amcham CL

IdD
INSTITUTO de DIRECTORES
CHILE

Directorios:

Las claves de una estrategia saludable en Ciberseguridad

Encuentro **AMCHAM & IdDC**

Encuentro **AMCHAM / IdDC**

Introducción

Por qué ahora es el mejor momento para re imaginar, desde el Directorio, la estrategia en ciberseguridad

La tecnología avanza a un ritmo vertiginoso. La velocidad con la que se introducen nuevos cambios en el área convierte a la ciberseguridad en un tema difícil de abordar, dado que muchas de las consideraciones que se toman en esta materia pronto quedan desactualizadas. Se crea un nuevo gadget o una nueva aplicación y lo que se creía que servía para proteger los datos de las personas, de pronto ya no lo hace.

Según las estadísticas de la Subsecretaría de Telecomunicaciones (SUBTEL), a septiembre

de 2020 existían en Chile 54 millones de servicios de telecomunicaciones, lo que se traduce en 2,8 teléfonos móviles per cápita. Es decir, en nuestro país hay más celulares que personas. Esto evidencia aún más la necesidad de re imaginar la estrategia en ciberseguridad, teniendo en cuenta que gran parte de la población ha traspasado datos personales sensibles a estos aparatos y que son susceptibles de ser robados o hackeados.

En ese sentido, en el balance anual de cibercrimen de la PDI señala que entre 2020 y 2021 se registraron alzas entre el 30% y el 45% en delitos de cibercrimen en Chile. Algo que, de acuerdo con las autoridades, estaría estrechamente relacionado a los cambios de comportamiento que la sociedad adoptó durante la pandemia.

"Se generó un cambio en todas las actividades de las personas, que pasaron de ser presenciales a remotas. Esto produjo un aumento en las transacciones por medios digitales, en el teletrabajo, actividades académicas, uso de plataformas de streaming y de redes sociales para comunicarse, así como de juegos en línea", explica el subprefecto Luis Orellana, Jefe de la Bricib Metropolitana.

Marcelo Wong, Jefe de Ciberseguridad de la PDI, afirma:

"Si se suma a la pandemia de Covid, hay una nueva oportunidad de generar ataques. A su vez, las organizaciones que no se supieron transformar por la pandemia se han ido quedando en el camino, entre ellas varias empresas de tamaño no menor".

Introducción

Tal como señala Wong, la revolución digital que provocó la pandemia no solo dejó expuestos los datos de las personas, sino también los de las organizaciones. Muchas de ellas debieron embarcarse en una verdadera revolución digital para poder hacer frente a las exigencias de la pandemia, pero al hacerlo podrían haber creado potenciales vulnerabilidades que deben ser atendidas.

Según la encuesta global de seguridad de la información 2021 (GISS) realizado por EY, aproximadamente tres de cada cuatro (73%) empresas de Asia-Pacífico destacaron que vieron un aumento en la cantidad de ataques disruptivos durante el año pasado, en comparación con solo el 47% en el anterior.

Bajo este panorama, ¿qué medidas pueden tomar las organizaciones para minimizar el riesgo de sufrir ciberataques, mientras continúan el camino de la digitalización?

Encuentro **AMCHAM & IdDC**

Encuentro **AMCHAM / IdDC**

Qué piensan los Directores en Chile en materia de Ciberseguridad

Para abordar esta problemática la Cámara Chilena Norteamericana de Comercio, AmCham Chile, a través del Comité de Inteligencia Artificial y Data, y en conjunto con el Instituto de Directores de Chile (IdDC), realizó el ciclo "Ciberseguridad para Directorios: Oportunidades y Amenazas desde una Mirada Estratégica".

En el encuentro, se realizó una encuesta cuyos resultados muestran que un 82% de los directores cree que la ciberseguridad debiera estar al centro de la agenda de los directorios. También, el 100% de los consultados piensa que es necesario que los directores profundicen sus conocimientos en ciberseguridad.

Encuentro **AMCHAM / IdDC**

Qué piensan los Directores en
Chile en materia de Ciberseguridad

Resultados de encuesta hecha en ciclo **Ciber Directores** de AMCHAM e IdDC.

82%

Un **82%** de los directores cree que **la ciberseguridad debiera estar al centro de la agenda de los directorios**

100%

El **100%** de ellos cree que **es necesario que los directores profundicen sus conocimientos en ciberseguridad.**

Encuentro **AMCHAM / IdDC**

Qué piensan los Directores en
Chile en materia de Ciberseguridad

¿Cuál diría que es el desafío más grande para los directorios en materia de ciberseguridad?

Que los propios directores sean cuidadosos con la información compleja.

Brecha competencias digitales y generacional.

Inversión y capacitación.

Tener un proceso de gestión de riesgos de manera que cumpla con los niveles definidos.

Tomarse el tema en serio y aplicar lo necesario para protegerse, como persona y como organización.

Entender la triada en su completitud. Esto es compliance, protección de datos y ciberseguridad cómo un esquema de protección.

Entender el nivel de riesgo y evaluar los planes de mitigacion apropiadamente.

Asumir que es una realizada, un riesgo que Manejar.

Subir el tema en la escala de riesgos a controlar y minitorar.

Trazabilidad en la seguridad.

Tomar conciencia de la importancia que se le debe dar al tema y hacerla parte de los riesgos de la compañia.

Entender el nivel de inversión necesaria que sea suficiente para dar cumplimiento. Claramente cada industria es diferente. Realmente no existe un benchmark.

Encuentro **AMCHAM / IdDC**

Qué piensan los Directores en Chile en materia de Ciberseguridad

Comprobar fehacientemente lo que he ta en CTO sobre las protecciones instaladas y vigentes.

Definir qué prioridad y qué presupuesto asignar al fortalecimiento de la agenda digital y por ende también, la ciberseguridad.

Dualidad entre acceso directo a información de la compañía versus información cifrada y censurada por departamento de seguridad de la compañía (lo que tema bien conlleva sus problemas).

Que esté incorporado a la cultura de la organización y en este riesgo instalaremos que cada persona es la la línea de defensa.

Tomar conciencia e incorporar en la Matriz de riesgo de la compañía buena prácticas en el cuidado de la información, tanto en las personas, como los sistemas utilizados.

Tomar conciencia en la administración de este riesgo y generar capacitación al respecto.

Tomar conciencia e incorporar en la matriz de riesgo de la compañía, buenas prácticas en el cuidado de la información, tanto en las personas como los sistemas utilizados.

Incorporarlo cono materia relevante donde hay que invertir en herramientas, cultura y Educacion.

Lograr motivar a reconocer la importancia de la ciberseguridad como tema relevante a incorporar en D para invertir en ello.

Brechas generacionales y de conocimiento.

Incluir ciberseguridad en los riesgos y así en nuestros comités y sesiones de Directorio.

Entender realmente dónde estamos y qué se necesita hacer.

Cerrar las brechas de talento

Dada la naturaleza sofisticada de los ciberataques actuales, las organizaciones necesitan profesionales expertos en ciberseguridad y con habilidades técnicas avanzadas. Al mismo tiempo, se requiere que la ciberseguridad amplíe su gama de habilidades blandas y calificaciones profesionales para facilitar la construcción de relaciones interdepartamentales.

Adoptar una política de financiamiento

A pesar de la creciente amenaza de los ciberataques, el gasto en ciberseguridad de las empresas de Asia-Pacífico sigue siendo bajo: solo el 0,05% de sus ingresos anuales, información que dio a conocer la Encuesta de Seguridad de la Información de EY (GISS).

Los Directores de Seguridad de la Información (CISO) luchan por ampliar los esfuerzos de sus funciones mientras trabajan con modelos de

presupuesto, en los cuales se les asigna una parte fija dentro de un gasto corporativo más grande de seguridad cibernética considerado para toda la organización. En ese sentido, se sugiere que las organizaciones adopten un modelo

Reimaginar el valor de la ciberseguridad

Hacer frente a estos desafíos no es solo responsabilidad del líder tecnológico, sino que requiere el compromiso y el apoyo del directorio y gerencia. GISS da a conocer que el 39% de las organizacionesglobalesincluyenlaciberseguridad en sus agendas de directorio trimestrales, frente al 29 % en 2020. Además, solo el 20% de las empresas de Asia-Pacífico incluyen la ciberseguridad en la fase de planificación de cualquier programa de transformación digital.

Encuentro **AMCHAM / IdDC**

5 Preguntas que debe hacerse el directorio en materia de ciberseguridad

¿Con qué frecuencia el Directorio discute asuntos de ciberseguridad y qué métricas utiliza para monitorear la resiliencia cibernética de la organización?

Encuentro **AMCHAM / IdDC**

5 Preguntas que debe hacerse el directorio en materia de ciberseguridad

¿Qué estructuras de gobierno tiene el Directorio para **supervisar la ciberseguridad** y están sujetas a revisiones regulares de efectividad?

Encuentro **AMCHAM / IdDC**

5 Preguntas que debe hacerse el directorio en materia de ciberseguridad

¿Cómo puede la organización invertir más estratégicamente en ciberseguridad **para abordar el creciente riesgo de filtraciones de datos?**

Encuentro **AMCHAM / IdDC**

5 Preguntas que debe hacerse el directorio en materia de ciberseguridad

¿De qué manera la organización **está diseñando la ciberseguridad en sus datos**, procesos y sistemas?

Encuentro **AMCHAM / IdDC**

5 Preguntas que debe hacerse el directorio en materia de ciberseguridad

¿El Directorio tiene una mirada sistémica de la ciberseguridad que incluye a sus proveedores, partners y clientes? Es decir, **¿es conciente de los accesos, integraciones y protocolos establecidos con ellos?**

Encuentro **AMCHAM / IdDC**

10 Acciones a implementar en materia de ciberseguridad

Iteración de la estrategia en seguridad. Según los expertos, no existe una sola receta para evitar ciberataques. Lo que sí pueden hacer las organizaciones es integrar a su estrategia de ciberseguridad el autocuidado y compartir recomendaciones. De esta forma, una mayor capacitación del equipo de la organización redundará en una mayor destreza, conocimiento y capacidad de reacción.

A continuación, algunas acciones a implementar en materia de ciberseguridad:

1. Integrar la ciberseguridad en la estrategia de talento.

2. Definir claramente las responsabilidades de ciberseguridad en su organización.

3. Establecer protocolos de ciberseguridad y confirmar de manera regular su cumplimiento.

4. Asegurar que la ciberseguridad esté en el corazón de la innovación digital de la empresa.

5. Comprender cómo la regulación afecta su negocio global y trabajar con los reguladores.

Encuentro **AMCHAM / IdDC**

10 Acciones a implementar en materia de ciberseguridad

6. Evaluar el riesgo de todos los activos clave y determinar un enfoque de protección para cada uno, con prioridad en los más críticos.

7. Desarrollar un modelo dinámico y ágil de gestión de riesgo de ciberseguridad para permitir a la organización crecer de manera ordenada.

8. Integrar el *compliance* en su estrategia de ciberseguridad, de modo que cualquier dinero invertido devuelva valor al negocio proporcionando una defensa adecuada para la organización.

9. Fortalecer la resiliencia teniendo un área de gestión de crisis y comunicaciones que pueda ser implementada y practicada en todos los niveles de la organización.

10. Colaborar con sus pares para buscar más soluciones fuera de su organizacióon, incluso en otras industrias.

Encuentro **AMCHAM / IdDC**

Acciones en ciberseguridad que los directores destacan de las organizaciones a la que pertenecen

¿Qué acciones destaca en su Directorio/Organización en materia de ciberseguridad?

La visión de conjunto en cuanto a no ver el tema de la ciberseguridad como un tema externo.

Políticas permanentes de acciones seguras y accesos de doble factor.

Capacitación sobre el tema a toda la organización.

Intercambio de experiencias con ejemplos.

Se han generado capacitaciones en ciberseguridad para tomar "conciencia" de los riesgos en estos temas.

Incorporar en la matriz de riesgo y mantenerla actualizada en este tipo de riesgos.

Actualización de procedimientos y políticas asociadas al cuidado de la información.

Ethical hacking es algo mandatorio (y barato) Benchmarks de configuración es en la nube.

Uso de matriz de riesgo.

Capacitaciones, utilización de alarmas en diferentes instancias (advertencias).

Encuentro **AMCHAM / IdDC**

Acciones en ciberseguridad que los directores destacan de las organizaciones a la que pertenecen

Presentación y recomendaciones de expertos al directorio.

Mailings recurrentes a los usuarios con información y recomendaciones.

Monitoreo constante con informe de resultados por usuarios.

Asignación de presupuesto a seguridad.

Crear cultura organizacional respecto a ciberseguridad.

Desarrollo de capacitación y entrenamiento de sensibilización, explicando conceptos básicos.

Testing de ingeniería social con castigo disciplinario a los infractores con su jefe presente.

Tener una gerencia encargada.

Establecerlo bajo un modelo de riesgo con 3 líneas de defensa, identificar el plan de cultura, los recursos y organización.

Permisos de acceso a la base de documentos según responsabilidades. Es decir muy pocos tienen acceso a la documentación secreta, uno más a la reservada y todos a la pública. Los permisos de acceso con claves doble factor.

"La ciberseguridad debe estar al centro de la agenda del directorio. Hoy, parte de los deberes de los directores es el *compliance*, mientras que la transformación digital se ha ido instalando cada vez más en las operaciones de las compañías. Hoy por hoy, los hackers ha visto una oportunidad no sólo de generar acciones indebidas, sino que fraudes con los que van entrenando softwares que son sumamente dañinos para las organizaciones. Es fundamental que estemos preparados, pues lo directores también respondemos por la seguridad y confidencialidad de los datos de nuestros clientes. Hoy es un deber, no una opción"

Cristián Retamal, director ejecutivo de Eurocorp

"Creo que es muy necesario que los directores profundicen su conocimiento en ciberseguridad, y no sólo hoy por las amenazas que vemos día a día, sino que es una tarea constante del directorio y que sin duda debe estar dentro de las matrices de riesgo corporativas. Es por ello que es responsabilidad del directorio conocer e interiorizarse en esta materia"

Juan Carlos Montjoy, Gerente Corporativo de Tecnología y soluciones digitales

"Los directores deben profundizar su conocimiento en ciberseguridad, quizá no en el detalle, pero este tema, por estar en la matriz de riesgo de una organización, debe ser parte de la agenda del directorio, apoyándose en la contratación de expertos en la materia que guíen este aprendizaje"

Manola Ramírez, directora de Vicsa, Ferrostaal y Red Inmobiliara S.A.

"El primer desafío en ciberseguridad para directores es educarnos. Debemos hacerlo profundamente en una temática muy reciente y que probablemente en América Latina no tiene más de 5 años. Para ello, es necesario participar de actividades donde referentes en la materia expongan la tendencia, los desafíos y puntos a tener en cuenta, para poder tener una opinión valiosa para compartir con las organizaciones de las que somos parte"

Pablo Riccheri, CEO de Cambridge Bussiness Association

"Los temas de ciberseguridad evolucionan tan rápido, que los directores debemos invertir constantemente en tiempo para capacitarnos. Debemos ser capaces de bajar las amenazas a un nivel cultural para evitar comportamientos que pueden ser dañinos o potencialmente peligros"

Claudio Robino, director ejecutivo de Inmunocenter

"El desafío más grande en ciberseguridad para los directorios es instalar el tema como una materia más y relevante, donde hay que hacer control y seguimiento, hay que educar y generar una cultura dentro de la organización. Uno puede invertir en distintas metodologías y tecnologías, pero si no invertimos en las personas, es muy difícil avanzar, pues las organizaciones están compuestas de personas, y somos nosotros los que cometemos los errores"

Patricia Norambuena, directora independiente

IdD
INSTITUTO de DIRECTORES
CHILE

amcham CL