Fomento de la capacidad en materia de ciberseguridad Cuadro de herramientas para organizaciones financieras

Guía para el CEO: Liderazgo en ciberseguridad

Gobernanza

La ciberseguridad de su organización comienza y termina en el nivel más alto de gerencia. El CEO (Chief Executive Officer [Director ejecutivo]), junto con la junta, debe mantener la comprensión de los riesgos y asumir la responsabilidad final de las actividades y el personal de ciberseguridad de la organización. Usted debe:

⇒ Contratar a un director de seguridad de la información (CISO) si no existe o, si los recursos son demasiado limitados, designar a alguien dentro de su organización para que cumpla con la función de un CISO.
⇒ Trabajar con el CISO u otro personal técnico para establecer y mantener una estrategia y un marco de seguridad cibernéticos adaptados a los riesgos cibernéticos específicos de la organización, utilizando normas y directrices internacionales, nacionales y sectoriales.
⇒ Articular funciones y responsabilidades claras para el personal que implementa y gestiona la ciberseguridad de la organización.

- Trabajar con el CISO para identificar las funciones de ciberseguridad y los derechos de acceso adecuados para todos los niveles de personal.
- Supervisar la comunicación y la colaboración para garantizar que la gestión de ciberseguridad sea holística, especialmente si las responsabilidades de ciberseguridad son compartidas por múltiples personas o divisiones dentro de la organización (como, por ejemplo, tener verticales independientes de seguridad de la información, riesgo y tecnología).

⇒ Garantizar que el CISO tiene una línea de comunicación clara y directa para comunicar las amenazas de forma oportuna con usted y con la junta.
⇒ Invitar al CISO u otro personal técnico para que informe de manera sistemática a la alta gerencia.
⇒ Garantizar que las políticas, normas, mecanismos de aplicación y procedimientos de seguridad de la organización sean uniformes en todos los equipos y líneas de negocio.

Evaluación y gestión de riesgos

Garantizar una sólida concienciación y preparación de ciberseguridad depende de un análisis continuo basado en el riesgo. Para mejorar la ciberseguridad de su organización:

⇒ Establezca la evaluación y la gestión de riesgos de ciberseguridad como prioridad dentro de los procesos más amplios de gestión de riesgos y gobernanza de su organización. Trabaje con su CISO u otro personal técnico en un plan para realizar una evaluación de riesgos que implique:

- Describir los activos de su organización y sus diversos niveles de dependencia tecnológica.
- Evaluar la madurez de su organización y los riesgos inherentes asociados a las dependencias tecnológicas de sus activos.
- Determinar el estado de madurez deseado de su organización.
- Comprender dónde se encuentran las amenazas de ciberseguridad en la lista de prioridades de riesgo de su organización.
- Identificar brechas entre su estado actual de ciberseguridad y el estado objetivo deseado.
- Implementar planes para alcanzar y mantener la madurez.
- Reevaluar continuamente la madurez, los riesgos y los objetivos de la ciberseguridad de su organización.
- Tener en cuenta el uso de pruebas de penetración de terceros o simulacros de ataque.
- Considerar tomar medidas de protección, como adquirir un seguro cibernético.

⇒ Lidere los esfuerzos de los empleados durante el proceso de evaluación de riesgos para facilitar las respuestas oportunas de toda la institución.
⇒ Analice y presente los resultados de la evaluación de riesgos para la supervisión ejecutiva, incluidas las partes interesadas clave y la junta.
⇒ Supervise cualquier cambio para mantener o aumentar la preparación de seguridad cibernética deseada de su organización, asegurándose de que los pasos adoptados para mejorar la ciberseguridad sean proporcionales a los riesgos y asequibles para su organización.
⇒ Supervise el rendimiento de la monitorización continua para permanecer hábiles y ágiles al abordar el riesgo cibernético en evolución.

Cultura organizativa

La ciberseguridad de su organización no es un proceso único ni el trabajo de unos pocos empleados; es un factor que debe tenerse en cuenta en todas las decisiones y operaciones empresariales, y una práctica que debe ser mantenida por todos los empleados. Para fomentar la ciberseguridad continua y holística dentro de su organización:

⇒ Inicie conversaciones sobre ciberseguridad con el equipo de liderazgo y comuníquese regularmente con el personal responsable de gestionar los riesgos cibernéticos.
⇒ Haga que la formación sobre ciberseguridad forme parte de la incorporación de todos los empleados, asegurándose de que todo el personal esté al tanto de las políticas de ciberseguridad de su organización, que los empleados hayan firmado documentos para adherirse a estas, y que su departamento de TI u otro personal técnico les hayan informado sobre las mejores prácticas.
⇒ Impulse la formación en ciberseguridad recurrente para todo el personal con respecto a sus responsabilidades de seguridad a corto y largo plazo.
⇒ Asegúrese de que la ciberseguridad siempre se tenga en cuenta cuando su organización evalúe los posibles proveedores y comparta datos con terceros.
⇒ Revise anualmente las políticas de ciberseguridad de su organización.
⇒ Fomente el intercambio voluntario de información sobre amenazas e incidentes de ciberseguridad dentro de su organización y con homólogos de confianza.

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