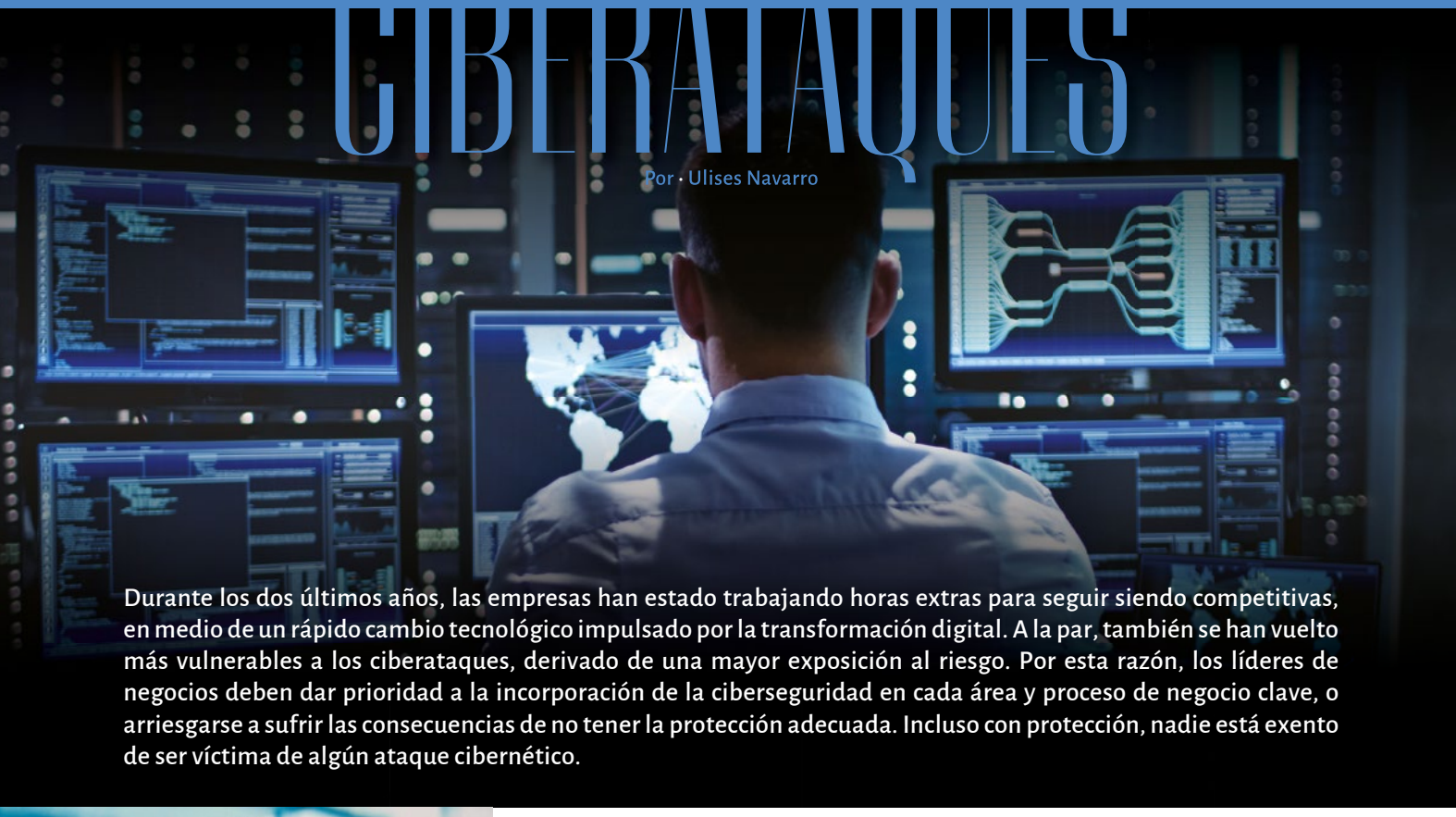
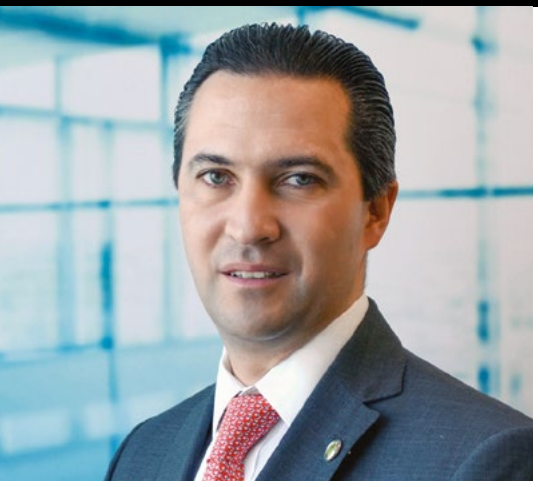
NEGOCIOS TRABAJANDO EN LA PROTECCIÓN CONTRA LOS CIBERATAQUES

Por · Ulises Navarro



Durante los dos últimos años, las empresas han estado trabajando horas extras para seguir siendo competitivas, en medio de un rápido cambio tecnológico impulsado por la transformación digital. A la par, también se han vuelto más vulnerables a los ciberataques, derivado de una mayor exposición al riesgo. Por esta razón, los líderes de negocios deben dar prioridad a la incorporación de la ciberseguridad en cada área y proceso de negocio clave, o arriesgarse a sufrir las consecuencias de no tener la protección adecuada. Incluso con protección, nadie está exento de ser víctima de algún ataque cibernético.



Santiago Gutiérrez, socio líder de Riesgo Cibernético en Deloitte México y Centroamérica

La firma de investigación especializada en seguridad cibernética Cybersecurity Ventures pronostica que los costos globales del cibercrimen crecerán 15% anual durante los próximos cinco años, alcanzando los 10.5 billones de dólares anuales para 2025, frente a los 3 billones de dólares de 2015. Esta cifra, que es la mayor transferencia de riqueza económica en la historia y es exponencialmente mayor que el daño causado por los desastres naturales en un año, pone en riesgo los incentivos para la innovación y la inversión, y será más rentable que el comercio global de las principales drogas ilegales juntas.

Los costos de los delitos cibernéticos incluyen daño y destrucción de datos, dinero robado, robo de propiedad intelectual, robo de datos personales y financieros, malversación, fraude, interrupción del curso normal de la operación del negocio posterior al ataque (que se traduce en pérdida de productividad), investigación forense, restauración y eliminación de datos y sistemas hackeados, así como consecuencias legales y reputacionales.

Las crecientes amenazas están ocasionando que las organizaciones y negocios de todo el mundo incrementen sus medidas de defensa para enfrentar el cibercrimen, el cual, como hemos visto, no se detendrá; peor aún, seguirá aumentando. ¿Por qué? Por un lado, el mundo se hace cada vez más digital, lo que significa que el campo de ataque hacia los usuarios –no solo hacia empresas y gobiernos– es cada vez mayor, es decir, están más expuestos a la ciberdelincuencia. Por otro lado, los delitos seguirán creciendo porque los ciberdelincuentes emplean mejores técnicas cada vez, más creativas y eficaces, lo que vuelve una labor prácti-

camente imposible el estar protegidos frente a las distintas ofensivas. Dicho en otras palabras: las amenazas seguirán evolucionando.

Los delincuentes tienen a su favor lo siguiente: 1) el anonimato, 2) como es difícil ubicarlos, los delitos que cometen representan una actividad de bajo riesgo para ellos y, 3) las ganancias que obtienen son altamente rentables, ya sea en términos monetarios o en ámbitos que impliquen asuntos geopolíticos. Como ejemplo está Corea del Norte, que tiene un ejército de "hackers" en su país para realizar campañas de ataques con distintos fines, ya sea el robo de dinero para fondear necesidades del gobierno (armamento), o lograr acceso a información que le provea de inteligencia a su gobierno (ciberespionaje).

Se estima que el valor de la industria del cibercrimen es de más de 700 billones de dólares, pero hay quien dice que su valor está por arriba de 1 trillón de dólares. ¿Qué podemos hacer ante esta situación? ¿Cómo podemos estar mejor preparados para contrarrestar los impactos de este tipo de crimen? Platicamos con Santiago Gutiérrez, socio líder de la práctica de Riesgo Cibernético en Deloitte México y Centroamérica, sobre las afectaciones del cibercrimen en las organizaciones, sin distinguir industria, sector o tamaño.

AN / Santiago, esta es una pregunta obligada: ¿cómo ha afectado el cibercrimen la seguridad de los sistemas y de la información empresarial con la pandemia?

Al acelerarse la transformación digital creció el mercado para los cibercriminales. Muchas organizaciones enviaron a sus empleados a sus casas, sin estar preparadas, la mayoría, en materia de ciberseguridad. Algunas empresas se vieron obligadas a invertir en ciberseguridad y otras aceleraron lo que ya habían venido trabajando en años previos. No es un tema elitista: los ciberdelincuentes atacan a empresas o entidades que pueden tener desde cinco empleados hasta miles de colaboradores, y no solo a financieras, sino a todo tipo de industria, llegando incluso a negocios dedicados al campo.

Antes, en la industria de manufactura, las plantas de producción no estaban tanto en el radar de los ciberdelincuentes, pero ahora es una tendencia en crecimiento en todas las regiones del planeta. Su objetivo es "afectar para monetizar", en este caso, afectando los procesos críticos o líneas de producción de una fábrica. Un ejemplo de monetización podría ser el caso de una armadora de vehículos, a la cual podrían dirigir un ataque para conseguir los planes de diseño de un nuevo modelo de automóvil. Muy probablemente esa información llegaría a ser monetizada. Recordemos que los ciberdelincuentes no solo van por el dinero, sino por todo aquello que hace a una empresa distinta de otra; eso tiene un valor.

Los cibercriminales han hecho de esto su trabajo de tiempo completo; son profesionales. Hay que hacer notar que no es un mundo de hombres; las mujeres también forman parte de estos grupos del cibercrimen.

AN / ¿Qué tanto se ha incrementado la delincuencia cibernética desde que empezó la pandemia?

Diferentes fuentes de expertos varían; algunos dicen que 30% y otros que 50%. Lo importante no es el porcentaje en sí, sino que ha crecido ampliamente. Hay empresas que pudieron y que no dejaron de invertir para seguir protegiendo sus negocios. Otras han tenido que vivir con una mayor exposición al riesgo.

Para dar una cifra únicamente como referencia, la demanda de las organizaciones por nuestros servicios creció cerca de 35% en 2021, respecto a 2020. Este último año también tuvo un crecimiento cercano al 23%. Muchos clientes me decían: "Entiendo que aunque mi negocio se ha visto afectado en ingresos, tengo que seguir protegiéndome porque los ataques van a continuar e incluso podrían ser más agresivos".

AN / ¿Cómo se puede saber si los protocolos de seguridad de una organización son los adecuados?

Creo que muchas empresas ya entendieron el problema o lo han sufrido en carne propia. Ya hay mayor conciencia en las mesas directivas de los negocios y en los órganos de control. Antes existía el pensamiento de que nunca les iba a suceder un ciberataque o que no eran blanco de los cibercriminales; o que lo que ya habían construido en capacidades de ciberseguridad los tenía bien protegidos, por no decir blindados. Ojo: el blindaje puede existir, pero no la inmunidad. Sin embargo, lo sucedido en 2018 –si recordamos el ataque al Sistema de Pagos Electrónicos Interbancarios (SPEI) del Banco de México–, de alguna manera sirvió para romper el mito de que las organizaciones pueden ser inmunes.

Desde entonces, las empresas han puesto mayor énfasis en el desarrollo de otras capacidades que no habían atendido, como la respuesta a incidentes, mediante la cual uno da por sentado que será víctima en algún momento y por ello deberá contar con protocolos bien establecidos para reaccionar y limitar el daño que se enfrente. Esto sin dejar de lado la instrumentación de medidas de control, las cuales siguen siendo necesarias, pero no suficientes. Llevar a cabo ejercicios de ciber-simulación periódicos puede ayudar a identificar si los protocolos de una organización son los adecuados o no.

AN / ¿Hay una conciencia generalizada en cuanto a este tema?

Desafortunadamente, no. Me atrevería a decir que en una escala del uno al cinco (de menor a mayor conciencia), a nivel global podríamos estar cercanos a un nivel dos de conciencia sobre este tema, en promedio. También es cierto

Los costos globales del cibercrimen crecerán 15% anualmente, durante los próximos cinco años, alcanzando los 10.5 billones de dólares anuales para 2025.

El mercado carece de talento especializado en ciberseguridad a nivel local, regional y global. La demanda no cubierta es cercana a los 4 millones de profesionistas.

que la industria de la ciberseguridad es una de las industrias de mayores tasas de crecimiento actualmente, pero aun así se puede considerar como una industria joven o inmadura. Todavía hay mucho camino por recorrer. Todos hemos aprendido con base a las incidencias que han tenido las empresas. Cada vez ocurren más casos diarios en todo el mundo y en todos los sectores, y también hay miles de afectaciones a usuarios individuales.

Para mí, existen cuatro tipos de empresas en cuanto a ciberseguridad: las que ya fueron víctimas de un delito, las que podrán sufrirlo en el tiempo, las que han sido atacadas más de una vez y las que ya fueron comprometidas, pero no se han dado cuenta; es decir, que los cibercriminales han logrado penetrar a la red de una organización y pueden pasar meses conociéndola en su operación para definir su objetivo y consumar el ataque.

AN / ¿Cómo pueden protegerse las empresas de las amenazas?

Lo primero es hacer un diagnóstico para saber su situación en términos de ciberseguridad, entender cuáles son las amenazas para su negocio e industria, e identificar sus "joyas de la corona" (los activos que causarían un gran problema si llegasen a ser comprometidos). No se puede proteger todo y no se debe proteger todo de la misma manera. No hay presupuestos infinitos.

Como resultado del diagnóstico, hay que diseñar un programa permanente de ciberseguridad e implementar las distintas iniciativas que lo conformen, ya sean de gobierno, de implementación de controles tecnológicos y no tecnológicos, de acceso a visibilidad (monitoreo) y de respuesta.

AN / ¿Qué papel juega la capacitación?

Sin importar el tamaño de la organización o si es pública o privada, todos los colaboradores deben recibir un programa de capacitación, no un curso. Este programa debe ser permanente, durante todo el año, e incluir pruebas o exámenes para cerciorarse de que los colaboradores están comprendiendo.

En caso de ser posible, debe hacerse el esfuerzo por llevar esta capacitación a personal externo, como clientes y proveedores. Ocuparse de la ciberseguridad de terceros es una tendencia que observamos cada vez más, porque los ataques pueden ocurrir a través de terceros. A inicios de enero, se divulgó la noticia del caso de un hospital reconocido, cuyo sistema hospitalario fue comprometido a través de uno de sus proveedores de servicios médicos que tenía acceso a la red del hospital para prestar sus servicios.

AN / ¿Qué prácticas comunes recomiendas para todos los sectores?

La recomendación de prácticas, indistintamente del sector, depende más del nivel de madurez de seguridad que tiene la organización. Para las que han avanzado poco o apenas inician, la recomendación sería que, primero, identifiquen las amenazas y las joyas de la corona, y después definan el apetito de riesgo de la organización. Con base en ello, deben identificar las brechas existentes entre la situación actual y la deseada, respecto a los riesgos de seguridad que se identifiquen. Luego podrán definir un programa de dos o tres años, que atienda distintas iniciativas, las cuales estarán enfocadas en mitigar los riesgos de que alguna amenaza se pueda materializar. Esto parece fácil, pero requiere de un compendio importante de personal, servicios y tecnologías específicas.

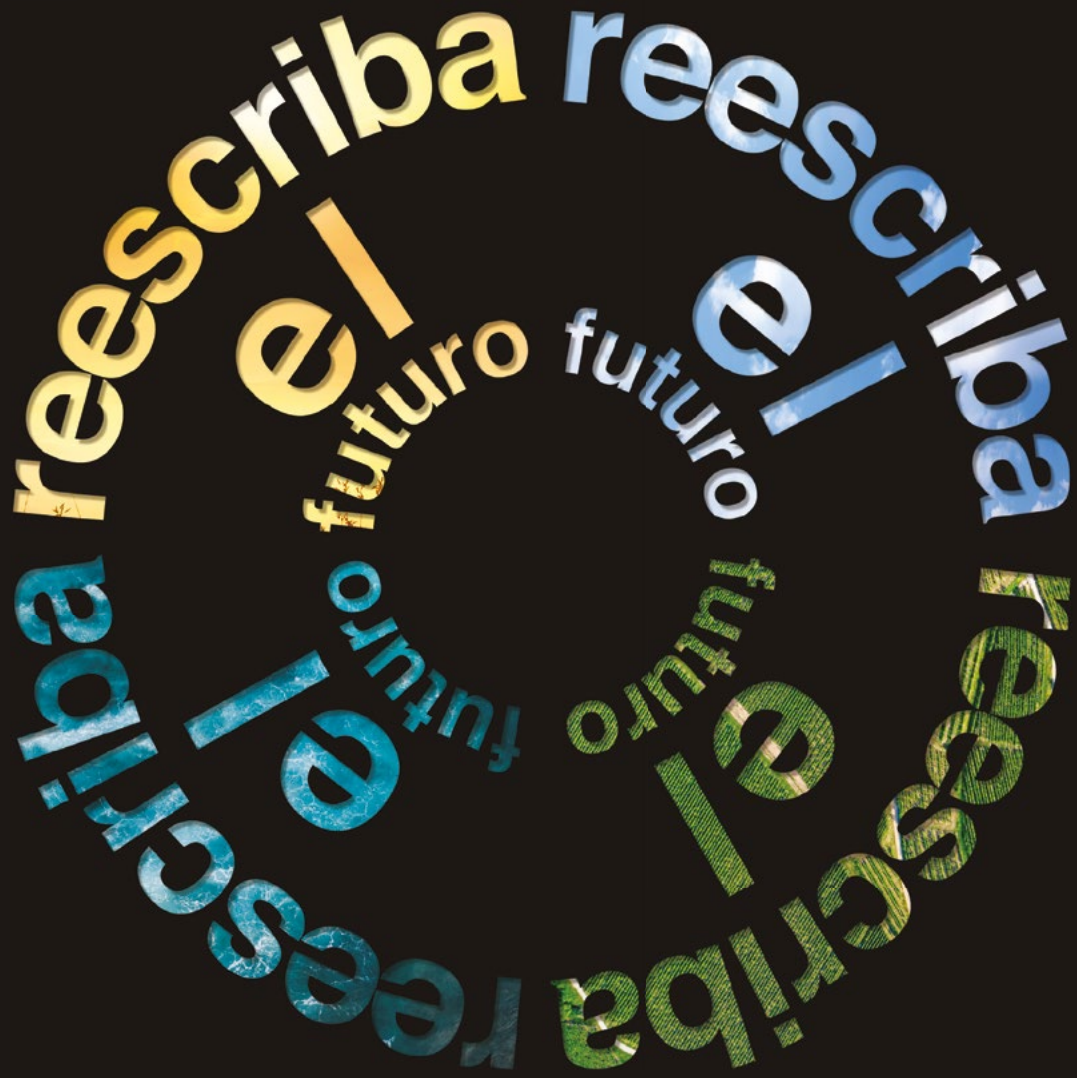
Por otro lado, en organizaciones con mayores niveles de madurez, otras prácticas que empiezan a volverse comunes son la realización de ejercicios de cibersimulación o *war gaming*, así como ejercicios ofensivos, conocidos como *red teaming*, para probar los distintos controles o capacidades de detección y respuesta de la organización.

AN / ¿Cuál es el mayor reto en el tema de ciberseguridad, actualmente?

Sin duda, la escasez de talento. El mercado carece de talento especializado en ciberseguridad a nivel local, regional y global. Una de las cosas que más nos afecta como industria es que no hay suficientes profesionistas especializados en ciberseguridad. Hace 10 años debimos haber empezado a formar de manera seria ese talento. Las vacantes o demanda no cubierta es cercana a los 4 millones de profesionistas en el mundo. Esto ha generado que se incremente la rotación de personal y se encarezca el talento.

Nosotros creamos una academia especializada en ciberseguridad para desarrollar talento. Entrevistamos a más de 800 jóvenes, hombres y mujeres, provenientes de muchas universidades de México y Latinoamérica. De ese universo seleccionamos a 110 personas, quienes entraron a estudiar con nosotros y se acaban de graduar hace unos meses; ahora forman parte de las filas de nuestra práctica regional. No hay otra manera de hacerte de talento que formándolo. AN

Clima
Acuerdo
Análisis
Acción
Cambio



Se agota el tiempo para actuar contra el cambio climático.
¿Qué puede hacer hoy para cambiar su visión del mañana?
Conéctese a nuestras mejores ideas sobre la sostenibilidad

Deloitte.