Reforço da capacidade de cibersegurança
Caixa de ferramentas para organizações financeiras

Guia ao nível do CEO: Liderança de cibersegurança

Governança

A segurança cibernética da sua organização começa e termina ao nível mais elevado da gestão. O CEO, juntamente com o Conselho, deve manter a compreensão dos riscos e assumir a responsabilidade final e responsabilidade pelas atividades e pessoal de cibersegurança da organização. Deve:

⇒ Contratar um Diretor Executivo de Segurança da informação (CISO), caso não exista, ou, se os recursos forem demasiado limitados, nomear alguém dentro da sua organização para desempenhar a função de um CISO.
⇒ Trabalhar com o CISO ou outro pessoal técnico para estabelecer e manter uma estratégia e estrutura de cibersegurança adaptada aos riscos cibernéticos específicos da organização, utilizando normas e diretrizes internacionais, nacionais e da indústria.
⇒ Articular funções e responsabilidades claras para o pessoal que implementa e gere a cibersegurança da organização.

- Trabalhar com o CISO para identificar as funções de cibersegurança adequadas e direitos de acesso para todos os níveis de pessoal.
- Supervisionar a comunicação e colaboração para garantir que a gestão de cibersegurança é holística, principalmente se as responsabilidades de cibersegurança forem partilhadas por vários funcionários ou divisões dentro da organização (como, por exemplo, ter informações de segurança da informação, risco e tecnologia).

⇒ Certificar-se de que o CISO tem uma linha direta e clara de comunicação para relacionar ameaças de forma atempada para si e para o Conselho.
⇒ Convidar o CISO ou outro pessoal técnico para informar regularmente a alta direção.
⇒ Certificar-se de que as políticas de segurança, normas, mecanismos de aplicação e procedimentos da organização são uniformes em todas as equipas e linhas de negócio.

Avaliação e gestão de riscos

Garantir que uma forte consciencialização e preparação de cibersegurança depende da análise contínua baseada no risco. Para melhorar a cibersegurança da sua organização:

⇒ Estabeleça a avaliação e gestão do risco de cibersegurança como uma prioridade nos processos de controlo e gestão de riscos mais amplos da sua organização. Trabalhe com o seu CISO ou outro pessoal técnico num plano para realizar uma avaliação de risco que envolva:

- Descrever os ativos da sua organização e os seus vários níveis de dependência tecnológica,
- Avaliar a maturidade da sua organização e os riscos inerentes associados às dependências tecnológicas dos seus ativos,
- Determinar o estado desejado da maturidade da sua organização,
- Compreender onde as ameaças de cibersegurança se encontram na lista de prioridades de risco da sua organização,
- Identificar lacunas entre o seu estado atual de cibersegurança e o estado alvo pretendido,
- Implementar planos para atingir e sustentar a maturidade,
- Reavaliar continuamente a maturidade, os riscos e os objetivos da segurança cibernética da sua organização, e
- Considerar a utilização de testes de invasão de terceiros ou red-teaming,
- Considerar medidas de proteção como a compra de um seguro cibernético.

⇒ Liderar os esforços dos funcionários durante o processo de avaliação de riscos para facilitar respostas atempadas de toda a instituição.
⇒ Analisar e apresentar os resultados da avaliação de risco para a supervisão executiva, incluindo os principais intervenientes e o Conselho.
⇒ Supervisionar quaisquer alterações para manter ou aumentar a preparação da cibersegurança pretendida da sua organização, assegurando que quaisquer medidas tomadas para melhorar a cibersegurança são proporcionais aos riscos e acessíveis para a sua organização.
⇒ Supervisionar o desempenho da monitorização contínua para se manter ágil e flexível no tratamento de risco cibernético em evolução.

Cultura organizacional

A cibersegurança da sua organização não é um processo único ou o trabalho de alguns funcionários; é um fator a considerar em todas as decisões e operações comerciais e uma prática que deve ser mantida por todos os funcionários. Para incentivar a cibersegurança contínua e holística dentro da sua organização:

⇒ Inicie discussões sobre cibersegurança com a equipa de liderança e comunicar regularmente com o pessoal responsável pela gestão de riscos cibernéticos.
⇒ Faça com que a formação de cibersegurança faça parte de toda a integração dos funcionários, assegurando que todos os funcionários estão atualizados – e assinaram documentos em que concordam em cumprir – as políticas de cibersegurança da sua organização e que o seu departamento de TI ou outro pessoal técnico os tenha informado sobre as melhores práticas.
⇒ Institua formação de cibersegurança recorrente para todo o pessoal relativamente às suas responsabilidades de segurança a curto e longo prazo.
⇒ Certifique-se de que a cibersegurança é sempre considerada quando a sua organização avalia potenciais fornecedores e partilha dados com terceiros.
⇒ Reveja anualmente as políticas de cibersegurança da sua organização.
⇒ Incentive a partilha voluntária de informação sobre ameaças de cibersegurança e incidentes dentro da sua organização e com contrapartes de confiança.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE