

Análisis

ÁLVARO BUSTOS

Profesor PUC, Princeton Ph.D., director CGC-UC.



GOBIERNOS CORPORATIVOS Y CIBERSEGURIDAD

La ciberseguridad es uno de los temas estratégicos más desafiantes que enfrenta la administración moderna. El costo mundial del "cibercrime" fue de US\$ 6 trillones en 2021, y se espera llegue a US\$ 10,5 trillones en 2025 (Cybercrime Magazine). Las formas de ciberataques varían desde sabotajes con demandas extorsivas a empresas (Colonial Pipeline) y gobiernos (NotPetya) hasta el robo de propiedad privada/datos (Yahoo y Equifax). Contrario a la antigua creencia de dominio exclusivo de departamentos de IT, hoy queda en claro que la ciberseguridad le compete a la alta dirección de las organizaciones, es decir, es un tema de gobiernos corporativos.

Un artículo del MIT Sloan Management Review del 2018 ya resaltaba el rol de los directorios en prevenir y lidiar con ciberataques. Centralmente, los autores enfatizaban que la mayoría de los ejecutivos desconocen el lenguaje y las métricas de la ciberseguridad. Aún más, no basta con enfocarse en seguridad (prevenir un ataque), sino que también hay que hacerlo en resiliencia (capacidad de seguir funcionando luego de ser atacada). Es decir, las organizaciones deben educar a sus directivos y crear políticas integrales de ciberseguridad.

Cuatro años después del mencionado artículo, Ernest & Young reporta que, si bien muchas empresas en EE.UU. han introducido mejoras, estas serían insuficientes. La inclusión del tema en reportes de riesgo, así como las firmas con procesos que informan al directorio sobre ciberseguridad llegaron a ser 95% y 74% en el 2022, respectivamente. Sin embargo, solo el 9% de las empresas posee simulaciones de respuesta a ciberataques, solo el 23% de los directores dicen "estar preparados" contra un ataque estilo *ransomware* y solo el 28% de los directorios tienen comités especializados.

En EE.UU. se espera que para principios del 2023 la SEC presente nuevos requerimientos de revelación de información sobre ciberseguridad para las empresas abiertas.

Nuestro país no está ajeno a las amenazas de los ciberataques. Según un artículo del Diario Financiero, "Chile sufrió más de 9,4 mil millones de intentos de ciberataques en 2021, cerca de cuatro veces más que los detectados en 2020". Si bien es cierto las brechas que hoy en día existen en el tema son importantes, ya hay esfuerzos encaminados a eliminarlas. Especial mención merece la iniciativa liderada por el Centro de Innovación UC Anacleto Angelini junto a Microsoft Chile que, desde abril de este año, está abocada a elaborar una hoja de ruta para los siguientes tres años con el fin de elevar sustancialmente los niveles de ciberseguridad en el país.