César Pallavicini, CEO de Pallavicini Consultores y Presidente Comunidad Riesgo Operacional:

"El estado de madurez de Chile en seguridad de la información es bajo"

Con una trayectoria de 21 años en la industria local y extranjera, el analista asegura lo que muchos saben y pocos se atreven a decir: las empresas en Chile aún muestran un claro retraso en desarrollo y gestión de políticas de seguridad de la información, mientras desde el Estado tampoco hay un claro avance.

¿Cómo determina usted el estado actual de la ciberseguridad en Chile hoy?

Cuando se dice que Chile tiene un buen avance en ciberseguridad, y si dejamos establecido que la seguridad de la información es el todo, es decir, ciberseguridad es un subconjunto de la seguridad de la información, se puede afirmar que el estado de madurez de Chile en seguridad de la información es bajo. Las cifras lo avalan. De hecho, existen alrededor de 130 empresas certificadas en ISO 27001. En gestión de continuidad de negocio, la cantidad de empresas certificadas (ISO 22301) es menos de 20.

Un análisis general del sector financiero indica que algunos bancos están certificados, nadie del retail, y casi ninguna compañía de seguros y Administradora de Fondos de Pensiones.

¿Hay otros elementos que afecten a este pobre desarrollo?

Las leyes relacionadas con la gestión de riesgos operacionales llevan años durmiendo en el Congreso, lo que nos lleva a cuestionar si existe conciencia y voluntad de avanzar por parte del Estado chileno en estas materias. Particularmente, me refiero a la Leyes de Protección de Datos Personales, de Delitos Informáticos, de Ciberseguridad y a la Ley de Infrestructuras Críticas, por mencionar las más relevantes del último tiempo.

¿Qué se ha hecho mal y qué se ha hecho bien?

La SBIF (CMF desde el 1 de junio próximo) ha emitido normas y ha realizado exigencias posteriores a los ataques ocurridos. Por tanto, más bien la pregunta es si el sector financiero podrá verdaderamente cumplir con las nuevas reglamentaciones.

En primer lugar, la autoridad ya emitió una circular que obliga a tener una base de datos de incidentes de ciberseguridad, separada de otros eventos de seguridad de la información. Además de ello, impone la figura del encargado de ciberseguridad como responsable y coordinador con la entidad regulatoria. Válido es preguntarse si este encargado tendrá las competencias y atribuciones necesarias o más bien será decorativo.

En 2018 se generaron graves hechos que hacen sospechar que aún no se toman las medidas correctas. ¿Por qué?

Todos los eventos ocurridos durante 2018 seguirán creciendo en forma exponencial en 2019 y se anuncian pérdidas globales del orden de US$3 trillones por ciberataques. Solo un dato como ejemplo: Corea del Norte y su ejército virtual continuán siendo una de las mayores amenazas en ciberseguridad. Sus hackers tienen estrategias de largo plazo y estudian sus ataques, además trabajan los días feriados para aprovechar que las empresas tienen menos personal dedicado a la defensa.

Hay que considerar también que ya existen ránking del "tiempo de quiebre", en otras palabras, tiempo de entrada y salida del hacker en entrometerse y/o robar datos desde una red, siendo actualmente los más veloces el grupo de hackers "Bear" (Moscú) con 18 minutos.

Está claro, con todo lo dicho, que la gobernanza de este tema es fundamental y prioritaria, e idealmente los presupuestos de inversión deben ser asignados y seguidos en forma separada de las inversiones en tecnologías. Así, los directivos asimilarán que es su responsabilidad asegurar la inversión de los accionistas frente a todo tipo de eventos que puedan ocurrir. Mayor información en **www.pallavicini.cl** G