El riesgo cibernético y cómo el C-Suite puede ayudar a mitigarlo

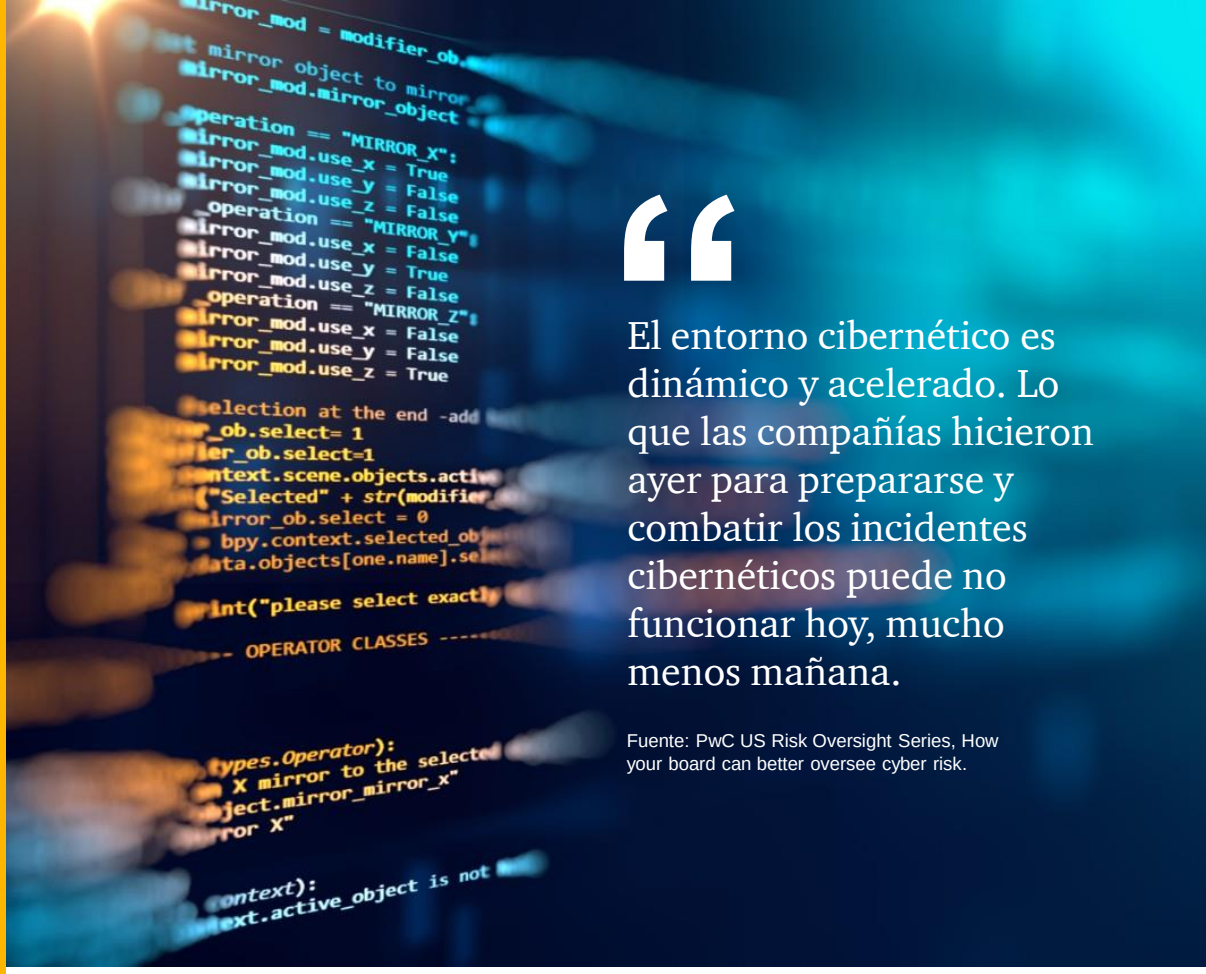
Por Aida Morales, Consultora de Riesgos en PwC Honduras

Según revelan algunos estudios, como el de Kaspersky Lab realizado en Latinoamérica, Honduras es considerado el segundo país con más ataques cibernéticos, con un 23.5% de los usuarios con ataques de malware, seguido de Panamá con 22.6% y Guatemala con 21.6%. Ahora bien, la responsabilidad de gestionar el riesgo de ataques cibernéticos no recae únicamente sobre el área de TI. El CISO (Director de Seguridad de la Información) y su equipo no pueden hacer el trabajo solos. Para hacerle frente al riesgo cibernético, la Junta Directiva, la Administración, los Líderes de Unidad de Negocio y los grupos de seguridad y de TI deben involucrarse para su debida gestión.

Es entonces donde el C-suite entra a jugar un rol fundamental en la gestión y mitigación de dicho riesgo. El C-suite se refiere a los gerentes de nivel ejecutivo dentro de una organización, usualmente al:

- Director Ejecutivo (CEO)
- Director Financiero (CFO)
- Director de Operaciones (COO)
- Director de Seguridad de la Información (CISO)

Más allá de este grupo, otros que deben formar parte de esta gestión son todos los colaboradores de la organización. Al recibir entrenamientos, cumplir las políticas y procedimientos establecidos, y reportar actividades sospechosas ayudan a mitigar los riesgos de seguridad de TI.



> El entorno cibernético es dinámico y acelerado. Lo que las compañías hicieron ayer para prepararse y combatir los incidentes cibernéticos puede no funcionar hoy, mucho menos mañana.

Fuente: PwC US Risk Oversight Series, How your board can better oversee cyber risk.

A continuación se detallan 7 aspectos claves que C-Suite debe tomar en cuenta al supervisar el riesgo cibernético:

1. Abordar el riesgo cibernético en todas las unidades de negocio. Es necesario saber quién reporta por parte de cada unidad, ya que están igualmente expuestas que el área de TI.

2. Tener un enfoque de supervisión con acceso a la experiencia cibernética, ya sea contratando a un director con dicha experiencia y/o recibiendo capacitaciones continuamente.

3. Comprender los requisitos legales y reglamentarios y saber si la C-Suite tiene los recursos necesarios para cumplirlos.

4. Discutir la adecuación de la estrategia y el plan cibernético periódicamente y dar a conocer cómo éstas se alinean con los objetivos de la organización.

5. Realizar discusiones entre la Alta Gerencia y C-Suite sobre el nivel de riesgo que la organización está dispuesta a aceptar: el apetito del riesgo cibernético.

6. Obtener la información correcta para monitorear el programa de ciberseguridad y privacidad.

7. Monitorear la resistencia cibernética con el objetivo de detectar y responder a los ataques cibernéticos lo suficientemente rápido para minimizar las interrupciones en el negocio y pérdidas financieras.

En la última encuesta de CEO regional, los líderes centroamericanos ubicaron las ciberamenazas en su top 5 de desafíos para el crecimiento de los negocios con un 63%.