TONE at the TOP®

Trazendo à alta administração, conselhos de administração e comitês de auditoria informações concisas sobre tópicos relacionados a governança.

Edição 106 | Agosto de 2021

Confrontando o Monstro da Cibersegurança

O risco cibernético afeta organizações de todos os tamanhos e em todas as indústrias, e parece que veio para ficar. Uma pesquisa com conselhos e executivos globais classificou as ciberameaças como um dos dez maiores riscos de 2021, e os entrevistados esperam que elas também sejam um grande risco em 2030. Na verdade, o crime cibernético global deve aumentar 15% ao ano, com seu impacto anual previsto para atingir US$ 10,5 trilhões até 2025, de acordo com a *Cybersecurity Ventures*. A empresa de pesquisa cibernética chama isso de "a maior transferência de riqueza econômica da história".

Ocorrências de cibersegurança podem assumir a forma de ransomware, ataques a recursos de trabalho remoto, ataques à cadeia de suprimentos, phishing ou qualquer outra prática criminosa. Elas podem prejudicar uma empresa, extrair um valor significativo da empresa e sujeitá-la a passivos ou aparições na mídia que prejudiquem sua reputação. Os custos de uma violação de dados são altos e crescentes, com média de US$ 4,24 milhões em 2021, um aumento de quase 10% em um ano, com base nos dados da IBM.

Além do mais, a pandemia do COVID-19 só criou novas vulnerabilidades que ainda precisam ser totalmente compreendidas ou tratadas.

Gerenciando os Perigos

Com tanto em jogo, há uma série de etapas que os conselhos podem seguir para melhorar sua supervisão dos riscos cibernéticos. Ao longo do processo, a auditoria interna pode servir como um parceiro fundamental. Trabalhando em colaboração com os especialistas em cibersegurança da organização, a equipe de auditoria interna pode oferecer avaliação objetiva de que os planos da organização estejam sendo executados conforme o planejado e de que são adequados para a tarefa. “Eles podem dizer ao conselho se há grande exposição ou uma falsa sensação de segurança”, disse Sandy Pundmann, CIA, sócia sênior aposentada da *Deloitte Risk and Financial Advisory*.

Existem várias estratégias do conselho para ajudar a lidar com o risco cibernético. Pundmann e outros recomendam que os conselhos mantenham um conhecimento aguçado do perfil de risco cibernético de suas organizações, adotem seu papel de supervisão e pratiquem o ceticismo saudável, para garantir que tenham uma compreensão clara das forças, fraquezas e vulnerabilidades.

Estabeleça papéis de supervisão e programe atualizações regulares. Embora menos de 10% dos conselhos hoje tenham um comitê dedicado à cibersegurança liderado por um membro qualificado do conselho, espera-se que esse número suba para 40% até 2025, de acordo com uma pesquisa da Gartner, Inc. O aumento esperado pode ser impulsionado pela expansão dos negócios digitais durante a pandemia e pela adoção do trabalho remoto e seus riscos potenciais adicionais.

Sobre o The IIA

The Institute of Internal Auditors Inc. (The IIA) é uma associação profissional internacional com mais de 200.000 membros em mais de 170 países e territórios. O The IIA serve como principal defensor da profissão de auditoria interna, criador global de tendências e maior pesquisador e educador.

The IIA

1035 Greenwood Blvd.
Suíte 149
Lake Mary, FL 32746 EUA

Assinaturas Gratuitas

Visite www.theiia.org/Tone para se cadastrar para uma assinatura gratuita.

Feedback do Leitor

Envie perguntas/comentários para Tone@theiia.org.

Atualmente, a responsabilidade pela supervisão da cibersegurança pode ser difícil de identificar, porque, muitas vezes, está dispersa entre a gestão e vários comitês, disse Pundmann. Um comitê deve ser encarregado da responsabilidade e deve discutir o assunto em todas as reuniões, acrescentou ela. A cibersegurança também deve estar na pauta do conselho pleno no mínimo duas vezes por ano.

Reconheça o nível de ameaça. A cibersegurança é mais do que um problema de TI. "Seja antes ou durante um incidente, você não deve apenas deixar [a cibersegurança] para o diretor de informações e a equipe técnica", disse John Noble, ex-diretor do *National Cyber Security Center* do Reino Unido, em um podcast da McKinsey. "Os líderes precisam decidir como gerenciar as tensões entre usabilidade, segurança e custo, e é exatamente aí que precisamos que o conselho questione e teste os processos."

Mergulhe mais fundo. Os conselhos devem estar cientes se suas organizações estão avaliando e aprimorando regularmente suas avaliações de risco cibernético. A equipe de auditoria interna é frequentemente chamada para conduzir uma avaliação ou projeto inicial, talvez uma auditoria de ataque e penetração, mas isso é apenas o primeiro passo, advertiu Pundmann. As empresas precisam de uma estratégia multifacetada para prevenir, detectar e responder a eventos cibernéticos. O esforço deve incluir uma avaliação das medidas em andamento que a empresa está tomando para entender os ataques, a eficácia das medidas que estão sendo tomadas, como os incidentes e as respostas são monitorados, e a mecânica e o sucesso da resposta da empresa. A avaliação completa da estratégia pode começar no nível do comitê, mas deve ser discutida por todo o conselho, disse ela.

Como observou uma publicação da Deloitte, a primeira linha contra o risco cibernético é composta pelas unidades de negócios e pela TI, que abordam o risco em suas decisões e operações diárias. A segunda linha da organização é a liderança de gerenciamento de riscos de informação e tecnologia, que assume a governança e a supervisão. A função de auditoria interna é cada vez mais a terceira linha, conduzindo uma revisão independente das medidas de segurança e desempenho.

Entenda o que diferencia esse risco. As organizações e seus conselhos estão familiarizados com os riscos, mas a cibersegurança é diferente por alguns motivos. Em primeiro lugar, é altamente especializada e as ameaças estão em constante mudança, o que as coloca além da experiência de muitos membros do conselho. Em segundo lugar, o uso da Internet é difundido na maioria das organizações, portanto, os riscos e seu impacto são multifacetados e complexos. "O acesso corporativo à Internet é fundamental para a entrega de valor, e todas as transações que dependem do acesso à Internet são inerentemente inseguras", disse um participante em um painel de discussão da *Cyber Risk Director Network*. "Isso não se aplica a qualquer outro aspecto dos riscos com os quais os conselhos lidam."

PERGUNTAS PARA MEMBROS DO CONSELHO

- Com que frequência o conselho recebe atualizações sobre as ameaças à cibersegurança da organização e sobre as medidas que estão sendo tomadas para abordar e gerenciar os riscos cibernéticos?
- A organização está abordando a cibersegurança como uma questão de risco corporativo, e não exclusivamente como preocupação de TI?
- O conselho tem função proativa no monitoramento dos riscos cibernéticos ou presume que tudo está bem, a menos que receba informação do contrário?
- O conselho tem um comitê de cibersegurança dedicado? Se não, outro comitê, como o comitê de auditoria, tem a responsabilidade de supervisão da cibersegurança?

Obtenha um exemplo da vida real. Em um exercício de simulação, *que pode ser executado pela auditoria interna, outra parte da gestão ou parte externa,* o conselho e a gestão podem supervisionar um ataque simulado para determinar como a organização responde, como os investidores são notificados e como os clientes ou parceiros de negócios são afetados. (Pundmann até trabalhou com um conselho que solicitou que apenas o CIO e o CEO estivessem cientes de que a situação foi simulada, para tornar o exercício o mais realista possível.) Depois que a organização avaliar sua resposta, o conselho pode receber uma atualização sobre as mudanças que foram feitas ou que estão em andamento.

A auditoria interna também pode ser um participante fundamental de outro exercício valioso: uma visualização do modelo de maturidade, que oferece uma visão empresarial de alto nível dos riscos cibernéticos e compara onde a organização está e onde deveria estar, tudo em termos para leigos. Como não é possível monitorar e abordar todos os riscos, esses exercícios também podem ajudar a esclarecer quais metas são as mais críticas, para que a organização possa melhorar a prevenção e detecção nessas áreas, disse Pundmann.

Não deixe os riscos pegarem você de surpresa. Conforme se expande a adoção da tecnologia, também aumentam os riscos associados a tecnologias emergentes desconhecidas. Até mesmo um novo sistema de ERP pode trazer desafios de segurança que não devem passar despercebidos, observou Pundmann. Muitas empresas, erroneamente, esperam até que haja problemas com um novo sistema para, então, planejar como lidar com eles. "Certifique-se de ter um plano de segurança para sua estratégia cibernética e de controle desde o início", disse ela.

Organizações envolvidas em fusões e aquisições também podem enfrentar novas vulnerabilidades. "Se você está adquirindo uma empresa, pergunte quais riscos você está assumindo ao interligar seus negócios", ela aconselhou. As empresas que trabalham com cadeias de suprimento ou outros terceiros também podem estar expostas a riscos dessas fontes. Além disso, na área de compliance, as organizações devem estar cientes dos regulamentos relevantes, como as regras da Comissão de Valores Mobiliários sobre divulgações de cibersegurança.

Alavancando os Recursos de Auditoria Interna

Ciberameaças podem ser assustadoras, mas a auditoria interna pode oferecer uma perspectiva única e independente sobre os riscos à organização e as melhores maneiras de enfrentá-los. Conselhos proativos em seu monitoramento das questões de cibersegurança e que alavancam totalmente o valor que a auditoria interna pode oferecer devem estar em melhor posição para tratar com eficácia os riscos de cibersegurança.

O QUE FALTA EM SEU CONSELHO?

60% das organizações não têm um chefe de cibersegurança que faça parte do conselho ou da equipe de gestão executiva.

59% das organizações dizem que a relação entre cibersegurança e as linhas de negócios são, no melhor dos casos, neutras, não confiáveis ou inexistentes.

20% dos conselhos estão extremamente confiantes de que os riscos de cibersegurança e as medidas de mitigação apresentadas a eles podem proteger a organização de grandes ciberataques.

36% das organizações dizem que a cibersegurança é envolvida desde o estágio de planejamento de uma nova iniciativa de negócios.

Fonte: *"The Risky Six: Key Questions to Expose Gaps in Board Understanding of Organizational Cyber Resiliency,"* IIA Global e EY, 30 de março de 2021.

[1] *Executive Perspectives on Top Risks for 2021 and 2030*, *ERM Initiative* da Protiviti e da NC State University, 2021.
[2] *"Cybercrime to Cost the World $10.5 Trillion Annually by 2025"*, Steve Morgan, *Cybercrime Magazine*, 13 de novembro de 2020.
[3] *Cost of a Data Breach Report*, IBM, 2021.
[4] *"Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025"*, press release da Gartner, 28 de janeiro de 2021.
[5] *"Boards and Cybersecurity"*, podcast da McKinsey & Company, 2 de fevereiro de 2021.
[6] *"Cybersecurity and the Role of Internal Audit: An Urgent Call to Action"*, Sandy Pundmann, Deloitte, 2017.
[7] *"Cybersecurity: An Evolving Governance Challenge"*, *Forum on Corporate Governance*, da Harvard Law School, 15 de março de 2020.
[8] *"Commission Statement and Guidance on Public Company Cybersecurity Disclosures,"* *Release Nos. 33-10459; 34-82746*, Securities and Exchange Commission, 26 de fevereiro de 2018.

Pergunta da Pesquisa Rápida

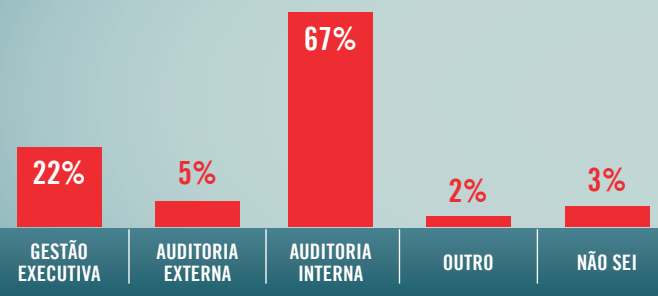
Seu conselho tem um membro com expertise em cibersegurança?

- ❑ Sim
- ❑ Não
- ❑ Não sei

Visite www.theiia.org/tone para responder à pergunta e ver como outros estão respondendo.

RESULTADOS DA PESQUISA RÁPIDA

Em quem o conselho confia principalmente, para garantir a eficácia do gerenciamento de riscos e do controle interno?



Fonte: Pesquisa do Tone at the Top de junho de 2021.