CGC UC
CENTRO DE GOBIERNO CORPORATIVO

DOCUMENTOS DE OPINIÓN

29.2018

Rol de directorios en ciberseguridad

Luis Hernán Paúl[1]

No sólo en Chile hemos vivido casos de empresas como el Banco de Chile que han enfrentado ciberataques. En el extranjero uno de los casos más impactantes es el de la cadena de supermercados Target que en diciembre del 2013 sufrió el robo de información de más de 70 millones de clientes y que tuvo un costo para la empresa de $61 millones, de los cuales 44 lo cubrieron los seguros. También están los casos de la empresa de solvencia crediticia Equifax en el 2017 y del portal de ventas de entradas Ticketmaster ocurrido hace pocos días.

Se trata en realidad de un riesgo que enfrentan muchas empresas, en especial aquellas a las cuales los hackers pueden robarles dinero o información de valor de la propia empresa o de sus clientes.

Dada esta realidad cada vez son más los directorios que se preguntan respecto a qué pueden hacer las empresas para enfrentar este riesgo.

Si bien yo no tengo mayor experiencia en ciberseguridad, lo que puedo aportarles es la visión que me he formado en los últimos años, luego de revisar las prácticas que han adoptado los directorios de diversas empresas en el extranjero para mitigar este riesgo, el cual es considerado de máxima relevancia desde hace ya algunos años.

Lo primero a destacar, aunque parezca obvio, es que este tema debe formar parte de las agendas de los directorios. Ahora, no se trata de una materia que haya que verla todos los meses, pero sí cada cierto tiempo. Lo normal es partir por entender en qué consiste exactamente este riesgo, clarificar las medidas que cuentan para mitigarlo y las que efectivamente está adoptando la empresa para dicho efecto. Digo, ex profeso, la palabra mitigar porque es crítico entender que es imposible eliminar de modo 100% seguro el riesgo de que se produzcan ciberataques. Sólo es factible reducir de forma sustantiva su ocurrencia. Por lo mismo, es fundamental que los directorios, especialmente en las empresas más expuestas a este riesgo, se aseguren de contar con un plan de contingencia para hacer frente a ciberataques de distinta significancia.

De igual forma, para que las medidas para minimizar el riesgo de ciberataques sean efectivas, es indispensable que el personal, en especial aquellos que pueden en forma consciente o inconsciente facilitar el acceso a los hackers a los sistemas informáticos de la empresa sean debidamente advertidos y capacitados.

En el fondo se trata de un tema que no debe ser visto en las organizaciones exclusivamente como una materia de relevancia tecnológica, sino que también de cultura organizacional.

[1] Ingeniero Civil, Pontificia Universidad Católica de Chile. Asesor y director de empresas. Director Centro de Gobierno Corporativo UC.