo tempo em que mantém a independência do auditor, apresenta aos membros da equipe de auditoria interna uma série de novos insights e conhecimentos sobre o ecossistema tecnológico e os riscos da organização. Ela também prepara o terreno para auditorias frutíferas no futuro, porque outras equipes saberão que a auditoria interna compartilha sua meta de proteger a organização de riscos desnecessários e garantir que ela possa atingir seus objetivos. A comunicação aberta também pode ajudar outras equipes a superar qualquer ansiedade sobre os objetivos da auditoria interna. “As equipes de TI e segurança estão focadas em resolver problemas importantes e encontrar soluções», disse Waberska. «Elas entendem os riscos e a necessidade de mitigá-los. A capacidade da auditoria interna de ter uma conversa muito focada em riscos com elas explica por que certos controles são necessários para tornar a auditoria interna muito mais eficaz.”

CRIAR RELACIONAMENTOS INTERNOS

Todos os membros de uma equipe de auditoria interna podem se beneficiar da criação e manutenção de relacionamentos com outros profissionais das equipes de segurança, conformidade e TI de sua organização para aprender sobre seu trabalho atual, mesmo que não estejam colaborando em um projeto específico. “Entender o que está acontecendo no ambiente da empresa é muito importante”, afirmou Waberska, e esses relacionamentos podem garantir que a equipe receba atualizações em tempo hábil. Auditorias específicas revelarão tendências e ameaças, “mas é melhor saber o que está mudando o mais rápido possível”, disse ela.

FAÇA USO DOS RECURSOS DISPONÍVEIS

"Se as equipes de auditoria interna reservarem um tempo para aprender as tecnologias modernas, pelo menos em um nível elevado, e os riscos que as acompanham, elas se manterão atualizadas sobre os riscos atuais e emergentes", apontou Waberska. As opções incluem o Centro de Recursos de Segurança Cibernética do The IIA, que inclui uma variedade de orientações de segurança cibernética, pesquisas, programas de certificação e informações sobre conferências relacionadas, como a Conferência Virtual de Segurança Cibernética anual do The IIA. O AuditBoard também oferece uma ampla variedade de recursos de segurança cibernética, que podem ser acessados em sua página de recursos.

O Risk in Focus 2024, da The Internal Audit Foundation, explora o risco de segurança cibernética globalmente e oferece perspectivas regionais exclusivas sobre como a segurança cibernética e outros riscos importantes são vistos e gerenciados em todo o mundo.

Conclusão

A pesquisa 2023 IIA Pulse constatou que o crescimento da equipe de auditoria interna está aumentando, mas ainda não retornou aos níveis pré-COVID. Os líderes de auditoria interna devem se lembrar de que as gerações que estão entrando na força de trabalho são digitalmente experientes. É inteligente considerar as melhores maneiras de usar o conhecimento que elas trazem, observou Gulvadi. As lojas de auditoria interna também se diferenciarão em um ambiente de pessoal competitivo, oferecendo à nova geração a chance de usar tecnologias emergentes, como IA/ML, para oferecer insights que ajudarão a resolver problemas críticos de negócios. Conforme a auditoria interna continua a reconstruir equipes ou a expandir sua expertise para assumir novos desafios, ela deve usar os conselhos e insights deste resumo em seu planejamento.

Parte 2: Inteligência artificial - amiga e inimiga da segurança cibernética

SOBRE OS ESPECIALISTAS

ANETA WABERSKA, CISA

Aneta é diretora de produtos de segurança da informação e conformidade da AuditBoard. Ela tem mais de 15 anos de experiência em auditoria de TI e domínios de conformidade e ingressou na AuditBoard para se concentrar nos esforços de desenvolvimento de produtos que atendem aos usuários de risco e conformidade de TI, aproveitando sua experiência no setor. Aneta iniciou sua carreira na KPMG e na PwC, onde ajudou os clientes a implementar e avaliar estruturas como SOC 1 e SOC 2. Ela trabalhou com empresas de diferentes portes para implementar e gerenciar programas de conformidade de complexidade variada, incluindo o gerenciamento de políticas de toda a empresa, programas de gerenciamento de riscos de terceiros, trabalhou em estreita colaboração com a gerência para implementar controles para atender aos requisitos da estrutura de segurança e trabalhou com a gerência executiva para garantir que a conformidade apoie os objetivos estratégicos da empresa.

TERRY GRAFENSTINE, CIA, CPA, CISSP, CISA, CRISC, CGAP, CGEIT

Terry é vice-presidente sênior do Conselho de Administração Global do Instituto de Auditores Internos (IIA) para 2023-24 e executiva-chefe de auditoria da Pentagon Federal Credit Union (PenFed). Ela foi reconhecida pelo The IIA como uma das "Top Ten Audit Thought Leaders of the Decade" por suas contribuições à profissão relacionadas a cibernética e tecnologia e também foi introduzida no Hall of Distinguished Audit Practitioners do The IIA. Ela ocupou cargos de liderança no Citi e na Deloitte e atuou como Inspetora Geral da Câmara dos Deputados dos EUA.

INTRODUÇÃO

A segurança cibernética é a principal consideração de risco para os auditores internos, e esse continuará sendo o caso em um futuro próximo. De fato, é o único risco que consome seu maior tempo e esforço, de acordo com o Risk In Focus 2024. A série de relatórios, da Fundação de Auditoria Interna do The Institute of Internal Auditor (IIA), perguntou aos executivos-chefes de auditoria e diretores de todo o mundo sobre os principais riscos que suas organizações estão enfrentando e como eles esperam que o quadro de ameaças mude nos próximos três anos.

As descobertas do Risk in Focus 2024 demonstram a complexidade da segurança cibernética como um risco e os desafios adicionais decorrentes das mudanças quase constantes na tecnologia e de como ela pode ser usada. Isso também se refletiu nas conclusões do relatório. Os líderes de auditoria interna esperavam ver a ameaça da ruptura digital saltar do quinto lugar na lista de ameaças hoje para o segundo lugar em três anos.

Este resumo, o segundo de uma série de três partes sobre segurança cibernética,examina como a inteligência artificial (IA) contribui para os desafios e oportunidades da segurança cibernética e o que os auditores internos precisam saber sobre essa área de risco emergente e em evolução como uma consideração de segurança cibernética. A IA é uma grande promessa como uma ferramenta sofisticada para melhorar a eficiência, a produtividade e o gerenciamento de riscos em praticamente qualquer organização. No entanto, ela também apresenta novos desafios de gerenciamento de riscos, incluindo considerações éticas, os perigos do viés algorítmico e a confiança excessiva ou cega no uso da IA. Embora possa ser uma ferramenta valiosa na batalha contra os ataques cibernéticos, os malfeitores também a estão usando para cometer seus crimes.

IA no trabalho

Uma espada cibernética de dois gumes

A auditoria interna deve explorar os usos e as ameaças da IA

O termo inteligência artificial refere-se à tecnologia que pode imitar a inteligência humana, como aprendizado, raciocínio e trabalho para resolver um problema difícil. Ele abrange vários tipos de tecnologias, inclusive o aprendizado de máquina, ou a capacidade de um sistema de aprender com os dados e aplicar esse aprendizado.

Uma maneira pela qual a IA e o aprendizado de máquina podem aprimorar significativamente os esforços de segurança cibernética é na detecção de ameaças e na análise de dados, disse Aneta Waberska, diretora de produtos de segurança da informação e conformidade da AuditBoard. Os criminosos cibernéticos tentam se infiltrar na rede de uma organização procurando pontos fracos e quebrando as defesas da rede. No passado, as organizações confiavam nos administradores de sistemas para bloquear essas ameaças externas. No entanto, devido ao avanço da automação e de outras tecnologias, o volume crescente de entradas de agentes mal-intencionados sobrecarregou a capacidade de análise humana eficaz, declarou ela. A IA pode resolver esse problema. Ela pode analisar grandes volumes de entradas de rede, reconhecer padrões e aprender com eles ao longo do tempo, compreendendo se um determinado evento ou grupo de eventos pode representar uma ameaça para uma organização. "Esse é um dos usos mais impactantes da IA nesse ambiente", segundo ela.[6]

Usando a IA como uma ferramenta de segurança cibernética

De acordo De acordo com a IEEE Computer Society, algumas das maneiras pelas quais a IA pode aprimorar as defesas de segurança cibernética de uma organização incluem:

- Detecção de atividades mal-intencionadas, comparando atividades aceitáveis e identificando anomalias continuamente e em tempo real.
- Apoiaraidentificaçãodeameaçasdemalwareexaminandoascaracterísticas dos arquivos ou padrões de código para identificar aqueles que não são seguros.
- Melhorar a capacidade da empresa de lidar com ataques de dia zero ou outras ameaças desconhecidas.
- Aprimorar a inteligência contra ameaças, reunindo informações de segurança de diversas fontes, procurando ameaças de forma proativa e auxiliando no gerenciamento de ameaças, facilitando a carga de trabalho dos analistas de segurança da empresa.

[6]"AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself," Gaurav Be- lani, IEEE Computer Society, September 6, 2023.

Além disso, as ferramentas de detecção de malware mais sofisticadas têm recursos melhores, incluindo a capacidade de bloquear uma das principais causas de violações e incidentes de segurança - o phising. Isso pode reduzir ou eliminar o potencial de erros humanos - como abrir um link em um e-mail de phishing e expor as redes da empresa a malware - porque as ferramentas os filtram antes que cheguem à caixa de entrada de alguém, afirmou Waberska. (Consulte a barra lateral para obter mais informações sobre algumas das maneiras pelas quais a IA pode melhorar as defesas de segurança cibernética).

A IA também pode pesquisar rapidamente anomalias e identificar problemas que já estão ocorrendo na rede da organização, algo que os humanos não conseguem fazer em dados de grande escala. O acesso não autorizado aos sistemas da empresa é um exemplo.Um ex-funcionário pode inadvertidamente disponibilizar o acesso a um criminoso cibernético compartilhando ou anotando uma senha ou pode entrar novamente no sistema com intenção maliciosa. No passado, um auditor interno que verificasse a existência de acessonãoautorizadoentreex-empregadosteriaquerealizarumacomparação manual entre as pessoas com acesso e aquelas que não deveriam mais tê-lo e, em seguida, escrever um e-mail para a equipe de TI detalhando quaisquer problemas, observou Terry Grafenstine, executiva-chefe de auditoria da Pentagon Federal Credit Union. A IA, por outro lado, pode pesquisar em várias plataformas, comparar dados no sistema de folha de pagamento e no sistema de acesso e gerar um e-mail para as equipes apropriadas sobre quaisquer anomalias.

Os auditores internos devem estar cientes de que os objetivos dos criminosos cibernéticos geralmente não são apenas roubar dados, mas se infiltrar e interromper sistemas alterando dados, apontou Grafenstine. No nível mais amplo, os agentes mal-intencionados do estado-nação podem manipular a infraestrutura crítica, como transporte, energia nuclear, bancos e muitos outros, mas as consequências também podem ser significativas para organizações de qualquer tamanho.

Considerações sobre o gerenciamento de riscos

Ética, preconceito e excesso de confiança

A AUDITORIA INTERNA PODE AJUDAR AS ORGANIZAÇÕES A EVITAR AS ARMADILHAS DA IA

Juntamente com seus muitos benefícios, a IA vem com sua própria lista de considerações de risco. Algumas das ameaças são internas, mas podem ser tão prejudiciais quanto os ataques cibernéticos.

ÉTICA

Muitas das preocupações nessa área estão relacionadas à IA generativa e aos grandes modelos de linguagem que podem ser usados pelos auditores internos para criar relatórios, escrever códigos e esboçar recomendações e análises, entre outras possibilidades. No entanto, essas ferramentas também levantam questões éticas e de segurança para as organizações. “Há o risco de que os funcionários vejam essas ferramentas como um jogo de salão ou um brinquedo”, declarou Grafenstine.

Os controles cibernéticos tradicionais usados em tecnologias anteriores também se aplicam a esses sistemas, mas “as repercussões de não fazer isso bem feito são ampliadas”, disse ela. Entre outras coisas, como será discutido em mais detalhes, os sistemas podem fornecer informações tendenciosas, imprecisas ou completamente fabricadas,dependendo de como sãotreinados. Ela também aponta as consequências dispendiosas e potencialmente embaraçosas para os negócios e a reputação de uma empresa se ela usar um chatbot voltado para o cliente que tenha sido treinado com base em dados da Internet de origem ruim e as respostas incorretas desse software tiverem um impacto negativo significativo sobre os clientes. Por esses motivos, deve haver uma revisão humana de tudo o que for produzido por um sistema de IA generativo quando a organização não estiver completamente ciente dos dados com os quais ele foi treinado. “A empresa precisa ser a dona das respostas”, completou ela.

Embora o uso de programas de IA generativa, como o ChatGPT, tenha explodido desde que foram lançados no final de 2022, a publicação de informações em IA generativa disponível publicamente pode expor dados da empresa ou do cliente e informações pessoais identificáveis, da mesma forma que um incidente de hacking pode fazer, e é uma consideração de risco significativa. Quando os funcionários publicam consultas que incluem informações da empresa em programas públicos de IA generativa, o programa retém essas informações e pode usá-las para responder a outras consultas fora da organização, expondo-as ao público. Isso não apenas pode divulgar informações confidenciais, mas os malfeitores também podem usar

os detalhes que descobrem na IA generativa disponível publicamente para criar seu caminho para os sistemas da empresa, com phishing ou outras ferramentas, alertou Grafenstine.

EXCESSO DE CONFIANÇA CEGA NA PRODUÇÃO DE IA

Qualquer profissional é, em última instância, responsável pelas ferramentas que utiliza e pelas informações que gera. Isso é particularmente verdadeiro para os auditores internos, que podem violar seus próprios padrões se confiarem demais em dados ou conteúdo não validados. "Ser confiável é o que fazemos para viver", apontou Grafenstine.

VIÉS ALGORÍTMICO

As máquinas são treinadas para aprender com base em algoritmos específicos e as informações que produzem podem ser influenciadas, intencionalmente ou não, com base nesses algoritmos. Por exemplo, os algoritmos podem filtrar currículos de mulheres para serem usados em uma decisão de contratação se os funcionários existentes em uma determinada função forem predominantemente do sexo masculino ou podem favorecer solicitações de hipotecas de compradores brancos se a maioria dos atuais detentores de hipotecas for branca.[7] "Eles não estão intencionalmente tentando ser maliciosos, mas os preconceitos estão embutidos", afirmou Grafenstine.

[7] "For minorities, biased AI algorithms can damage almost every part of life" (Para minorias, algoritmos de IA tendenciosos podem prejudicar quase todas as partes da vida), The Conversation, www.theconversation.com, 24 de agosto de 2023.

Protegendo a IA - e protegendo-se contra ela

Os controles internos são essenciais

Proteção da integridade do acesso aos sistemas de IA

A segurança da própria IA e a capacidade de usá-la são outras considerações sérias para as organizações e os auditores internos. Deve haver controles sobre quem pode acessar os recursos de IA, como a autoridade para alterar o código é protegida e quem tem permissão para levar informações de uma área de teste para a produção. Como auditora interna,"quero ter certeza de que posso saber se um algoritmo de IA foi alterado ou se alguém pode interrompê-lo no meio de um processo e alterá-lo", declara Grafenstine. Os auditores internos também precisam estar cientes do possível escopo da interferência. "Se eu puder acessar a IA da sua empresa, não é apenas uma transação que posso alterar", apontou ela. Em vez disso, o malfeitor pode acessar todo o data lake ou data warehouse de uma organização, ou qualquer outra coisa a que a IA tenha acesso.

Ao mesmo tempo, é importante estar ciente de que a IA está tornando mais fácil para os criminosos cibernéticos criarem malware rapidamente, automatizarem ataques e aumentarem a eficácia de seus golpes ou ataques de engenharia social usando ferramentas como deepfakes, que alteram digitalmente vídeos ou fotos, e geradores de voz de IA para criar imagens ou mensagens falsas. "O cenário de ameaças cibernéticas está se tornando mais perigoso, e a IA desempenha um papel importante nisso", de acordo com um artigo da IEEE Computer Society.[8]

> "O fato de você ter implementado uma solução que aproveita a IA não significa que agora você está à prova de balas"
>
> ***Aneta Waberska***
> ***AuditBoard***

Osauditoresinternosdevemvera IAcomoumaferramentaofensivaedefensiva, disse Waberska. "Só porque você implementou uma solução que aproveita a IA, não significa que agora você está à prova de balas", afirmou ela. Enquanto os ataques anteriores eram frequentemente lançados por um hacker em uma única organização, a IA pode realizar ataques em uma escala muito maior, atingindo várias organizações. A IA pode aprimorar o malware aprendendo com programas anteriores e usar esse conhecimento para gerar malware mais forte e melhor, fazendo isso por conta própria, sem a necessidade de um desenvolvedor. "Se a IA estiver tentando invadir sua organização, ela pode ser muito mais poderosa do que sua solução existente", apontou Waberska. Os auditores internos podem garantir que suas organizações entendam e estejam preparadas para lidar com esses riscos. A equipe de auditoria interna

[8] "AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself", Gaurav Belani, IEEE Computer Society Tech Trends, 6 de setembro de 2023.

não pode implementar soluções, mas pode ter uma conversa informada com a equipe de segurança para ver se ela está considerando essas ameaças e implementando soluções. “Levará algum tempo para que as organizações adotem novas soluções, mas é importante estar ciente das ameaças e ter um plano para se defender”, alertou Waberska.

NÃO SE ESQUECE DO ELEMENTO HUMANO

Enquanto as organizações se preparam para afastar as ameaças cibernéticas externas, os auditores internos devem ter em mente o perigo representado pelas ameaças inadvertidas representadas por seu próprio pessoal. As tentativas de phishing, por exemplo, são bem-sucedidas devido ao erro humano de não reconhecer que um criminoso cibernético está tentando obter acesso ao sistema, a uma senha importante ou a outros dados confidenciais. “Os auditores internos devem observar como a organização está educando os usuários sobre essas ameaças”, enfatizou Waberska. Em particular, os funcionários podem não entender que os e-mails de phishing evoluíram. Embora antes fosse fácil identificar sinais de alerta, como erros de ortografia ou fontes estranhas, a IA está sendo usada para escrever e-mails de phishing que são muito mais sofisticados e realistas. “Eles parecem muito reais, e é muito mais fácil para os malfeitores gerá-los”, afirmou ela.

Conclusão

A ameaça de ataques cibernéticos é uma característica permanente dos negócios no mundo digital, e a IA e seu uso em evolução apresentam uma reviravolta nova e provocativa na batalha do gerenciamento de riscos contra essa ameaça. Os auditores internos têm um papel importante a desempenhar:

- Garantir que a liderança e as principais equipes estejam cientes dos benefícios e perigos relacionados à IA.
- Determinar e fornecer recomendações sobre como a IA pode aprimorar vários esforços de segurança cibernética dentro da organização.
- Promover a conscientização sobre a necessidade de considerar defesas atualizadas contra ferramentas de ataque cibernético com tecnologia de IA.
- Fornecer garantia sobre a compreensão e o uso de tecnologias de IA pela empresa.

A IA e as tecnologias relacionadas podem servir como recursos valiosos, mas não são uma resposta definitiva.“Os avanços tecnológicos podem ser ótimos, desde que você saiba como usá-los de forma inteligente e segura”, declarou Waberska. “Você deve sempre usar o julgamento profissional ao considerar o que você recebe.”

Lembre-se também de que, embora ser conservador seja um ativo para os auditores internos, eles não devem ser “o escritório do não”, apontou Grafenstine. Os auditores internos devem oferecer boas recomendações de controle e risco, incluindo insights sobre o risco de não acompanhar a tecnologia.“É um risco enorme não adotar a tecnologia, mas precisamos fazer isso de forma ponderada”, disse ela.

Parte 3: Gerenciamento de riscos de segurança cibernética de terceiros

SOBRE OS ESPECIALISTAS

RICHARD MARCUS, CISA, CRISC, CISM, TPECS

Richard Marcus é vice-presidente de segurança da informação da AuditBoard, onde se concentra em produtos, infraestrutura e segurança de TI corporativa, além de liderar as iniciativas de conformidade interna da AuditBoard. Nessa função, ele se tornou um usuário avançado do produto AuditBoard, aproveitando o conjunto robusto de recursos da plataforma para atender aos casos de uso de conformidade, avaliação de riscos e auditoria.

JOHN A. WHEELER

John A. Wheeler é o fundador e CEO da Wheelhouse Advisors, uma empresa de consultoria executiva sênior que ajuda empresas globais a obter maior visibilidade e compreensão dos riscos. Ele aproveita sua experiência em gerenciamento de riscos, segurança cibernética, negócios digitais, riscos operacionais e gerenciamento integrado de riscos para fornecer orientação estratégica e soluções tecnológicas aos seus clientes.

INTRODUCÃO

O mundo está se tornando cada vez mais interconectado, e o setor não é exceção. Atualmente, quase todos os principais setores de negócios dependem de terceiros em alguma medida. Nas gerações anteriores, isso poderia ter sido feito principalmente a partir de uma perspectiva física, com uma parte dependendo de outra para obter bens ou serviços. Embora isso ainda seja verdade, agora a conexão entre as partes se entrelaçou com o domínio digital.

Naturalmente, embora essa tendência traga muitos benefícios, principalmente em relação à eficiência, produtividade e melhor cumprimento dos compromissos de sustentabilidade, também há riscos que devem ser considerados. De acordo com a Pesquisa Global de Gerenciamento de Riscos de Terceiros de 2022 da Deloitte, 73% dos entrevistados agora têm uma dependência de nível moderado a alto de provedores de serviços de nuvem terceirizados, e espera-se que esse número aumente para 88% nos próximos anos. No entanto, para que esses relacionamentos sejam bem-sucedidos, deve haver uma confiança implícita entre as organizações de que os dados transferidos estarão tão seguros quanto possível contra ataques cibernéticos, violações de dados ou outros incidentes cibernéticos relacionados. Para obter essa confiança, as organizações devem ter um programa dedicado e abrangente de gerenciamento de riscos de terceiros (TPRM) que exerça a devida diligência ao integrar fornecedores terceirizados e monitorá-los continuamente durante o ciclo de vida do relacionamento.

A verdade, no entanto, é que muitas vezes as empresas assumem a confiança sem antes fazer a devida diligência. “Qualquer terceiro - fornecedor, provedor de componentes de produtos, parceiro ou cliente - pode apresentar novos riscos cibernéticos para sua organização”, disse Richard Marcus, vice- presidente de segurança da informação da AuditBoard. “A necessidade de um gerenciamento robusto de riscos de terceiros vem crescendo ao longo do tempo, e muitas organizações não estão acompanhando esse crescimento.”[9]

Como parte final desta série de três partes sobre segurança cibernética, este Global Knowledge Brief destacará o quão significativos se tornaram os riscos cibernéticos associados a terceiros e abordará onde os auditores internos podem se encaixar no gerenciamento de riscos cibernéticos de terceiros.

[9]Global Third-Party Risk Management Survey, Deloitte, 2022, https://www.deloitte.com\content\dam\Deloitte\us\Documents\TPRM_Survey_Report_Interactive.pdf.

Um grande desafio

Os riscos cibernéticos dominam a discussão sobre o gerenciamento de riscos de terceiros

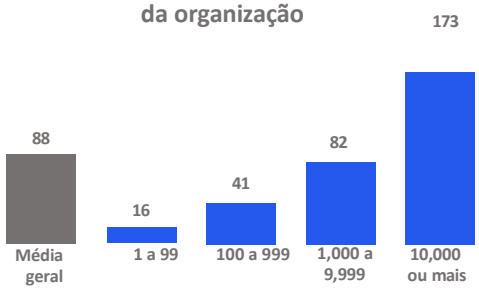
Um risco em ascensão

Um relatório recente da CyberRisk Alliance, patrocinado pela AuditBoard, fez uma pesquisa com 209 líderes e executivos de segurança e TI, administradores de segurança e profissionais de conformidade sediados nos EUA. Ele revelou o quão vasto se tornou o risco cibernético de terceiros. Os insights da pesquisa incluem:

- Em média, as empresas usam 88 parceiros terceirizados (incluindo fornecedores de software, fornecedores de serviços de TI, parceiros de serviçosdeTI, parceirosdenegócios, corretores, subcontratados, fabricantes contratados, distribuidores, agentes e revendedores). Os números variam significativamente de acordo com o tamanho da organização, sendo que as empresas com 1 a 99 funcionários usam 16 parceiros em média, enquanto as empresas com 10.000 ou mais funcionários usam 173 em média (consulte a Figura 1).
- 57% dos entrevistados informaram que foram vítimas de um incidente de segurança de TI (ataque ou violação) nos últimos 24 meses. Ademais, as organizações sofreram, em média, dois incidentes de segurança relacionados a terceiros nos últimos dois anos.
- Entre os afetados, 52% disseram que a origem do ataque foi um fornecedor de software, enquanto 39% disseram que um parceiro de negócios, subcontratado ou provedor de serviços de TI foi responsável pelo incidente (veja a Figura 2).[10]

Figura 1

Número médio de terceiros por tamanho da organização

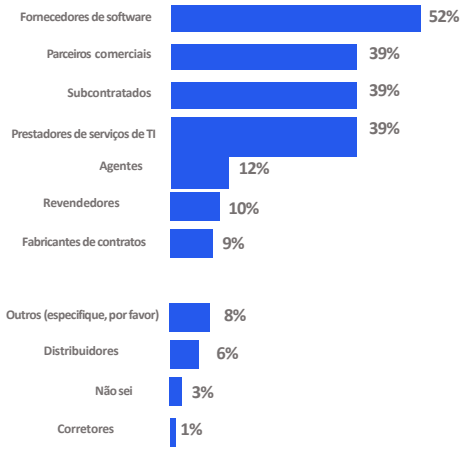


Com quantos terceiros, aproximadamente, sua organização está contratada atualmente? Inclua todos os fornecedores (inclusive fornecedores de software e prestadores de serviços de TI), parceiros comerciais, corretores, subcontratados, fabricantes contratados, distribuidores, agentes e revendedores.

Observação: os gráficos e dados da Figura 1 e da Figura 2 foram extraídos de "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations", da CyberRisk Alliance e Auditboard. p. 9 e p. 18, janeiro de 2023.

Figura 2

Quais das seguintes opções foram a(s) fonte(s) desses ataques ou violações?
Selecione todas as opções aplicáveis:



[10]"Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations", CyberRisk Allian- ce e AuditBoard, janeiro de 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limite- d-supply-chain-visibility-big-risks-for-organizations/.

ACOMPANHANDO AS MUDANÇAS

Os principais motivos para esses problemas são variados, mas decorrem de uma combinação de modelos de negócios que mudam rapidamente e da incapacidade de atualizar os processos de gerenciamento de riscos de terceiros para acompanhar a mudança, de acordo com John Wheeler, fundador e CEO da Wheelhouse Advisors. "Em minha experiência", disse Wheeler, "os maiores e mais relevantes riscos são gerados por grandes mudanças. O desafio do crescimento está impulsionando grandes mudanças, estimulando as empresas a criar novos produtos e serviços digitais."

44%

A PORCENTAGEM DE ORGANIZAÇÕES QUE DEPENDEM DE TECNOLOGIAS MANUAIS PARA GERENCIAR RISCOS CIBERNÉTICOS DE TERCEIROS

Relatório de risco digital do AuditBoard 2023 Risco generalizado, fragmentação persistente e aceleração do investimento em tecnologia

Sobre esse ponto, Wheeler é o autor do Relatório de Risco Digital 2023 da AuditBoard: *Pervasive Risk, Persistent Fragmentation, and Accelerating Technology Investment.* Em uma pesquisa com mais de 130 líderes de risco dos EUA, 21% informaram que não realizam avaliação de risco qualitativa ou quantitativa ao gerenciar e monitorar o risco digital de terceiros, e 56% dependem apenas de abordagens de avaliação qualitativa, o que é limitado em comparação com as avaliações quantitativas.[11]

Igualmente preocupante, disse Wheeler, foi o fato de que, entre as empresas que gerenciam riscos digitais, como riscos cibernéticos de terceiros, surpreendentes 44% ainda dependem de tecnologias manuais (planilhas, e-mail, unidades compartilhadas e Sharepoint) para fazer isso. "É uma abordagem que consome muito tempo", afirmou ele. "A realidade é que o software legado de governança, GRC [governança, risco e conformidade] fragmentado, inflexível e orientado para a conformidade simplesmente não pode fornecer os recursos de risco conectados necessários para acompanhar o ritmo do risco digital - e, como resultado, a maioria das organizações ainda depende de processos manuais fragmentados."

Isso é particularmente preocupante em relação à mudança nos padrões de ataque dos malfeitores, que se tornam mais sofisticados a cada dia. "Se você observar as causas básicas de como as violações ocorreram nas últimas décadas, a maioria ocorreu na porta da frente, nas camadas de aplicativos ou de infraestrutura. Portanto, é aí que as equipes de segurança investiram seu tempo e seus recursos. Mas os invasores são inteligentes. Eles vão procurar o caminho de menor resistência e, na maioria das vezes, esse caminho será pelas portas dos fundos causadas por lacunas nas medidas de segurança cibernética de terceiros", disse Marcus.

[11]"Digital Risk Report 2023: Pervasive Risk, Persistent Fragmentation, and Accelerating Techno- logy Investment", John A. Wheeler, Auditboard, julho de 2023, https://www.auditboard.com/resources/ ebook/digital-risk-report-2023/.

PRESSÕES REGULATÓRIAS

Também contribui para a pressão que as organizações estão sentindo em relação aos riscos cibernéticos de terceiros o cenário regulatório em constante mudança, que recentemente acelerou o ritmo para corresponder à velocidade do risco. Essas mudanças incluem as novas exigências que o governo federal dos EUA está impondo aos seus parceiros da cadeia de suprimentos, o que teve efeitos indiretos em vários setores. “Você pode pensar que as exigências federais de maior transparência em relação à segurança de dados afetariam apenas as empresas que fazem negócios com o governo federal, mas há exigências de terceiros e de terceiros que fluem pela cadeia de suprimentos e se propagam pela hierarquia ou pelos prestadores de serviços”, apontou Marcus. “Isso cria uma cultura de responsabilidade que permeia muitos setores.”

Os órgãos reguladores também começaram a tomar medidas mais formais para lidar com os riscos de segurança cibernética de terceiros. Isso incluiria as novas regras recentemente promulgadas pela Comissão de Valores Mobiliários (SEC) dos EUA, como as novas regras que exigem que os registradores divulguem incidentes materiais de segurança cibernética. “Mesmo que sua empresa não seja diretamente aplicável a novas regras ou regulamentações, essas regras permeiam a cultura da segurança cibernética”, declarou Marcus. “É uma mudança cultural que está criando uma expectativa de transparência e responsabilidade.”

Estabelecimento de uma cultura de ação cibernética

As organizações não ignoram essas deficiências. De fato, a maioria está ciente delas de alguma forma, mesmo que essa consciência nem sempre se traduza em entendimento e ação em toda a organização. Embora poucas funções de auditoria interna possam alegar ter conhecimento adequado de cibersegurança para abordar diretamente os aspectos técnicos da cibersegurança de terceiros, o que elas podem fazer é alavancar suas posições únicas para unir os pontos de vista de vários stakeholders envolvidos no gerenciamento desse risco (por exemplo, jurídico, compras, TI e os próprios terceiros). Isto posto, os auditores internos podem usar sua interação direta com o comitê de auditoria e o conselho para garantir que esse ponto de vista seja comunicado regularmente e com precisão.

Esse ponto de vista é extremamente importante para que os CEOs e os líderes organizacionais estimulem a ação apropriada, disse Wheeler, e é algo que as funções de gerenciamento de riscos devem se esforçar para entender o suficiente para articular. "Os CEOs precisam de insights em tempo real, tanto de dentro quanto de fora da organização, em todo o ecossistema de ativos de tecnologia que estão mudando dinamicamente", afirmou ele. "Por meio desse processo, eles terão uma melhor compreensão de seus produtos e serviços digitais."[12]

A unidade dentro da organização, entretanto, não é suficiente. Ela deve incluir as partes interessadas de fora da organização. "Cada relacionamento com terceiros deve ter um proprietário designado ou uma pessoa responsável que seja responsável por manter o relacionamento com o fornecedor, manter as informações de contato do fornecedor e gerenciar os termos do contrato", alertou Marcus. "Os relacionamentos com terceiros diferem de um fornecedor para outro - alguns podem oferecer à sua organização uma equipe designada de suporte ao cliente ou de sucesso que fornece serviços suplementares, enquanto outros adotam uma abordagem 'pronta para uso'. Manter as linhas de comunicação abertas e claras entre sua organização e os terceiros é um componente importante, mas frequentemente negligenciado, do gerenciamento eficaz de riscos de terceiros."

[12] "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations", CyberRisk Alliance e AuditBoard, fevereiro de 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties--limited-supply-chain-visibility-big-risks-for-organizations/.

Acriação dessa cultura não só pode estimulara ação preventiva,como também pode aumentaravelocidade das reações quando ocorre um ataque cibernético ou uma violação. No relatório da CyberRrisk Alliance, 20% dos entrevistados disseram que poderia levaruma semana ou mais para avaliarum ataque ou uma violação, atribuindo o tempo prolongado às dificuldades de fazer com que os fornecedores ou parceiros denunciem ou assumam a responsabilidade porisso. Criar uma cultura cibernética positiva e transparente dentro da organização e em toda a sua cadeia de suprimentos pode reduzir esse tempo de uma semana para horas, diminuindo drasticamente as perdas no processo.

"Todo o processo de gerenciamento de riscos de terceiros", disse Marcus, "deve ser construído em torno de uma cultura de responsabilidade em que todos estejam cientes dos riscos de terceiros".

UMA ABORDAGEM DE MONITORAMENTO CONTÍNUO COM BASE NO NÍVEL DE RISCO

Além de ser um definidor de tom, a auditoria interna pode e deve atuar como um recurso valioso na elaboração do programa de gerenciamento de riscos de terceiros no que diz respeito aos riscos cibernéticos - e avaliá-lo continuamente.

"Eu diria que a principal responsabilidade da auditoria interna, assim como na maioria dos casos, é avaliar a eficácia do programa de TPRM", disse Marcus. "Isso pode incluir um inventário completo ou uma imagem de todos os terceiros que estão em uso na organização, entendendo os riscos aos quais esses terceiros podem expor a organização e entendendo como a organização está avaliando a força dos controles nessas organizações terceirizadas."

Novamente, embora os especialistas no assunto devam ser usados para análise técnica, muitos dos princípios de gerenciamento de riscos usados pela auditoria interna são aplicáveis a esse tópico.

Por exemplo, a auditoria interna deve ter um sólido entendimento da análise de riscos, geralmente visualizada por meio de mapas de calor ou outras ferramentas. Essas táticas podem ser usadas como um guia para as partes interessadas responsáveis pela integração e monitoramento de terceiros, a fim de obter um melhor entendimento de quem e o que priorizar.

"O fator de sucesso mais importante para um programa de TPRM é estruturar e formalizar as atividades de monitoramento contínuo com base no nível de risco", disse Marcus. "Terceiros de alto risco devem receber mais atenção com mais frequência, e terceiros de baixo risco devem receber menos atenção com menos frequência." É importante observar, continua ele, que embora o terceiro em questão possa não ser de alto risco por si só, a natureza do relacionamento - como o tipo de dados que está sendo transferido (por exemplo, dados confidenciais, dados de clientes, dados proprietários) - pode aumentar ou diminuir a categorização de risco.

Para ajudar nessa tarefa, o AuditBoard usa o exemplo a seguir (Figura 3) como ponto de partida para estruturar revisões relacionadas às três categorias de níveis de risco a seguir:[13]

Figura 3

Característica do Nível de risco	Nível 1 Alto risco	Nível 2 Risco médio	Nível 3 Baixo risco
Data de acesso	Confidencial	Privado	Público ou não
Frequência de revisão	1 ano	2 anos	3 anos
Requerimentos de revisão	Auditoria interna Questionários de controle Revisão de certificação	Certificação de revisão	Nenhum

Observação: os gráficos e dados da Figura 1 e da Figura 2 foram extraídos de "Effective Third-Pary Risk Management: Key Tactics and Success Factors" da AuditBoard. p. 8, 2022.

A verificação de terceiros não termina na integração, mas deve ser continuamente revisada com base no nível de risco percebido. Garantir que as partes interessadas se mantenham a par de seus próprios compromissos com revisões regulares, bem como dos processos que usam para conduzir essas revisões, deve estar diretamente dentro do universo de riscos da auditoria interna. As ideias para esses processos podem incluir:

- Verificação de certificações e relatórios de conformidade, como o SOC 2. As estruturas comuns para verificar as certificações de conformidade incluem SOC 2, ISO 27001 e NIST SP 800-161.
- Uso de questionários padronizados. Eles podem incluir o Questionário de Coleta de Informações Padronizadas (SIG) ou o CCM e o CAIQ da Cloud Security Alliance.
- Questionários de controles de segurança.

[13] "Gerenciamento eficaz de riscos de terceiros: Key Tactics and Success Factors", AuditBoard, janeiro de 2022, https://www.auditboard.com/resources/ebook/effective-third-party-risk-managemen- t-key-tactics-and-success-factors/?utm_campaign=effective-third-party-risk-management-key-tactics--and-success-factors-0122022&utm_medium=download-image&utm_source=blog.

EMBRACE SOFTWARE SOLUTIONS

Para manter tantas variáveis juntas, a auditoria interna, assim como outras funções de gerenciamento de riscos, também deve priorizar o abandono do processo manual em favor de soluções de software. “A auditoria interna pode ser uma defensora do investimento em tecnologias para tornar os processos de gerenciamento de riscos de terceiros mais eficientes”, declarou Marcus. “Em muitas situações, as eficiências de escala simplesmente exigem isso. Lembro-me de uma das primeiras organizações em que implementei práticas de riscos de terceiros - fizemos avaliações de riscos para cinco ou seis fornecedores e depois consideramos expandir esse processo para todos os fornecedores. Ficamos chocados ao descobrir, no entanto, que havia 17.000 fornecedores nessa empresa. Simplesmente não há como fazer isso sem alguma plataforma habilitada por tecnologia que facilite o dimensionamento para centenas, milhares ou dezenas de milhares de fornecedores.”

Além do mais, essas soluções também apresentam uma excelente oportunidade para a auditoria interna colaborar mais estreitamente com outras funções de risco de terceiros. “Muitas das barreiras à colaboração envolvem problemas de compartilhamento de dados e fluxo de trabalho”, disse Marcus. “Ter uma plataforma de tecnologia em que as duas equipes possam avaliar o cenário de fornecedores juntas - usando o mesmo painel, o mesmo banco de dados de fornecedores etc. - permite que elas trabalhem juntas de forma muito mais eficiente e busquem resultados comuns.

FOCO NA INTEGRAÇÃO EXTERNA E INTERNA

Os relacionamentos com terceiros raramente duram para sempre. Entretanto, o fato de um relacionamento terminar formalmente nem sempre significa que as linhas de dados entre as partes se fecham. Por mais óbvio que isso possa parecer, essas linhas esquecidas são responsáveis por algumas das maiores lacunas encontradas nos sistemas de segurança cibernética de terceiros das organizações, criando “backdoors digitais” que estão prontos para serem explorados intencionalmente ou não. Ao avaliar as práticas de revisão de terceiros, isso é algo que a auditoria interna não deve ignorar.

“É essencial estar atento aos detalhes na fase de desinstalação”, alertou Marcus. “No atual ecossistema digital entrelaçado, é fácil não perceber contas, serviços ou usuários de terceiros que precisam ser removidos ou desativados. Os privilégios de acesso precisam ser revogados, as contas de usuário desativadas e qualquer software ou aplicativo emitido por terceiros removido. Isso é algo que a auditoria interna deve absolutamente observar.”

Conclusão

O futuro das organizações é cibernético. A cada ano que passa, fica claro que essa tendência veio para ficar - e o fato de a segurança cibernética exigir conjuntos de habilidades mais especializados não significa que o cenário de negócios vai esperar que as partes interessadas se instruam. A segurança cibernética é uma jornada contínua de aprendizado, e todas as partes envolvidas em relacionamentos com terceiros devem considerá-la como tal.

Felizmente, há sinais positivos de que as organizações estão aceitando essa realidade. No relatório de inteligência comercial da CyberRisk Alliance, quase dois em cada três entrevistados disseram que a medida mais comum que usaram para evitar ou atenuar o risco de ataques de terceiros foi o treinamento dos funcionários. Embora os riscos associados a terceiros nunca acabem, as políticas e respostas amadurecerão até o ponto em que eles sejam tão facilmente gerenciados quanto qualquer outro risco estabelecido. Esse momento não é hoje, mas estamos chegando lá, e a garantia eficaz do gerenciamento de riscos da auditoria interna ajudará as organizações a chegarem em segurança.[14]

[14]"Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Orga- nizations", CyberRisk Alliance e AuditBoard, fevereiro de 2023, https://www.auditboard.com/resources/ ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

Sobre o IIA

O Institute of Internal Auditors (IIA) é uma associação profissional internacional sem fins lucrativos que atende a mais de 235.000 membros globais e concedeu mais de 190.000 certificações de Certified Internal Auditor (CIA) em todo o mundo. Fundado em 1941, o The IIA é reconhecido em todo o mundo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para obter mais informações, acesse theiia.org.

Sobre o AuditBoard

A AuditBoard é a principal plataforma baseada em nuvem que transforma o gerenciamento de auditoria, risco, conformidade e ESG. Mais de 40% das empresas listadas na Fortune 500 utilizam o AuditBoard para fazer seus negócios avançarem com mais clareza e agilidade. A AuditBoard é bem avaliada pelos clientes no G2, Capterra e GartnerPeer Insights, e foi recentemente classificada pelo quinto ano consecutivo como uma das empresas de tecnologia que mais crescem na América do Norte pela Deloitte. Para saber mais, acesse: AuditBoard.com.

Isenção de responsabilidade

O IIA publica este documento apenas para fins informativos e educacionais. Este material não tem a intenção de fornecer respostas definitivas para circunstâncias individuais específicas e, como tal, destina-se apenas a ser usado como liderança de pensamento informada por colegas. Ele não é uma orientação formal do IIA. O IIA recomenda a busca de aconselhamento especializado independente relacionado diretamente a qualquer situação específica. O IIA não se responsabiliza por qualquer pessoa que confie exclusivamente neste material.

Os Global Knowledge Briefs têm como objetivo abordar tópicos oportunos e relevantes para um público global de auditoria interna, e cada tópico abordado é examinado por membros do Comitê Consultivo de Conteúdo Norte-Americano voluntário do The IIA. Os especialistas no assunto são identificados e selecionados principalmente na lista de Colaboradores de Orientação Global do The IIA.

Para se inscreverna lista de Colaboradores do Global Guidance, envie um e-mail para Standards@ theiia.org. Para sugerir tópicos para futuros Global Knowledge Briefs, envie um e-mail para Content@theiia.org.

Direitos autorais

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