Deloitte.
University Press

El riesgo cibernético en los negocios de consumo♦

♦ Documento original: "**Cyber risk in consumer business. Consumer businesses discuss the six main cyber risk challenges they face today**", Deloitte University Press, June 15, 2017. Written by Sean Peasley, Kiran Mantha, Vikram Rao, Curt Fedder, Marcello Gasdia. Cover image by Sam Falconer. https://dupress.deloitte.com/dup-us-en/industry/retail-distribution/cyber-risk-management-in-consumer-business.html?id=us:2sm:3tw:4dup3810:5awa:6DUPress:20170702::du_press&linkId=39183829.
Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.

Deloitte ofrece un completo portafolio de servicios para ayudar a que organizaciones complejas establezcan su apetito por el riesgo cibernético, diseñen e implemente programas Seguros. Vigilantes. Con capacidad de recuperación, y ayudar en la administración, mantenimiento, y adaptación continuos de sus programas en la medida en que el negocio y los entornos de amenaza cambien. Contacte a los autores para más información, o lea más acerca de nuestros servicios relacionados con el riesgo cibernético, en https://www2.deloitte.com/us/en/pages/risk/solutions/cyber-risk-services.html.

IMAGEN DE LA PORTADA POR SAM FALCONER

CONTENIDOS

Entender al riesgo cibernético en los negocios de consumo

LAS TECNOLOGÍAS INNOVADORAS están ayudando a incentivar un aumento sin precedentes en las expectativas del consumidor. Para los negocios hoy, aprovechar las tecnologías emergentes en orden a re-definir productos, servicios, y experiencias del consumidos es a menudo el nuevo costo de hacer negocios. La inversión en tecnología, sin embargo, puede orientar más que el solo potencial de utilidades. Las iniciativas amplias alrededor de analíticas del cliente, integración en la nube, dispositivos conectados, y tecnología digital para el pago es probable que dejen a los negocios crecientemente expuestos ante las amenazas cibernéticas.

Algunas amenazas, tal como el fraude de tarjeta de crédito y robo de identidad, se están volviendo muy familiares en el mercado del presente y pueden ser significativamente perjudiciales para la confianza del cliente y la reputación de la marca. Otros riesgos, tales como los relacionados con seguridad alimentaria y robo de propiedad intelectual, parece que se están escalando, llevando a muchos negocios (y a sus clientes) a territorio no familiar.

Los negocios que tienen contacto directo con los clientes, tales como minoristas, restaurantes, y compañías de productos de consumo, deben considerar tomar las precauciones adecuadas para mitigar al riesgo cibernético durante este período de transformación digital. Su creciente huella de tecnología, junto con la aceleración del ritmo del cambio en los negocios, puede tener un impacto dramático en la profundidad y complejidad de los riesgos cibernéticos que los negocios de consumo probablemente necesitarán abordar en la próxima década.

Elaborando a partir de nuestra anterior investigación sobre la seguridad cibernética en la fabricación,[1] Deloitte lanzó el Cyber Risk in Consumer Business Study [Estudio sobre el riesgo cibernético en los negocios de consumo] para valorar los desafíos actuales enfrentados por las compañías en los sectores de productos de consumo, minorista, restaurantes, y agroindustrias. Usando una combinación de una encuesta en línea y entrevistas en profundidad, obtuvimos las opiniones de más de 400 directores de información jefes [chief information officers (CIOs)], directores de seguridad de la información jefes [chief information security officers (CISOs)], directores de tecnología jefes [chief technology officers (CTOs)], y otros ejecutivos principales en esos sectores.

Los resultados de este estudio están diseñados para ayudar a que los negocios de consumo comprometan a sus equipos de liderazgo senior y a sus juntas en conversaciones más profundas cobre cómo hacer que sus negocios sean más seguros, vigilantes, y con capacidad de recuperación. Aplicar las lecciones aprendidas a partir de este estudio puede ayudarles a los negocios a:

Estar seguros: Tomar un enfoque mesurado, basado-en-el-riesgo, para lo que es asegurado y cómo asegurarlo. Esto incluye administrar los riesgos cibernéticos como un equipo e incrementar la preparación mediante elaborar estrategias de administración del riesgo cibernético en la empresa y las tecnologías emergentes cuando sean desplegadas.

Estar vigilantes: Sistemas de monitoreo, aplicaciones, personas, y el entorno para detectar más efectivamente los incidentes. Esto incluye desarrollar conciencia situacional e inteligencia ante la amenaza para entender el comportamiento dañino y los riesgos principales para la organización, y monitorear activamente el panorama dinámico de la amenaza.

Tener capacidad de recuperación: Estar preparados para los incidentes y disminuir el impacto en sus negocios mediante mejorar la preparación organizacional para abordar los incidentes cibernéticos antes que ellos se escalen. Esto también incluye capturar las lecciones aprendidas, mejorar los controles de seguridad, y regresar al negocio tal y como es usual tan rápidamente como sea posible.

Seis áreas de atención para las compañías de negocios de consumo

MUCHOS negocios están aprovechando las tecnologías innovadoras para mejorar la experiencia del cliente, construir lealtad, y, quizás, lo más importante, permanecer competitivos en un mundo digital. Sin embargo, las compañías deben considerar balancear su ampliación de las huellas digitales con una creciente atención puesta en el riesgo cibernético. Las tecnologías emergentes a menudo son atractivas avenidas de oportunidad para los criminales que buscan exponer las debilidades en el ecosistema digital de la organización.

El camino adelante probablemente no será fácil. Los negocios de consumo enfrentan numerosos desafíos cuando intentan manejar los problemas complejos del riesgo cibernético. Como tal, nosotros hemos identificado los siguientes seis temas que las compañías deben considerar:

- **Compromiso a nivel ejecutivo**: Para muchas organizaciones, la responsabilidad por prevenir, administrar, y recuperarse de los incidentes cibernéticos tiende a ser altamente fragmentada. Los negocios de consumo deben considerar ganar un mejor entendimiento del panorama del riesgo cibernético en orden a establecer una estructura más efectiva para este problema crítico a través de sus organizaciones. También hay una oportunidad importante para lograr un balance más efectivo entre invertir en las tecnologías avanzadas correctas para avanzar al negocio al tiempo que se asegura que al hacerlo, no se están abriendo ante riesgo cibernético incrementado.

- **Confianza del cliente**: Los negocios de hoy pueden estar patinando en el hielo cuando se trata de las potenciales reacciones del consumidor ante las violaciones cibernéticas. La investigación longitudinal a través de miles de consumidores de los Estados Unidos revela un aumentado estado de incertidumbre alrededor de la seguridad de los datos en la década pasada. Los negocios no solo deben considerar cómo las percepciones de la incertidumbre acerca de la privacidad de la información personal puedan impactar las futuras decisiones de compra sino también asegurar a sus clientes que están dando los pasos apropiados para mitigar el riesgo cibernético.

Nuestra investigación previa, *Cyber risk in advanced manufacturing*, identificó seis desafíos clave del riesgo cibernético que enfrenta la industria avanzada de fabricación. muchos de esos temas, incluyendo **compromiso a nivel ejecutivo, talento y capital humano, propiedad intelectual,** y **productos conectados,** se encontró que son áreas fuertes de atención y preocupación entre los negocios de consumo. Sin embargo, los negocios de consumo también enfrentan dos áreas únicas de riesgos cibernéticos, **confianza del consumidor** y **pagos**, las cuales pueden ser críticas para su panorama en evolución de la seguridad cibernética.

Nosotros consideramos que esos temas son críticos para la capacidad de los negocios orientados-al-consumidor para capturar y proteger el valor asociado con esta nueva frontera de tecnología, al tiempo que de la manera apropiada abordan en el largo plazo los riesgos cibernéticos dinámicos.

- **Productos conectados**: El éxito futuro de los productos conectados probablemente depende no solo de la tecnología que facilite la conectividad sino también de la confianza del consumidor, la cual puede orientar la demanda. El rápido crecimiento de los productos conectados no solo ofrece numerosos beneficios potenciales para los negocios de consumo y sus clientes, sino que también puede incrementar el riesgo cibernético. Es esencial que los negocios de consumo garanticen la seguridad de los productos conectados si tanto los negocios como los consumidores quieren cosechar sus beneficios.

- **Pagos**: Las tecnologías emergentes de pago están facilitando que los negocios eleven la experiencia del consumidor mediante racionalizar y, en muchos casos, reinventar los procesos de pago. Las compañías que sean capaces de aprovechar las tecnologías emergentes de pago al tiempo que mantienen la atención en la seguridad de esas plataformas estarán posicionadas para ganar a partir de su implementación. Tecnologías tales como los sistemas emergentes de pago que proporcionan experiencias del cliente nuevas y eficientes también están siendo objetivo de los criminales cibernéticos.

- **Propiedad intelectual**: La propiedad intelectual [Intellectual property (IP)] orienta la innovación, la competitividad, y el crecimiento de la compañía. La naturaleza en evolución y el aumento de la incidencia del robo de IP requiere un enfoque comprensivo del riesgo cibernético alrededor de la administración de la identidad y el acceso a los datos.

- **Talento y capital humano**: La capacidad de la organización para administrar efectiva y eficientemente el riesgo cibernético debe ser parte de su cultura. El talento puede ser el vínculo más débil en el panorama cibernético. En orden a mitigar este riesgo, es imperativo atraer, entrenar, y retener al principal talento cibernético al tiempo que se implementan programas educativos para todos los empleados sobre el rol que ellos juegan para minimizar el riesgo a través del panorama digital en evolución.

Compromiso a nivel ejecutivo

Dirigir el compromiso con los ejecutivos de la sala directiva para ayudar a mitigar el riesgo cibernético

El involucramiento del nivel ejecutivo con la administración del riesgo cibernético, incluyendo prevención, mitigación, y recuperación, es crítico para el éxito de los programas sobre el riesgo cibernético. Los ejecutivos de la sala directiva pueden establecer políticas y procedimientos líderes. Pero para muchas organizaciones, la administración de las iniciativas relacionadas con el riesgo cibernético tienden a estar fragmentadas debido a los crecientes vectores de amenaza que las compañías están experimentando (figura 1). Para ayudar a mitigar los potenciales incidentes del riesgo cibernético y además alinear a los *stakeholders* del negocio, los negocios de consumo, liderados por los ejecutivos de la sala directiva, deben considerar entender el panorama del riesgo cibernético y definir la propiedad organizacional. Los negocios de consumo se podrían beneficiar de que sus ejecutivos de la sala directiva asuman un rol más proactivo en relación con los problemas del riesgo cibernético que sus compañías enfrentan y de la brecha actual entre percepción y realidad en términos de la preparación cibernética de su organización. También puede ser una oportunidad importante para lograr un balance más efectivo entre inversión en las tecnologías avanzadas correctas para hacer que sus negocios avancen, al tiempo que aseguran que, al hacerlo, están administrando de manera efectiva cualesquiera riesgos nuevos que puedan salir a su paso.

Figura 1: Principales iniciativas de seguridad cibernética (porcentaje de negocios que orientan cada iniciativa)

Nota: Tamaños de muestra: n(general)=402, n(productos de consumo)=150, n(restaurantes)=100, n(minoristas)=100
Fuente: Análisis de Deloitte

El 82 por ciento de los negocios de consumo no ha documentado y probado los planes de respuesta cibernética que involucraron a los stakeholders del negocio en el último año.

El 29 por ciento de los negocios carece de claridad sobre los roles y responsabilidades de los individuos durante una violación cibernética actual.

Algunos negocios de consumo pueden estar operando con un falso sentido de confianza acerca del riesgo cibernético

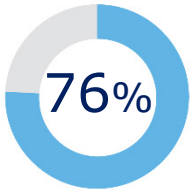
Cerca de tres cuartos de los ejecutivos entrevistados reporta que está altamente confiado en su capacidad para responder a un incidente cibernético, si bien simultáneamente citan muchos problemas que críticamente deterioran su capacidad para responder de manera efectiva ante los incidentes cibernéticos que podrían ser abordados mediante más involucramiento de los ejecutivos de la sala directiva y de los ejecutivos de la junta (figura 2). Esta paradoja sugiere que muchas compañías operan con un falso sentido de seguridad.

Los juegos de azar pueden ayudar a que los ejecutivos de la sala directiva mitiguen el riesgo cibernético

A los ejecutivos también se les preguntó acerca de los desafíos que enfrentan cuando responden a una violación cibernética *actual*. Sus respuestas hacen eco de lo que dijeron acerca de las preocupaciones que enfrentan cuando intentan establecer programas efectivos (figura 3).

Esos desafíos pueden ser abordados y planeados mediante **ejercicios de juegos de azar**. Los juegos de azar cibernéticos son un ejercicio interactivo que sumerge a los participantes en un incidente de riesgo cibernético simulado, seguido por una documentación de lo que hicieron y de lo que no hicieron, exponiendo por lo tanto potenciales vacíos en el protocolo de la respuesta general de la compañía del individuo. En comparaciones con las valoraciones tradicionales para la amenaza cibernética, que se centran en evaluar los controles de tecnología y la completitud de los controles de respuesta ante los incidentes, los juegos de azar cibernéticos traen a la vida la experiencia de responder a un ataque de riesgo cibernético. Algunos de los beneficios de los juegos de azar y de las simulaciones relacionadas incluyen reunir *stakeholders* dispares para probar su brío al tomar decisiones de negocio bajo presión y trabajar como un equipo centrado que despliega herramientas y técnicas específicas.[2]

Figura 2. Preparación para la seguridad cibernética



SE SIENTE ADECUADAMENTE PREPARADO PARA LOS INCIDENTES CIBERNÉTICOS, SIN EMBARGO…

82%	En los últimos 12 meses no ha documentado y probado los planes de respuesta cibernética que involucra a los *stakeholders* del negocio.
Solo el 46%	Realiza juegos de guerra y simulaciones sobre una base trimestral o semestral.
25%	Reporta carencia de financiación para lo cibernético.
21%	Carece de claridad sobre mandato, roles, y responsabilidades

Q30. ¿Qué tan preparada está su compañía para el siguiente evento cibernético de crisis?
Q26. ¿Su organización tiene un plan de respuesta ante incidentes, y ha sido probado en los últimos 12 meses?
Q37a. ¿Qué tan a menudo su organización hace seguimiento a las iniciativas relacionadas con la seguridad cibernética?
Q25. ¿Cuáles son los más importantes desafíos que su organización enfrenta para establecer/mantener un programa efectivo de seguridad cibernética?

Fuente: Análisis de Deloitte

Figura 3. Reacción ante una violación

Aspectos más desafiantes de los incidentes relacionados con el riesgo cibernético

29% Carencia de claridad sobre roles y responsabilidades

18% Carencia de acuerdo sobre cómo responder

18% Negación de que el incidente fue a nivel de crisis

11% Carencia de preparación para este tipo de crisis

Q28. ¿Cuál fue el aspecto más desafiante del incidente/crisis cibernético severo que su compañía experimentó en los últimos 12 meses?

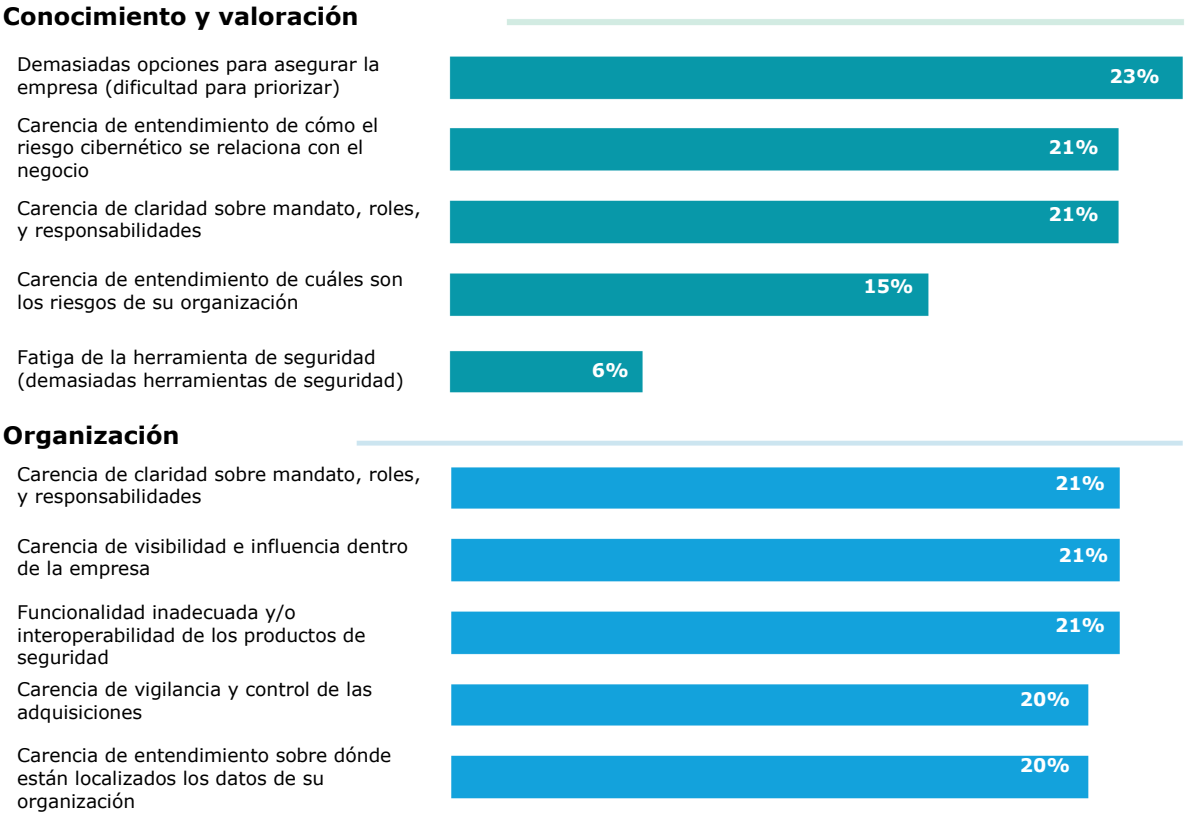
Fuente: Análisis de Deloitte

A pesar de los beneficios de los juegos de azar y otras simulaciones, solo el 46 por ciento de los negocios de consumo los realizan sobre una base trimestral o semestral. Las organizaciones que no se comprometen en simulaciones de la violación cibernética están perdiendo una oportunidad para estar mejor preparados, si experimentan un incidente cibernético.

Resolver los desafíos organizacionales a menudo es primordial para administrar de manera efectiva al riesgo cibernético

Las organizaciones enfrentan muchos problemas operacionales que comprometen su capacidad para administrar efectiva y eficientemente al riesgo cibernético. A los ejecutivos se les pidió que identificaran los desafíos más importantes que enfrentan cuando establecen y mantienen un programa efectivo de seguridad cibernética. La carencia de financiación surgió como la preocupación principal, junto con la carencia de claridad tanto sobre el mandato cibernético como también sobre los roles y responsabilidades (figura 4). Observe que esto es consistente con los desafíos que enfrentan cuando responden a una violación actual (tal y como se destaca en la figura 3 arriba), donde la carencia de claridad alrededor de los roles y responsabilidades durante una violación fue la preocupación principal. Esto sugiere que esos son problemas sistémicos en la administración del riesgo cibernético.

Figura 4. Desafíos al establecer programas efectivos relacionados con el riesgo cibernético (porcentaje de negocios que citan el desafío)



Q25. ¿Cuáles son los desafíos más importantes que su organización enfrenta para establecer/mantener un programa efectivo de seguridad cibernética?

Fuente: Análisis de Deloitte

Solo el 9 por ciento de los negocios de consumo que participaron en nuestra encuesta reportan que han tenido una violación en los últimos 12 meses. Esto es considerablemente más bajo que la tasa de incidencia reportada en el sector de fabricación (39 por ciento) y sugiere que, si bien los negocios de consumo pueden no sentir que estén ante peligro inmediato, de hecho, el nivel del riesgo de incidente probablemente permanece alto, tal y como un ejecutivo lo expresó durante una discusión en profundidad:

> Yo diría que nosotros somos bastante vulnerables. Ahora mismo, para muchos fabricantes de CPG y proveedores terceros, hay un enorme movimiento hacia la nube… el 90 por ciento de los sitios de marca ahora están ubicados en Microsoft Azure o sistemas en la nube. Cuando usted se mueve fuera del sitio, sus herramientas y procesos heredados ya no aplican o se transfieren a la nube… La manera como nosotros nos comprometemos [con los clientes] ha cambiado en los últimos años. [Nosotros somos] un bit más vulnerables que otros verticales de la industria que han estado en esto--- Nosotros lo estamos haciendo… Nosotros estamos intentando ponernos al día.

Los reportes de medios de comunicación sobre incidentes cibernéticos han ayudado a centrar la atención en la necesidad de iniciativas sobre seguridad cibernética, ayudando a los ejecutivos cibernéticos a solicitar más financiación para programas futuros. Al solicitar fondos adicionales, sin embargo, los ejecutivos de la seguridad cibernética podrían beneficiarse de asumir un enfoque comprensivo y sistemático frente al tema y ser cuidadosos en evitar la apariencia de exagerar ante incidentes específicos. Tal y como lo dijo un ejecutivo con el cual hablamos:

> Una manera para conseguir dinero en seguridad es experimentar una violación o una auditoría vergonzosa, o tener un equipo de liderazgo que entienda el riesgo junto con un equipo de seguridad que pueda transmitir las preocupaciones sobre la seguridad de una manera que resuene. Por ejemplo, "Esta es nuestra postura sobre la seguridad… nuestras brechas… y lo que debemos hacer acerca de ella… y tenemos en funcionamiento un plan para abordarla."

Ayudar a asegurar el involucramiento pleno del liderazgo en la administración del riesgo cibernético

El compromiso pleno del ejecutivo es necesario para coordinar las necesidades específicas de todos los departamentos tocados por los problemas de seguridad cibernética. A los participantes en el estudio se les preguntó acerca de la administración del día-a-día del riesgo cibernético y cuáles *stakeholders* están involucrados en el evento de una violación actual. Especialmente preocupante para los participantes fue que la administración del riesgo cibernético carece de representación del rango amplio de *stakeholders* a través de la organización.

En nuestra encuesta, aprendimos que en la administración del día-a-día del riesgo cibernético, los CIO son principalmente responsables por las funciones de la seguridad cibernética, seguidos por los CISO. Los CIO tienen estrategia, presupuesto, y le reportan a la junta (66 por ciento); medición del programa y presentación de reportes (59 por ciento); y respuesta ante incidentes (55 por ciento). Sin embargo, en el evento de una violación cibernética, solo el 76 por ciento de los negocios orientados al consumidor reportan al CEO o tienen un involucramiento equivalente. El involucramiento de otros ejecutivos de la sala directiva es aún más bajo: solo el 48 por ciento de directores financieros jefe (CFO) están presentes, y el 28 por ciento de cada uno de los directores de riesgo jefe (CRO) y directores de mercadeo jefes (CMO). De manera similar, el compromiso a nivel de la junta es bajo, de solo el 40 por ciento.

Dadas la importancia que el mercadeo tiene para los negocios orientados al consumidor, y la necesidad de ayudar a asegurar la confianza del consumidor y la reputación de la marca, que puede ser impactada durante una violación cibernética, el involucramiento de solo el 28 por ciento de los CMO parece bajo. Sin embargo, de acuerdo con los ejecutivos cibernéticos con quienes hablamos, hay un creciente involucramiento de los CMO, quienes están interesándose en proteger la información personalmente identificable [personally identifiable information (PII)] y los sitios web de la marca, en particular.

Dado que muchas compañías ahora están vendiendo directamente a los consumidores, y que el acceso a los datos de los medios sociales de comunicación se está volviendo común, los negocios de consumo están comenzando a recoger más datos de PII tales como información de tarjeta de crédito, números de teléfonos celulares, direcciones en línea y fuera de línea, y fechas de nacimiento. Por lo tanto, proteger la PII ya no es solo responsabilidad de los CIO y CTO sino también de los CMO. Tal y como lo señaló un ejecutivo cibernético que entrevistamos:

> Me reuní con el CMO la última semana acerca del PII que se está comenzando a construir en nuestro sistema en la nube. Si tenemos los cumpleaños de las personas, los correos electrónicos y las direcciones de sus casas, y si hacemos seguimiento acerca de los regalos después de un evento, [nosotros estamos abiertos ante la vulnerabilidad]. Todos los proveedores de aplicaciones de mercadeo en la nube con quienes trabajamos conocen la necesidad de estar en cumplimiento y dar aseguramientos. [Mi CMO] está muy preocupado si hay una violación de esas cosas, aún si ello ocurre inadvertidamente por [un] empleado, o [debido a una] nube insegura. De manera que aquí este es un gran tema.

Con el potencial de causar pérdida a la reputación de la marca, el *hackeo* de sitios web del producto (los cuales tienden a estar basados en la nube sin cortafuegos de la aplicación en la nube) es otra preocupación creciente entre los ejecutivos que entrevistamos. Puede haber un enorme potencial para que los hackers accedan a la información interna o difundan contenido falso. Para muchas compañías grandes de productos de consumo con múltiples productos, cada uno con un sitio web individual, este problema se agrava. Además, si es una organización global, habrá sitios específicos-del-país para el mismo producto, incrementándose exponencialmente la posibilidad de *hackeo*.

Permanecer competitivo en un mundo digital

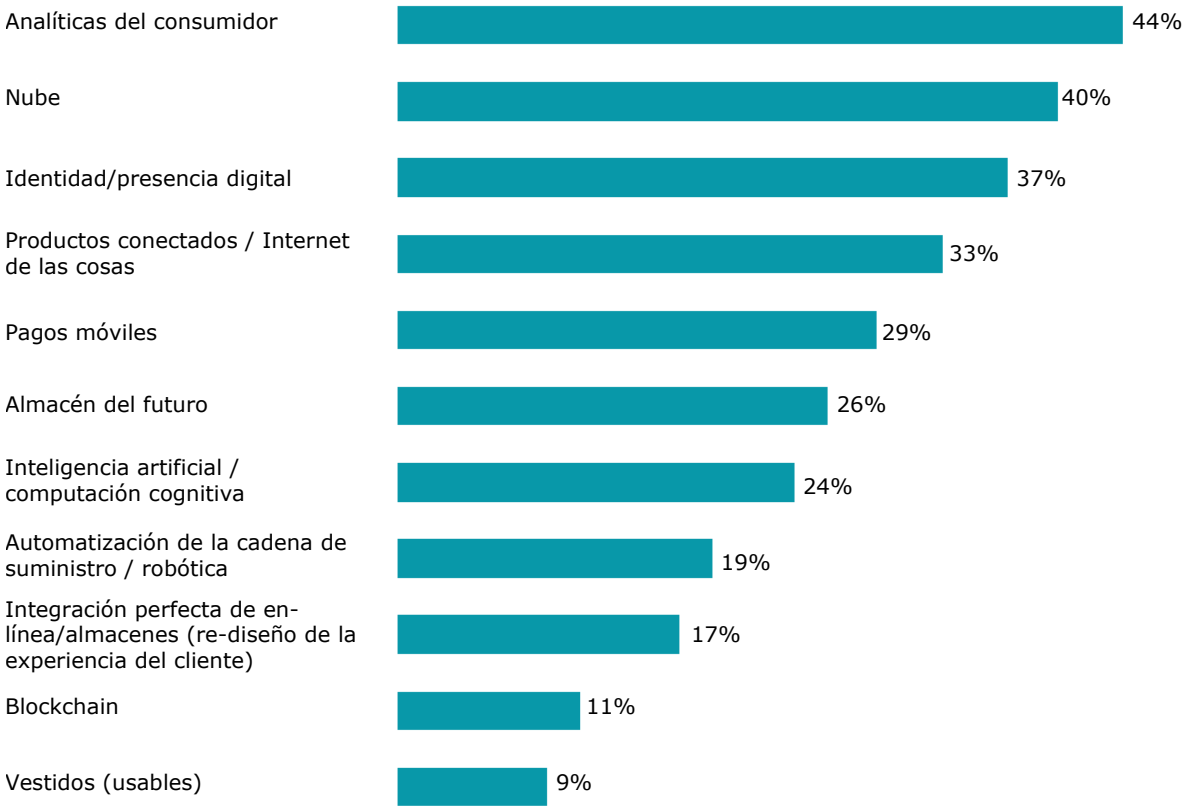
A menudo, para permanecer competitivos en el mercado de hoy y competir efectivamente en un mundo digital, muchos negocios de consumo están persiguiendo un rango amplio de iniciativas basadas-en-tecnología que pueden incrementar la oportunidad para el riesgo cibernético. Muchos ejecutivos de la sala directiva están en una posición fuerte para ayudar a asegurar que haya un balance sólido entre la adopción rápida de tecnología y la administración apropiada del riesgo cibernético.

Por ejemplo, a los ejecutivos se les solicitó que listaran sus iniciativas estrategias críticas para el liderazgo del negocio. La segunda iniciativa más alta fue la "innovación facilitada-por-tecnología para mejorar la

propuesta de valor." Además, a los ejecutivos cibernéticos se les solicitó que listaran las tecnologías en las cuales estaban invirtiendo para apoyar sus iniciativas (figura 5). Muy importante, aprendimos que para hacer de sus iniciativas estratégicas una realidad, por lo tanto, contribuyendo a las metas generales del negocio, la administración efectiva de la seguridad cibernética es probablemente crítica. Esto porque las iniciativas estratégicas trasladan las inversiones en una serie de tecnologías avanzadas tales como la nube, identidad y presencia digital, productos conectados, y pagos móviles. Sin embargo, muchos negocios de consumo están desarrollando y desplegando esas tecnologías a un ritmo récord. Si no es administrada de la manera adecuada, esta adopción potencialmente abre la puerta a riesgo cibernético incrementado.

Además, el hecho de que las analíticas de consumo estén en lo alto de la lista de inversiones planeadas en tecnología (figura 5) implica que los negocios de consumo están haciendo todo lo posible para capturar y aprovechar tantos datos del consumidor como sea posible. La consecuencia no-intencional de esta obtención de datos es que incrementa la posible superficie de ataque cibernético, dado que esos datos son no solo valiosos para la compañía, sino que también pueden ser monetizados por los atacantes. De hecho, el peligro de robo va más allá del PII del cliente para incluir patrones de gasto, datos de ubicación, tiempo gastado en almacenes, e incluso cartas de compra en línea abandonadas, de manera que la obtención de esos datos de los clientes puede proporcionar un motivo fuerte para un ataque cibernético.

Figura 5. Inversiones planeadas en tecnología para apoyar iniciativas estratégicas (porcentaje de inversión de los negocios en cada tecnología)



Nota: Tamaños de muestras: n(general)=402, n(productos de consumo)=150, n(restaurantes)=100, n(minorista)=100

Fuente: Análisis de Deloitte

Libro de jugadas del compromiso del ejecutivo

¿CÓMO LOS NEGOCIOS PUEDEN COMPROMETERSE CON LOS EJECUTIVOS DE LA SALA DIRECTIVA PARA DESARROLLAR UN PROGRAMA DE RIESGO CIBERNÉTICO ORIENTADO-AL-NEGOCIO?

A menudo, los ejecutivos de la sala directiva están en la mejor posición para vigilar la dirección de sus organizaciones, particularmente en cuanto se relaciona con cambiar las actitudes y el comportamiento alrededor de la seguridad cibernética. Hay varios enfoques para comprometer adicionalmente a los ejecutivos de la sala directiva en la administración del riesgo cibernético:

- **Establezca un comité inter-funcional a nivel de la sala directiva** con representación de la junta dedicado al riesgo cibernético.

- **Revise la estructura de administración de incidentes de violación cibernética**. Establezca criterios de escalonamiento para incluir ejecutivos de la sala directiva y miembros de la junta.

- **Comparta los resultados de las valoraciones del riesgo cibernético de la empresa y** su impacto en los resultados del negocio en las áreas de protección de datos sensibles y productos conectados.

- **Establezca un tablero de mando de indicadores de riesgo cibernético** y tendencias para apoyar el diálogo continuo alrededor de las inversiones estratégicas diseñadas para mejorar la madurez cibernética a través de la organización.

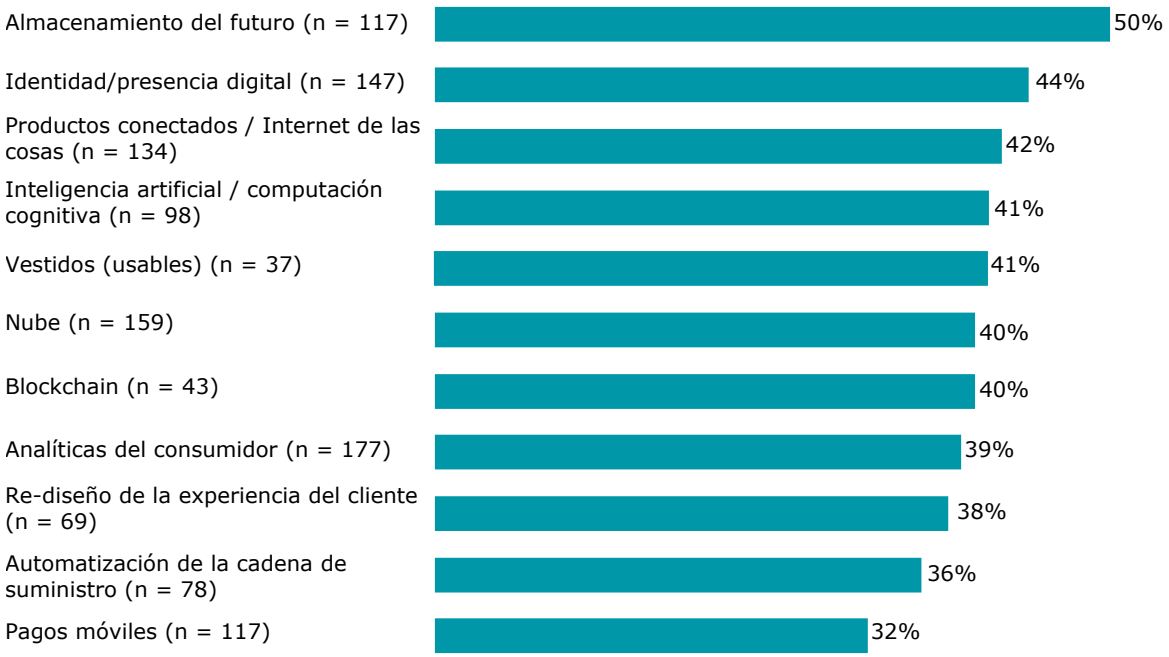
- **Proporcione actualizaciones a nivel ejecutivo y de la junta** que incluyan resultados de los esfuerzos amplios de conciencia y capacidad de recuperación del empleado, tales como lecciones aprendidas de simulaciones de juegos de azar y ejercicios de mesa. Los temas a abordar incluyen transparencia sobre los eventos más probables de riesgo cibernético que la compañía puede experimentar, estrategias clave de mitigación y respuesta ante incidentes, y oportunidades continuas identificadas.

Confianza del cliente

Armonización de los imperativos del negocio

El futuro puede parecer brillante para los negocios determinados a empujar los límites de la tecnología. Las analíticas de grandes datos están formando la base para las experiencias personalizadas que orientan la lealtad del cliente a lo largo de la vida. La funcionalidad móvil tiene el potencial para crear experiencias de compra y venta sin problemas en el almacén y en línea. Los productos conectados les ofrecen a los consumidores estilos de vida mejorados, "inteligentes," y descubrir nuevas maneras para que los negocios minimicen las ineficiencias operacionales. La innovación digital, sin embargo, llega con más que solo potencial de utilidades. Las iniciativas de tecnología populares entre los negocios de hoy incluyen aprovechar las analíticas del consumidor (44 por ciento), transición hacia tecnologías basadas-en-la-nube (40 por ciento), producción de productos conectados (33 por ciento), e implementación de pagos móviles (29 por ciento). Todas esas tecnologías requieren mayor agregación y almacenamiento de información sensible del cliente a través de un conjunto creciente de nuevos puntos de contacto (figura 6).

Figura 6. Porcentaje de compañías con programas maduros de seguridad cibernética en funcionamiento para abordar los riesgos emergentes*



Q16. *¿En cuáles tecnologías/iniciativas su organización está invirtiendo para apoyar las iniciativas estratégicas?*
Q17. *¿Su organización ha considerado los riesgos de seguridad cibernética para estas tecnologías clave?*

* *Entre quienes emplean esas tecnologías*
Nota: La muestra varía según los sectores dado que la pregunta fue hecha a quienes respondieron con base en su selección de la opción que aparece en la figura 1.

Fuente: Análisis de Deloitte

Muchos negocios parecen están priorizando la innovación rápida (y a menudo generar utilidades) sobre la seguridad cibernética. Si bien aprovechar la tecnología emergente comúnmente ha abierto nuevas corrientes de valor, los ejecutivos encuestados revelaron que esas tecnologías también incrementan su riesgo cibernético. Por ejemplo, solo el 30-40 por ciento de los ejecutivos encuestados que actualmente están invirtiendo en plataformas tales como analíticas de consumo, integración en la nube, y pagos móviles dijo que tienen en funcionamiento programas maduros para abordar los riesgos relacionados (figura 6).

La innovación y el riesgo cibernético a menudo están inextricablemente vinculados. Para los negocios, priorizar uno sobre el otro puede poner en peligro la creciente relación estrecha que las compañías tienen con sus clientes, particularmente porque las iniciativas de nueva tecnología pueden tomar ventaja de un portafolio excepcionalmente amplio de tipos de datos. Esos tipos de datos pueden exponer a los consumidores ante mucho más que al robo de tarjetas de crédito y al robo de identidad.

La seguridad alimentaria proporciona un buen ejemplo. Nuestro complicado sistema alimentario se está volviendo crecientemente conectado. Una variedad de jugadores, incluyendo compañías de alimentos y bebidas, agroindustria, restaurantes, y compañías de transporte comúnmente están aprovechando la conectividad para crear más eficiencia en el proceso complejo de alimentar millones de personas en todo el mundo. Este crecientemente conectado ecosistema alimentario, sin embargo, puede abrir maneras nuevas para que los criminales cibernéticos hagan daño, lo cual puede poner en peligro la salud de los clientes y causar daño potencialmente irreversible a la reputación de la marca. Muchos restaurantes que invierten en la cadena de suministro digital y en tecnología de almacenamiento de alimentos, por ejemplo, pueden abrir nuevos caminos para que los criminales cibernéticos estropeen la calidad de los alimentos. Actores maliciosos que tengan como objetivo la agroindustria podrían manipular la cantidad de los químicos que se colocan en los alimentos, causando enfermedad generalizada y, potencialmente, muerte.

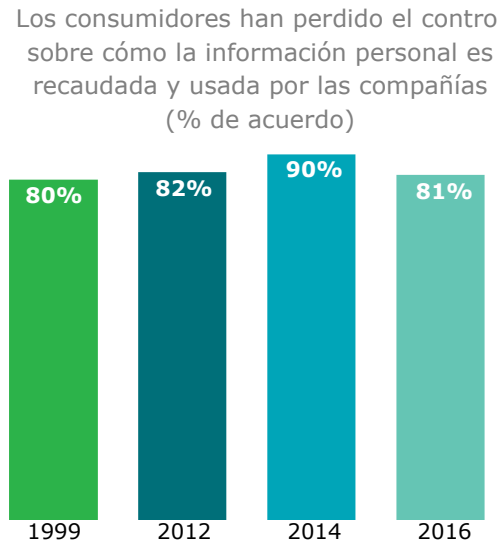
Los consumidores preocupados pueden ser implacables cuando se trata de violaciones cibernéticas

Los negocios de hoy pueden estar patinando en el hielo cuando se trata de que consumidores potenciales contragolpeen ante las violaciones cibernéticas. La investigación longitudinal a través de miles de consumidores de los Estados Unidos revela un estado aumentado de incertidumbre alrededor de la seguridad de los datos en la última década. En el año 2016, aproximadamente el 80 por ciento de los consumidores de los Estados Unidos sintió que perdieron el control sobre cómo su información personal estaba siendo usada por las compañías (figura 7).[3] Este sentimiento ha permanecido relativamente sin modificación desde 1999, a pesar de las violaciones de alto perfil ocurridas en la última década.

Esta desconfianza de larga data representa una oportunidad para que los negocios de consumo aborden este problema y quizás creen una ventaja competitiva mediante ser más transparentes con (1) cómo y dónde recaudan los datos de los clientes; (2) qué hacen con esos datos; y (3) cómo protegen los datos. Mediante invertir en capacidades de seguridad cibernética, los negocios de consumo pueden incrementar sus oportunidades para defender esta confianza y mejorar su marca.

Los negocios también deben considerar cómo la incertidumbre acerca de la privacidad de la información personal puede impactar las futuras decisiones de compra – particularmente cuando se trata de que los consumidores escojan de quién comprar. Los consumidores de hoy no carecen de opciones, y el cambio de marcas es tan fácil como descargar una nueva aplicación.

Figura 7. Los consumidores sienten que han perdido el control sobre cómo las compañías usan su información personal



Fuente: Análisis de Deloitte

Los consumidores han demostrado que pueden ser implacables con los negocios que sean negligentes con sus datos. En este estado aumentado de malestar, los clientes permanecen vigilantes, y los esfuerzos para mitigar su propio riesgo a menudo se convierten en acciones y comportamientos cautelares e incluso punitivos, tales como disminuir el compromiso en línea y fuera de línea con las marcas que perciben son un riesgo. Durante los últimos 12 meses, el 31 por ciento de los consumidores de los Estados Unidos eliminó de sus teléfonos inteligentes aplicaciones específicas, y el 27 por ciento evitó sitios web específicos para mitigar su propio riesgo cibernético. Algunos consumidores, si bien solo una cantidad pequeña, no compró cierto producto o compró el mismo producto de una marca diferente (figura 8).

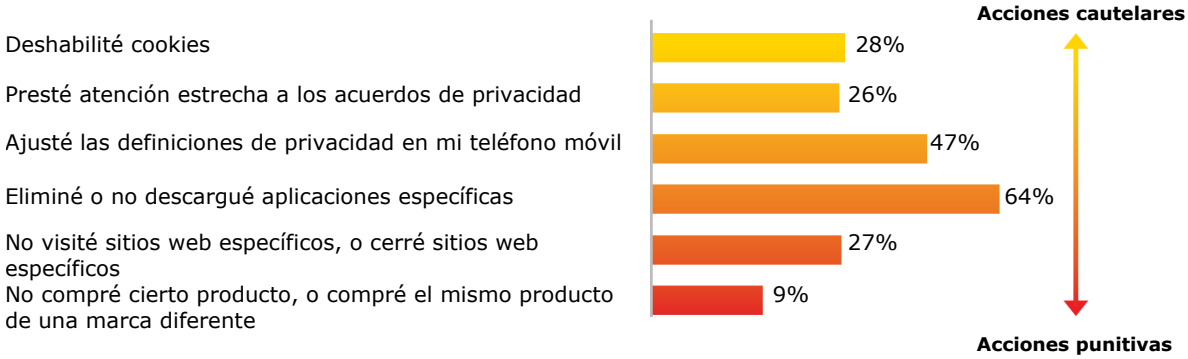
Las consecuencias potenciales de subestimar la confianza

La industria de productos de consumo ofrece un ejemplo de la creciente importancia (y desafío) de mantener la confianza del cliente en la era digital – particularmente en el mercado rápidamente creciente de productos conectados. En los almacenes físicos y en línea, muchos de los consumidores de hoy se están encontrando a sí mismos en un territorio nuevo y no familiar. Productos que durante décadas han permanecido relativamente sin modificación, tales como termostatos, cerraduras de puertas, e incluso accesorios de cocina tales como refrigeradores, a menudo ahora vienen equipados con conectividad con la Red. Esta nueva generación de productos puede ofrecer a los consumidores funcionalidad nueva, innovadora, al tiempo que también les ofrece a los negocios una nueva frontera para el crecimiento de los ingresos ordinarios.

De lejos, la demanda por muchos tipos de dispositivos conectados, incluyendo seguidores del acondicionamiento físico y dispositivos hogareños inteligentes, permanece saludable.[4] Sin embargo, aprovechando el segmento completo, el potencial de crecimiento en el largo plazo depende ampliamente de la confianza del consumidor. Muchos consumidores tienen que sentir confianza de que esos productos no solo operan impecablemente, sino que también no conducen a abrir nuevas puertas para la actividad criminal. En la medida en que productos tales como cerraduras inteligentes se instalan en más viviendas, por ejemplo, probablemente llamarán la atención de los criminales cibernéticos que buscan explotar las potenciales debilidades. Contribuyendo al crecimiento de la preocupación, los riesgos cibernéticos emergentes continúan golpeando la industria de atención en salud, dado que las debilidades de la seguridad de los dispositivos conectados tales como monitores del corazón ocupan los titulares de las noticias.[5] Las continuas noticias de violaciones mediante esos dispositivos pueden no solo amenazar las ventas de un producto o marca particular sino también empañar las percepciones amplias que los consumidores tienen de los productos conectados en general – poniendo en peligro billones en el crecimiento de ventas futuras.

Figura 8. Los consumidores actúan para evitar la violación de los datos

En los últimos 12 meses, ¿hizo usted cualquiera de los siguientes debido a preocupaciones por la privacidad de los datos?



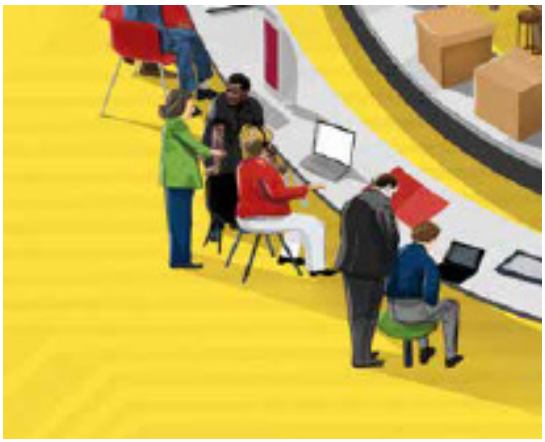
Fuente: Deloitte, SSI, and JD Power, estudio sobre la privacidad del consumidor presentado en la Next2017 Conference, Mayo 9-10, 2017, New York.

Las compañías de productos de consumo pueden estar subestimando la importancia de construir confianza del consumidor alrededor de la seguridad cibernética y la innovación digital. De hecho, cuando se piensa acerca de potenciales incidentes cibernéticos, las compañías de productos de consumo en nuestra encuesta parece que están principalmente preocupadas en las disrupciones de la producción (48 por ciento) y la pérdida de propiedad intelectual (42 por ciento), mientras que significativamente pocas (16 por ciento) están preocupadas por la pérdida de las percepciones de la marca relacionadas con la confianza.

En un mercado competitivo, la inmensa presión para lograr metas agresivas de producción en orden a ganar la "ventaja de quien se mueve primero" en las categorías de productos emergentes puede arrojar una sombra sobre la importancia de construir percepciones del cliente positivas, de largo plazo, alrededor de los productos conectados. En últimas, en este entorno, la protección cibernética alrededor de los productos conectados no es tan robusta como debe ser. De hecho, cerca de un tercio de los negocios de consumo que participaron en nuestra encuesta no sienten que sean efectivas sus iniciativas actuales en relación con el riesgo cibernético y sus prácticas alrededor de los productos conectados.

Re-imaginar la seguridad cibernética como una potencial ventaja competitiva

Independiente de la industria, muchos negocios orientados al consumidor están enfrentando batallas similares. Permanecer relevante en el mercado de hoy a menudo requiere que las compañías desplieguen iniciativas de tecnología con cronogramas y presupuestos apretados – lo cual puede agregar a los desafíos de la mitigación del riesgo cibernético. Pero los negocios no pueden darse el lujo de evitar la seguridad cibernética. Las compañías necesitan pensar acerca de cómo décadas de sub-invertir en la seguridad cibernética impactará el crecimiento en el largo plazo. La protección de los datos es algo que los consumidores han llegado a esperar, y las inversiones en seguridad pueden crear una ventaja competitiva en el mundo de hoy de crecientes ataques cibernéticos.



Libro de juegos de la confianza del consumidor

¿CÓMO PUEDE USTED CONSTRUIR LA CONFIANZA DEL CONSUMIDOR TENIENDO EN MENTE LA SEGURIDAD CIBERNÉTICA?

Muchas organizaciones están adoptando nuevas tecnologías, ya sea analíticas del consumidor o productos conectados, con la meta de generar nuevas corrientes de ingresos ordinarios. Si bien a menudo vemos la adopción saludable de esos servicios y productos por los consumidores, la adopción de largo plazo probablemente dependerá de la capacidad de la marca para invocar la confianza del consumidor. Esta podría ser una oportunidad de oro para que los negocios construyan diferenciación de la marca en el mercado mediante acoger la seguridad cibernética como un principio fundamental para construir esa confianza del consumidor. Las maneras como se puede lograr esto incluyen:

- **Construya una reputación por la protección de la información y privacidad del consumidor:** Es importante dejar que sus consumidores sepan que la protección de su información y privacidad es tomada muy en serio. Comunique los pasos dados para mantener segura su información. Eduque a los consumidores sobre la seguridad cibernética en cuanto ella se relacione con el uso de sus productos y servicios. Comparta su responsabilidad con los consumidores en relación con las potenciales implicaciones legales de los productos conectados.

- **Construya seguridad en sus productos y servicios**: Cada vez, como organización, que usted piense en desarrollar un nuevo producto o servicio para crecimiento, inserte la seguridad en primer lugar cuando usted piense acerca de diseñar la funcionalidad del producto o servicio. Este puede

ser un elemento fundamental del desarrollo de la confianza del cliente. Usted quiere que su producto o servicio sea de clase mundial. Parte de esa expectativa incluye no dejar que ese producto o servicio sea explotado por criminales, causando daño a sus consumidores.

- **Sea transparente con sus consumidores y deles el control**: Muchos consumidores están dispuestos a compartir su información con usted por algún control sobre cómo la información es usada. Sea transparente acerca de cómo su información será usada y compartida. Haga que sea fácil para sus consumidores tener voz en el proceso de manera que puedan controlar el flujo de la información. Implemente procesos fuertes para hacer honor a sus solicitudes.

- **Administre a sus asociados de negocio y a sus proveedores terceros**: En el mundo de hoy, cuando las líneas entre la empresa y el exterior se están borrando, la información del consumidor a menudo es compartida con terceros, o productos y servicios son adquiridos de ellos, lo cual puede poner en peligro la reputación y por consiguiente la confianza del consumidor. Ordene que los proveedores terceros sigan el mismo estándar de seguridad cibernética de su organización a fin de establecer que usted es serio acerca de la construcción de la confianza del consumidor.

- **Conozca a sus consumidores, pero también conozca cómo proteger ese conocimiento**: Entienda lo que usted recolecta de sus clientes y por qué. Entienda dónde y cómo esa información fluye en su organización y más allá. Tome opciones responsables; limite la recolección de información a lo que usted necesita para el negocio, y luego conténgala y protéjala.

- **La experiencia del consumidor supera todo**: La administración del riesgo cibernético es un componente central de la experiencia de los consumidores. Tener una mala experiencia a causa de un incidente cibernético probablemente erosionará su marca y la confianza del consumidor. Eleve el rol del riesgo cibernético, e insértelo como una responsabilidad de trabajo para los ejecutivos de la sala directiva tales como el director jefe de la experiencia con el cliente, el CMO, y otros que sean directamente responsables por su marca y por el compromiso del consumidor.

Productos conectados

Los productos conectados pueden tener potencial ilimitado – incluyendo un incrementado riesgo cibernético

La adopción de productos conectados se espera que crezca dramáticamente en los próximos años. Si bien los estimados del crecimiento en los dispositivos conectados varían de manera considerable, Gartner sugiere que habrá un estimado de 20.8 billones de ellos para el 2020, y otros sugieren que el número podría ser tan alto como 31 billones.[6] Sin embargo, el éxito futuro de los productos conectados puede depender no solo de la tecnología que facilite la conectividad sino también de la confianza del consumidor, la cual puede orientar la demanda.

El rápido crecimiento de los productos conectados ofrece no solo numerosos beneficios para los negocios de consumo y sus clientes, sino también riesgo cibernético incrementado. Esto porque muchos productos conectados confían en tecnologías avanzadas tales como la nube para almacenar información, así como también en los pagos móviles para facilitar las transacciones. Junto con los beneficios de la conectividad cada vez más creciente, las vulnerabilidades de la seguridad cibernética son cada vez más comunes en la medida en que las compañías incrementan los puntos de entrada a sus sistemas, abriendo la puerta a violaciones que puedan surgir en cualquier parte a través de todos los ecosistemas conectados – desde consumidores hasta proveedores terceros.

El potencial inconveniente de los productos conectados

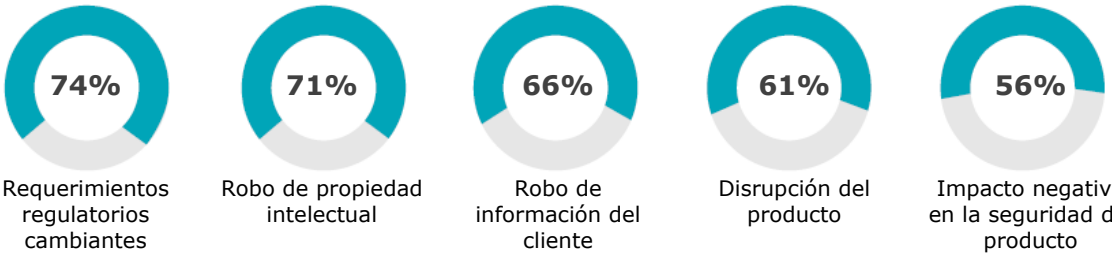
En nuestra encuesta, aprendimos que los ejecutivos no confían en la seguridad de los productos conectados: el 32 por ciento no considera que su programa de administración del riesgo cibernético sea efectivo en mantener su estrategia para desarrollar y comercializar productos conectados.

No sorprende, entonces, que los negocios orientados al consumidor reporten una variedad de preocupaciones acerca de su despliegue de productos conectados, con el 74 por ciento de quienes despliegan productos conectados citando los requerimientos regulatorios cambiantes como su preocupación principal (figura 9).

El riesgo operacional también puede ser introducido por productos conectados. En un mundo crecientemente conectado, los ecosistemas de los negocios de consumo están expuestos a mayor riesgo de que un incidente cibernético pueda tener un impacto directo en las operaciones centrales del negocio. Esto puede incluir impactos tales como disrupción de la cadena de suministro, interrupción de ventas de almacén minorista, o mal funcionamiento del sitio de comercio electrónico. En la medida en que aumenta la adopción de productos conectados, también lo hace la dependencia del Internet de las cosas en general [Internet of Things (IoT)] en general – y, por consiguiente, del riesgo cibernético asociado con ello. A causa de esto, los negocios de consumo necesitan ampliar su enfoque para la administración del riesgo cibernético desde solo protección de datos, evitar el riesgo, y respuesta al incidente para asegurar operaciones sostenibles.

Figura 9. Preocupaciones más grandes alrededor de los productos conectados

"Piense acerca del centro de atención de su compañía puesto en los productos conectados, ¿qué tan preocupado está usted por cada una de las siguientes amenazas cibernéticas?"
(% muy o extremadamente preocupado)



Fuente: Análisis de Deloitte

El 32 por ciento de las compañías no considera que su programa de administración del riesgo cibernético sea efectivo en mantener su estrategia para desarrollar y comercializar productos conectados.

Los productos conectados presentan un desafío importante para los ejecutivos de la seguridad cibernética debido tanto al creciente número de dispositivos conectados como también a su desarrollo y despliegue rápidos. Algunos ejecutivos cibernéticos nos dicen que nunca saben de dónde vendrá la amenaza, haciendo que sea extremadamente difícil poner en funcionamiento las salvaguardas correctas. Tal y como un ejecutivo de industria nos lo dijo:

Con relación hacia dónde la industria está yendo con el Internet de las cosas, la pregunta es cómo aseguraremos estas cosas. Es una gran parte de nuestro futuro en el corto plazo. Asegurar que tenemos un buen manejo del entendimiento de lo que los dispositivos son, cómo las personas los están usando, y cómo asegurarlos – hay una cantidad de trabajo por asegurar. En la industria, necesitamos gastar una cantidad de tiempo en esto en el futuro. Sólo mantenerse al día con estas cosas es suficientemente desafiante.

No olvide el potencial ilimitado de los productos conectados

Los productos conectados facilitados por el IoT pueden hacer posible un mundo donde todas las cosas y todo el mundo estén potencialmente conectados – consumidores, minoristas, y compañías de productos de consumo. Los dispositivos conectados pueden ofrecer a los negocios orientados al consumidor y a sus clientes potencial sin límites para alcanzar beneficios tales como experiencia mejorada del cliente y personalización de productos y servicios.

APLICACIONES INNOVADORAS PARA DISPOSITIVOS CONECTADOS

La tecnología se une con la industria de la moda con vestidos elaborados a partir de datos de las aplicaciones. Además del uso de LED y comunicación cercana-al-campo [near-field communication (NFC)], los jugadores globales de tecnología y moda revelaron ejemplos de la intersección entre moda y conectividad en la Semana de la moda realizada en Nueva York en febrero de 2017. Si bien las prendas no estaban conectadas al usuario, el proceso de diseño lo estaba. Los diseñadores de moda aprovecharon datos de aplicaciones personales obtenidos vía teléfonos inteligentes para crear vestuario digitalmente personalizado, hecho a la medida, basado en el entorno del usuario, incluyendo sus rutas habituales, nivel de actividad, y las temperaturas típicas en el área del usuario. Esta información, conocida como señales de contexto, fue pasada a través de un algoritmo para informar el diseño del vestuario.[7]

El almacén del futuro. En el evento "Store of the Future" realizado en el Design Museum en Lonfres en abril de 2017, las marcas de comercio electrónico desplegaron bastidores de ropa conectados, espejos con pantalla táctil, y estaciones de inicio de sesión que ayudaron a eliminar la brecha entre en línea y el minorista de ladrillo-y-cemento. Por ejemplo, los clientes pudieron escanear sus teléfonos inteligentes a partir de ingresar a una localización minorista para permitir que los asistentes de venta vieran sus perfiles, incluyendo qué elementos previamente compraron o guardaron en una lista de deseos en línea. Los bastidores de ropa conectados registraron qué elementos los clientes físicamente se probaron, almacenando esta información en aplicaciones que los clientes posteriormente podrían deslizar a izquierda o derecha para editar sus selecciones. Los vidrios inteligentes les permitieron a los compradores solicitar elementos de otro tamaño, buscar alternativas en línea, e incluso pagar sin abandonar el vestidor. Los minoristas también demostraron pantallas holográficas que les permitieron a los clientes crear y ordenar zapatos personalizados, experimentando con diferentes cueros, pieles, y colores.[8]

Para las compañías que despliegan dispositivos conectados, los dados que esos dispositivos recaudan pueden ser invaluables, proporcionando una ventana sobre las preferencias del consumidor y permitiendo que los negocios orientados al consumidor optimicen la experiencia del cliente y la innovación. Pero cómo esta información es obtenida, almacenada, y analizada puede hacer tanto a los usuarios como a los negocios de consumo más vulnerables ante el riesgo cibernético.

Si bien los usos de la recordación de los consumidores para los productos conectados tienden a centrarse en aplicaciones de salud y bienestar, muchos negocios orientados al consumidor están invirtiendo en maneras nuevas, creativas, para desplegar productos conectados – por ejemplo, en moda y minoristas (vea el recuadro "Aplicaciones innovadoras para dispositivos conectados"). Es decir, esas aplicaciones necesitarán ser aseguradas de la manera apropiada para que sean exitosas.

Un cuento de dos juguetes: potencial al alza y a la baja de los productos conectados

Incluso los juguetes conectados potencialmente pueden entregar valor para sus usuarios finales – o, inversamente, robar información de propietario cuando los fabricantes del dispositivo no den los pasos necesarios para asegurar los datos que capturan. Esos tipos de violaciones pueden ser problemáticos para los fabricantes de dispositivos, considerando que el niño hoy puede tener muchos de sus propios dispositivos conectados. En esos casos, asegurar los dispositivos conectados puede no ser ya solo un problema de seguridad cibernética, sino una preocupación acerca de la seguridad física y emocional actual del niño que los usa para diversión y entretenimiento.

En el show 2017 Consumer Electronics, un fabricante de juguetes líder introdujo la primera muñeca interactiva del mundo, la cual puede jugar juegos y contar historias, así como también escuchar y aprender en lo que las niñas estén interesadas. La información recaudada es subida a la nube y continuamente actualizada vía las capacidades Wi-Fi de la muñeca. La muñeca llega a conocer las preferencias, gustos, y disgustos de la niña, y luego incorpora este conocimiento en sus conversaciones, teniendo por lo tanto el potencial para hacerse amiga de la niña.[9]

Pero los juguetes interactivos también pueden tener inconvenientes: demasiada información puede ser compartida y/o usada de manera inapropiada. Un ejemplo reciente involucra a un fabricante de osos de peluche cuya colección de 2.2 millones de grabaciones de voz de niños y sus padres puede haber sido expuesta a una violación de datos; los datos comprometidos también incluyeron direcciones de correos electrónicos y datos de claves para más de 800,000 cuentas.[10]

Libro de juegos de productos conectados

¿CÓMO LOS PRODUCTOS CONECTADOS PUEDEN SER ASEGURADOS?

En general, es esencial que los negocios de consumo aseguren la seguridad de los productos conectados si tanto los negocios como sus clientes están cosechando beneficios de esos productos. Esto puede ser logrado mediante múltiples esfuerzos, incluyendo:

- **Cree un inventario comprensivo, holístico, de los productos conectados vinculados a la red** para ayudar a identificar los potenciales puntos de entrada y vulnerabilidades.

- **Valore el valor agregado para la nueva funcionalidad del producto conectado, antes de su liberación**. Cada nueva característica establecida puede ofrecer riesgo adicional para tanto el consumidor como para la organización; ambos pueden requerir protección incrementada ante intentos maliciosos. El valor agregado de cualquier característica dada que se establezca debe compensar el costo de asegurar esas características. De otra manera, el apetito que la organización tenga por las medidas de seguridad cibernética puede ser insuficiente ante el nivel requerido de inversión.

- **Comprométase activamente con legal** para asegurar que los acuerdos con el cliente de manera clara establecen los roles y las responsabilidades, tanto de la compañía como del consumidor, con relación a materias tales como la propiedad de los datos recaudados por los productos conectados y las acciones a realizar en el evento de una violación. Es importante tener claras y anticipadas cualesquiera responsabilidades que el cliente pueda tener para ayudar a administrar de manera efectiva los riesgos cibernéticos.

- **Considere los principios de la seguridad-por-diseño y de la seguridad fuerte de la aplicación**. Los consumidores no siempre son capaces de actualizar el software permanente programado en la memoria de solo lectura, y algunas veces descuidan hacerlo incluso cuando las actualizaciones estén disponibles. La expectativa es que los negocios de consumo producirán productos que sean inmediatamente seguros después de la línea de ensamble, o potencialmente pueden sufrir impactos negativos en operaciones, marca, funcionalidad, o cumplimiento regulatorio.

- **Recuerde que la vieja escuela de la higiene de la protección de datos todavía aplica a la nueva era de productos conectados**. Mucha de la información recaudada por los productos hoy puede ser considerada privada y/o confidencial. Tal y como ocurre con cualesquiera de tales datos, los

datos recaudados por productos conectados deben ser protegidos a partir del recaudo, mientras estén en tránsito, y cuando sean almacenados tanto en el dispositivo como en el almacén de datos. Adicionalmente, las políticas de privacidad y uso de datos, incluyendo las políticas relacionadas con transferencia de datos transfronterizos, deben ser actualizadas para reflejar la nueva era de recaudo de datos 24/7 en hogares, en carreteras, en personas, y de otras maneras.

- **Evalúe el alcance de otros esfuerzos de empresa**, tales como el monitoreo de amenazas cibernéticas y ejercicios de juegos de azar / capacidad de recuperación, a fin de determinar si esos esfuerzos son suficientemente comprensivos para cubrir los principales riesgos cibernéticos relacionados con productos conectados.

Pagos

Las tecnologías emergentes de pago están atrayendo muchos negocios orientados al futuro – y criminales cibernéticos oportunistas

Las tecnologías emergentes de pago pueden facilitar que los negocios eleven la experiencia del cliente mediante racionalizar – y en muchos casos reinventar – el proceso de pago. Si bien NFC y otras tecnologías móviles de pago han existido durante algún tiempo, los consumidores finalmente están calentando ideas tales como usar sus teléfonos inteligentes como billetera, señalando un cambio de la corriente principal de cómo se hacen los pagos. De hecho, el mercado de billeteras móviles, valuado en aproximadamente $594 billones en 2016, se espera que surja vertiginosamente hasta $3.142 billones para el 2022, con una tasa de crecimiento anual compuesto de alrededor del 32 por ciento entre 2017 y 2022.[11] Las compañías que sean capaces de aprovechar las tecnologías emergentes de pago al tiempo que simultáneamente mantengan la seguridad de sus plataformas de pago estarán mejor posicionadas para ganar a partir de esas inversiones.

Muchos restaurantes, minoristas, y otros negocios orientados al consumidor están compitiendo para mantenerse por delante de la tendencia del pago móvil. El treinta por ciento de los ejecutivos en nuestra encuesta resaltó la experiencia del cliente como una prioridad estratégica principal para sus organizaciones, y para muchos, la inversión en tecnología móvil de pago es una parte clave de esa iniciativa. Además, tres de diez ejecutivos citaron los pagos móviles como la principal iniciativa de tecnología.

Menos de un tercio (32 por ciento) de los ejecutivos que invierten en soluciones de pago móvil sienten que tienen en funcionamiento controles de seguridad maduros alrededor de la tecnología.

Si bien los negocios continúan explorando cómo la tecnología móvil de pago puede transformar la experiencia en-el-almacén, y muchos están incorporando la tecnología automática de pago en sus aplicaciones, relativamente pocos están construyendo protección adecuada. Nuestro estudio reveló que solo el 32 por ciento de los ejecutivos de compañías que implementan tecnología móvil de pago sienten que tienen en funcionamiento programas de seguridad cibernética "maduros." Los líderes deben recordar que las mismas tecnologías que emplean para proporcionar nuevos y eficientes canales de entrega para sus clientes también están siendo usadas agresivamente por hackers y elementos criminales. Los criminales cibernéticos probablemente probarán los sistemas emergentes de pago porque no están tan protegidos como algunos otros.

Manténgase al día con el panorama en evolución de los pagos

La constante evolución de la tecnología de pago requiere vigilancia cibernética perpetua. El largo tiempo esperado desarrollo de la tecnología de chip EMV, por ejemplo, fue una ganancia en la batalla contra el crimen cibernético y el fraude. Sin embargo, los negocios no deben tener un sentido falso de seguridad. Últimamente, estratagemas tales como la tecnología EMV de "chip-y-PIN" probablemente no erradicarán el fraude en el pago, sino que simplemente cambiarán el tipo de fraude que ocurre cuando los criminales cibernéticos buscan explotar nuevas debilidades.

En orden a mantenerse al día con el cambio, los programas efectivos de seguridad cibernética deben asignar suficiente presupuesto para el desarrollo de controles de seguridad nuevos y para el mantenimiento de los existentes. Los ejecutivos en nuestra encuesta señalaron que actualmente están asignando aproximadamente un tercio del total de sus presupuestos cibernéticos para desarrollar nuevos controles de seguridad y para mantener los existentes.

La vulnerabilidad alrededor de los pagos está en aumento en la medida en que los consumidores comienzan a acoger a terceros proveedores de pago

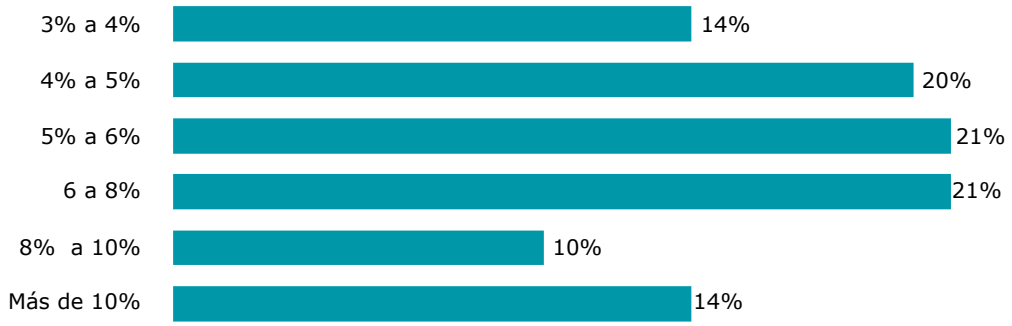
Muchos negocios de consumo crecientemente están aprovechando la tecnología de pago digital de compañías que se especializan en pagos electrónicos. Esta confianza en terceros puede crear obstáculos completamente nuevos en el mundo de la seguridad cibernética. Los negocios pueden invertir fuertemente en sus propias iniciativas de seguridad cibernética, pero puede ser un todo por nada si el tercero vendedor crea un vínculo débil en la cadena. Mientras muchos negocios de consumo parecen confiar extremadamente en los terceros proveedores con los cuales trabajan, nuestra encuesta señala que solo pocos regularmente revisan y prueban las capacidades de la seguridad cibernética de sus proveedores.

Las franquicias aumentan la vulnerabilidad cibernética de la marca

Para muchas marcas, particularmente en los sectores de restaurantes y hospitalidad, la expansión geográfica es clave para el crecimiento. Si bien las franquicias pueden darles a las marcas una manera efectiva para escalar, también puede crear una variedad de problemas de seguridad cibernética. A pesar de parecer grande, marcas globales en la superficie, muchas franquicias operan más como negocios de tamaño pequeño a mediano, y el gasto en seguridad cibernética a menudo toma el asiento trasero de las iniciativas relacionadas con utilidades.

A menudo, las franquicias asumen que los criminales están detrás de los "chicos grandes," negocios que manejan miles de pagos diariamente. Este falso supuesto puede actualmente hacer a las franquicias más susceptibles de violaciones porque generalmente no hacen de la seguridad cibernética una prioridad alta. Las organizaciones de restaurantes proporcionan un excelente ejemplo. Con financiación limitada para la seguridad cibernética (figura 10), muchas franquicias de restaurantes tercerizan sus sistemas de punto-de-venta [point-of-sale (POS)] con terceros proveedores de servicios, los cuales pueden no siempre adherirse a las mejores prácticas de seguridad.

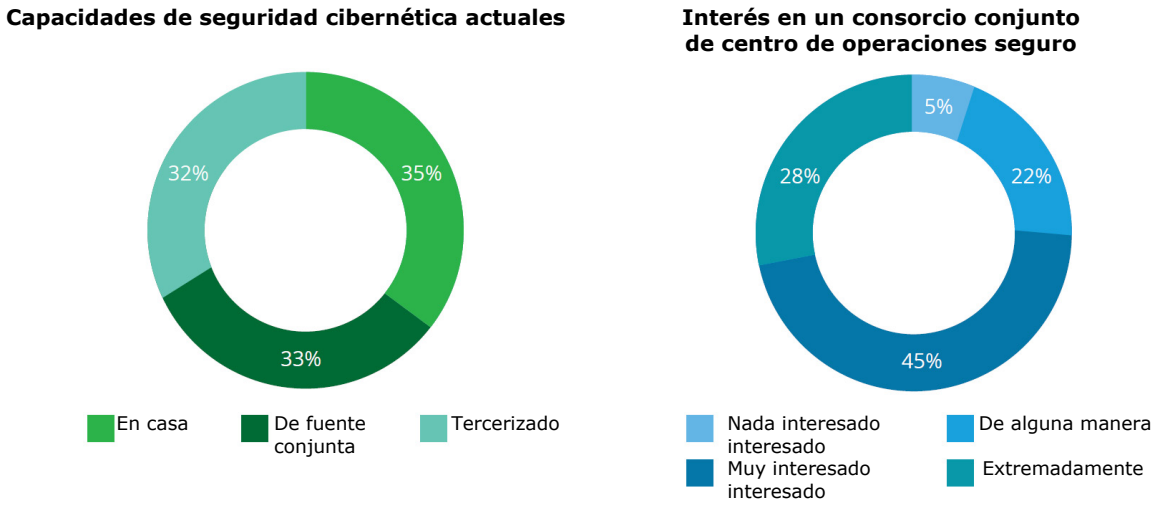
Figura 10. Presupuestos de seguridad cibernética (como un porcentaje del presupuesto anual de TI)



Nota: Tamaños de muestra: n(general)=400, n(productos de consumo)=149, n(restaurantes)=99, n(minorista)=100. Excluye agroindustria.

Fuente: Análisis de Deloitte

Figura 11. Tercerización de seguridad cibernética e interés en un consorcio conjunto de centro de operaciones seguro (solo restaurantes)



Q11. ¿Qué tanto sus capacidades actuales de seguridad cibernética son tercerizadas, en casa, o de fuente conjunta?
Q10. ¿Qué tan interesado estaría usted en unirse a un consorcio de centro de operaciones seguras de industria restaurantes/minorista?

Fuente: Análisis de Deloitte

La tercerización de servicios de seguridad cibernética a menudo ha sido una manera efectiva para que las franquicias de restaurantes aprovechen al máximo los presupuestos limitados de seguridad cibernética. Como grupo, los restaurantes que encuestamos ya sea tercerizaron o tuvieron fuente conjunta para cerca de dos tercios de sus capacidades de seguridad cibernética (figura 11). Particularmente cuando se trata de capacidades para monitorear y dar acceso, las organizaciones de restaurantes encuestadas están muy interesadas en unirse a consorcios de colaboración cibernética que les permitiría reunir de manera efectiva recursos con otros restaurantes participantes.

Libro de juegos de los pagos

¿CÓMO PUEDEN LOS NEGOCIOS DE CONSUMO ASEGURAR QUE LOS PAGOS ESTÉN SEGUROS?

Es crítico tanto para los negocios como para los consumidores que los sistemas de pago sean seguros. Los negocios pueden dar varios pasos para lograr esto:

- **Considere establecer un cuerpo formal de gobierno** responsable por la seguridad y el cumplimiento en el pago.
- **Mantenga a las unidades de negocio aplicables y a las funciones de negocio informadas** de e incluidas en las discusiones acerca de la seguridad del pago.
- **Realice un ejercicio de alcance** para mapear el ciclo de las transacciones de pago, y entienda completamente tanto las tecnologías como las unidades de negocio involucradas (tales como transacciones con tarjeta presente, centros de llamadas, transacciones automatizadas de compensación, comercio electrónico, y funciones de respaldo tales como contabilidad y finanzas).
- **Revise los acuerdos contractuales con terceros proveedores** tales como la adquisición de bancos. Entienda las obligaciones de cumplimiento de su organización (tales como PCI DSS) en cuanto se relacionan con su entorno de pago.
- **Implemente procesos y tecnologías** que ayuden a mantener un inventario exacto, actualizado, de los puntos finales de pago (tales como dispositivos POS).
- **Realice escaneos regulares de la vulnerabilidad** y mantenga actualizadas las tecnologías de pago con los últimos parches de seguridad.
- **Registre y monitoree la actividad** sospechosa en relación con la salud y seguridad de sus tecnologías de pago.
- **Documente y pruebe los planes de respuesta** en el evento de caídas no planeadas del pago o violaciones de los datos.

Propiedad intelectual

El impacto potencialmente devastador de una violación de IP: robo cibernético y pérdida de IP

Si bien la pérdida de datos del cliente durante una violación puede hacer crujir la confianza del cliente y empañar la imagen de la marca, la pérdida de propiedad intelectual [intellectual property (IP)] podría amenazar el futuro de la compañía. La IP orienta la innovación, la competitividad, y el crecimiento de cualquier negocio, y puede constituir más del 80 por ciento del valor de una sola compañía hoy.[12] Para una compañía de productos de consumo, la IP puede ser información crítica acerca de una nueva línea de productos o la formulación del producto a partir de la cual la compañía fue construida. Para un restaurante, puede ser el ingrediente secreto de una receta increíble.

La propiedad intelectual aumenta como una preocupación principal relacionada con los datos

El estudio de Deloitte sobre el riesgo cibernético en la fabricación avanzada reveló que la IP era, entre los ejecutivos encuestados, una preocupación principal relacionada con los datos – solo después del robo financiero.[13] Este aumento de la preocupación por el robo de IP se refleja en los negocios de consumo, si bien el público en general, cuando piensa sobre las compañías de negocios de consumo, tiende a centrarse más en los crímenes cibernéticos familiares tales como robo de tarjeta de crédito y robo de otra PII. El cuarenta y dos por ciento de los ejecutivos de alimentos y bebidas que encuestamos, por ejemplo, estuvo preocupado por los criminales cibernéticos que intentan robar información propietaria de producto tal como recetas de alimentos y códigos de producto.

El 42 por ciento de los ejecutivos de alimentos y bebidas que encuestamos, por ejemplo, estuvo preocupado por los criminales cibernéticos que intentan robar información propietaria de producto tal como recetas de alimentos y códigos de producto.

El aumento de la preocupación por el robo de IP entre los negocios de consumo no carece de razón. El robo de IP está en aumento a través de la junta. De acuerdo con una encuesta reciente realizada por Deloitte, el número de incidentes de robo cibernético de IP se espera que se incremente en los próximos 12 meses.[14]

La evolución del robo de IP

El aumento de la preocupación alrededor del robo de IP puede originarse ampliamente en la naturaleza en evolución de las violaciones. Históricamente, el robo de IP principalmente tomó la forma de empleados descontentos que huían con documentos físicos, discos de computador, o prototipos. Para cometer el crimen los malhechores tenían ya sea conocimiento directo de o eran capaces de tener acceso físico a los secretos comerciales. En contraste, en un mundo digital, los ladrones de IP pueden operar desde cualquier lugar con relativo anonimato, haciendo que el grupo de posibles sospechosos sea amplio y profundo. La lista de potenciales perpetradores puede además incluir personal interno tales como empleados actuales y anteriores, pero también incluye competidores, hackers recreativos, e incluso actores de nación-estado.

El sistema emergente de productos conectados es un ejemplo de una tecnología que puede cambiar la forma del robo moderno de IP. Si bien la conectividad ofrece maneras nuevas para que los negocios creen valor, también crea nuevas oportunidades para que se pueda tener acceso a la información y ésta pueda ser comprometida.[15] De hecho, quienes nos respondieron citaron al robo de IP como la principal preocupación alrededor de la inversión continuada en dispositivos conectados, superando las preocupaciones sobre el robo de información del cliente, disrupción de producto, e impactos negativos para la seguridad del producto (vea la figura 9 en la discusión sobre los productos conectados).

La naturaleza en evolución y el aumento de la incidencia del robo de IP probablemente requiere un enfoque comprensivo del riesgo cibernético alrededor de la administración de la identidad y el acceso a los datos, teniendo en consideración quién puede tener acceso a cierta información, dónde y cómo la información es

almacenada, y la aplicación de los controles de seguridad a nivel de los datos mismos. Desafortunadamente, la administración de la identidad y el acceso a menudo es un vínculo débil en la cadena de la seguridad cibernética de la organización. Los ejecutivos que encuestamos citaron "la administración de los datos y del acceso" como el elemento menos maduro del programa de seguridad cibernética de su compañía – calificándolo por debajo de otros siete atributos, incluyendo administración del cumplimiento y del programa, seguridad de la aplicación, y estrategia de seguridad cibernética (figura 12).

Libro de juegos de la propiedad intelectual

¿CÓMO PUEDE SER ASEGURADA LA PROPIEDAD INTELECTUAL?

Asegurar la IP comúnmente es desafiante, dado que no es bala de plata. La historia muestra que las medidas tradicionales de seguridad tales como la seguridad perimetral son necesarias, pero no son completamente efectivas. Se necesita un cambio fundamental en el enfoque para aplicar los controles de seguridad de una manera estratificada que considere los riesgos y amenazas tanto internos como externos. En otras palabras, este enfoque debe considerar no solo quiénes pueden atacar desde afuera y qué tecnologías pueden emplear, sino también quiénes desde el interior – tales como empleados deshonestos o terceros contratistas – quiénes pueden tener los motivos, los medios, y la oportunidad para robar IP.

A menudo se recomienda que las organizaciones apliquen controles de seguridad a nivel de los datos mismos (el modelo de seguridad "dentro afuera") además de otras capacidades básicas tales como seguridad perimetral, administración de la vulnerabilidad, seguridad de la aplicación, y similares. La protección de los datos desde el interior se centra en tres principios principales:

- Hacer inventario, clasificar, y mantener los datos sensibles y los activos correspondientes.
- Implementar capacidades de protección de los datos, preventivas y de detección, a nivel de los datos.
- Reducir el valor de los datos sensibles si y cuando sean comprometidos.

Las acciones a tener en cuenta en este sentido incluyen:

- **Haga inventario y clasifique la IP en la fuente** y entre los sistemas correspondientes que almacenan y procesan la IP. Determine quién usa la IP, incluyendo otros departamentos y terceros, y valore qué tan ampliamente es distribuida.

Figura 2. Maduración del programa de seguridad cibernética

Fuente: Análisis de Deloitte

- **Implemente capacidades de protección de la IP a nivel de los datos**. Una vez que la IP sea identificada y especificada, aplique controles de seguridad a nivel de los datos mismos, ya sea que la IP sea almacenada en documentos o en bases de datos. Esos controles podrían incluir soluciones preventivas tales como administración de los derechos digitales [digital rights management (DRM)] así como también soluciones de detección tales como protección ante la pérdida de datos, gobierno del acceso a los datos, y monitoreo de la actividad de la base de datos. Desarrolle una estrategia general para proteger la IP, y seleccione herramientas que se complementen una con otras y cubran al riesgo de manera holística.

- **Reduzca el valor de los datos sensibles para los criminales cibernéticos**. Este es quizás el principio más importante en la seguridad dentro-fuera, y se basa en la premisa de que la pregunta no es "si," sino "cuándo," la IP se volverá expuesta. Una manera para reducir el valor de los datos sensibles es encriptar u oscurecer los datos para hacer que su uso sea difícil cuando sean comprometidos. Un segundo método es destruir de manera segura los datos sensibles cuando ya no sean necesarios para propósitos legítimos de carácter legal o de negocios. En todos los casos, la protección de los datos sensibles es un desafío complejo que requiere una estrategia holística y comprensiva de la protección de los datos, apoyo del ejecutivo, e inversiones en tiempo, talento, y financiación. La implementación de soluciones individuales centradas-en-los-datos de una manera aislada sin integración puede llevar a brechas críticas en la seguridad de la organización.

Estrategias adicionales que las compañías pueden emplear para proteger la IP pueden incluir:

- Implementar estrategias globales de segmentación de la red.

- Establecer orientación central sólida sobre las políticas y los procedimientos de protección de la IP.

- Monitorear continuamente las amenazas relacionadas-con-la-IP.

- Entrenar a los grupos de empleados de riesgo alto, que frecuentemente manejen IP sensible, sobre conciencia cibernética, personalizando el entrenamiento para sus roles específicos.

- Usar sitios seguros para compartir la IP cuando sea necesario – con proveedores y sub-contratistas clave, por ejemplo – en oposición a enviar fuera información de una manera descontrolada.

Las organizaciones también pueden necesitar tomar decisiones estratégicas de negocio con base en su tolerancia frente al riesgo, para los riesgos de protección de la IP, cuando evalúen los tipos de actividades de negocio que puedan o no estar dispuestas a emprender en mercados emergentes.

Talento y capital humano

Tenga un propósito al abordar los desafíos relacionados-con-el-talento

La capacidad de una organización para administrar efectiva y eficientemente al riesgo cibernético depende de su cultura. El talento puede ser el vínculo más débil en el panorama cibernético. A través de este reporte, hemos abordado las oportunidades para que los negocios de consumo administren la seguridad cibernética mediante creciente compromiso a nivel del ejecutivo, construyan confianza del cliente, salvaguarden la información intercambiada mediante productos conectados, protejan la IP, y aseguren los sistemas de pago. Pero para que sean exitosos en esas áreas, a menudo es críticamente importante tener los empleados correctos centrados en las tareas correctas para mitigar el riesgo cibernético. Para hacer eso, la organización debe tener propósito al abordar los desafíos relacionados-con-el-talento alrededor del riesgo cibernético – específicamente, mediante atraer, entrenar, y retener el talento superior para la seguridad cibernética, y mediante entregar educación frecuente sobre los nuevos enfoques para la seguridad cibernética a la luz de la naturaleza en evolución de las amenazas cibernéticas.

El 25 por ciento de quienes respondieron la encuesta citan como un desafío la carencia de talento disponible y encontrar el talento con el conjunto correcto de habilidades.

Sólo el 25 por ciento proporciona entrenamiento sobre la conciencia cibernética, dirigido a ejecutivos, empleados, y terceros proveedores, sobre una base trimestral.

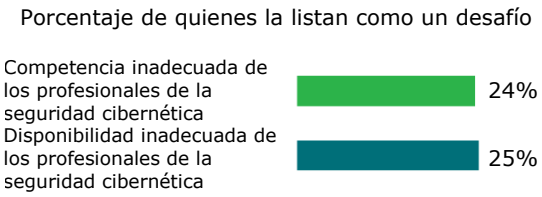
Los desafíos de atraer, entrenar, y mantener el talento para la seguridad cibernética

Atraer el talento correcto surgió como un problema en nuestra encuesta cuando preguntamos acerca de los principales desafíos de establecer y mantener un programa efectivo de seguridad cibernética (figura 13). Los negocios de consumo que entrevistamos reportaron obstáculos importantes relacionados con dos problemas: la disponibilidad de talento para la seguridad cibernética (dado que los profesionales cibernéticos son de demanda alta), y encontrar el talento con el conjunto correcto de habilidades. Los ejecutivos de seguridad cibernética con quienes hablamos expresaron frustración alrededor de reclutar talento, acertadamente expresado por un ejecutivo:

> Las compañías no pueden contratar suficiente [talento cibernético]. Es difícil escalar un equipo. Nosotros estamos buscando aumentar nuestro equipo.

Desafortunadamente, la disponibilidad es solo parte del problema. Una vez que el talento cibernético ha sido identificado y contratado, pueden surgir desafíos alrededor del entrenamiento y de retener ese talento, dado que algunos profesionales de la seguridad cibernética pueden no percibir que el entrenamiento sea de vanguardia o suficientemente desafiante. Y siempre hay el riesgo de desgaste, un problema reportado por el 16 por ciento de quienes respondieron (figura 14).

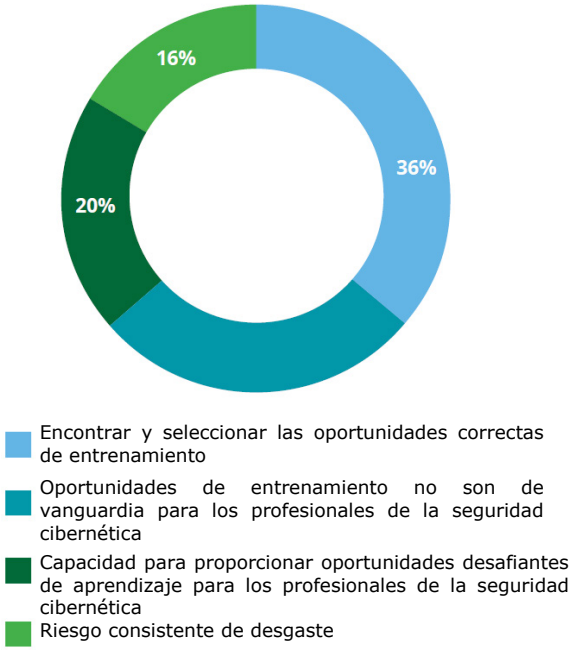
Figura 13. La brecha del talento en la seguridad cibernética



Q25. ¿Cuáles son los desafíos más importantes que su organización enfrenta para establecer/mantener un programa efectivo de seguridad cibernética?

Fuente: Análisis de Deloitte

Figura 14. Problemas en el desarrollo de talento para la seguridad cibernética



Q48. ¿Cuál es el problema más desafiante con relación al desarrollo del talento para la seguridad cibernética?

Fuente: Análisis de Deloitte
Deloitte University Press | dupress.deloitte.com

En nuestras discusiones en profundidad con ejecutivos cibernéticos, aprendimos que la dificultad para contratar y retener el talento superior a menudo está relacionada con el atractivo variante de trabajar para una compañía de tecnología versus un negocio de consumo. Dicho de manera sencilla, muchos negocios de consumo no tienen el mismo atractivo que las compañías de tecnología, las cuales tienden a ofrecer compensación más alta y oportunidades más sofisticadas de entrenamiento y aprendizaje tecnológico. A menudo, las compañías de tecnología tienen a estar localizadas en ciudades atractivas o centros de tecnología, lo cuales los profesionales más jóvenes de la seguridad cibernética encuentran especialmente atractivos. Tal y como un ejecutivo dijo:

> [Nosotros estamos en] un mercado de trabajo caliente; es muy competitivo. Yo pienso que contratar personal externo es difícil, incluso si somos una gran compañía. Puede ser que nuestra compensación no sea tan alta como la de otros. Lo que nosotros hemos hecho es agregar roles a nuestros equipos, y buscamos personas existentes en funciones relacionadas para entrenarlas mediante desarrollarlas desde el interior – tomando algunos de otras disciplinas de TI y entrenándolas. Lo cibernético es una cosa caliente, de manera que algunas personas pueden estar interesadas en entrenarse. Para nosotros, esta es una estrategia de desarrollo más segura que contratar externamente.

Las compañías de negocios de consumo reconocen la necesidad de invertir en entrenamiento y desarrollo de sus empleados. El entrenamiento del personal interno en conciencia de seguridad y riesgo cibernético probablemente debe ser una prioridad, con las compañías en nuestra encuesta calificando su nivel de maduración en esta área solo de 3.73 en una escala de cinco puntos (figura 12).

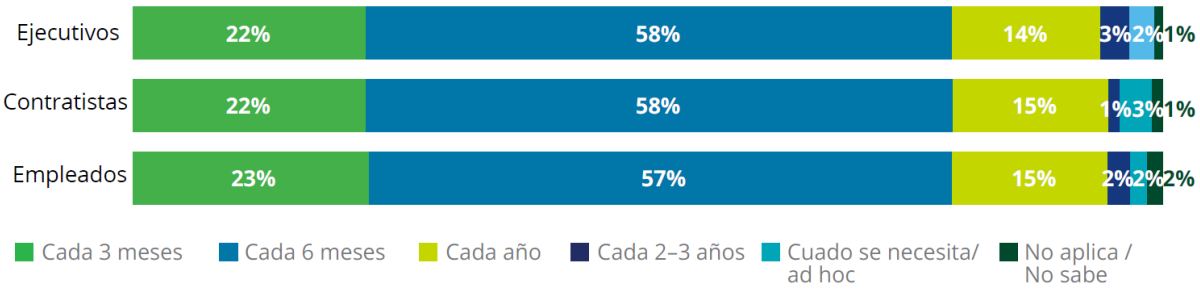
La administración de las amenazas internas a menudo es una prioridad

La amenaza que proviene de los empleados al interior de la organización también es una prioridad para muchos negocios de consumo. El daño hecho por un agente interno puede ser devastador, dependiendo de a cuál información el empleado ha tenido acceso. Reflejando esto, la administración de las amenazas internas es una de las cinco iniciativas principales de la seguridad cibernética en el 26 por ciento de los ejecutivos que participaron en nuestro estudio. Nuestras discusiones con los ejecutivos cibernéticos sugieren que muchos ejecutivos ven que las amenazas internas se deben más a menudo a error del empleado que a intención maliciosa; aun así, esas amenazas internas pueden ser tan potencialmente devastadoras como las amenazas externas. Un ejecutivo comentó:

> El error humano lleva a problemas de seguridad, de manera que tenemos que asegurar [la seguridad] alrededor de la administración del acceso a la identidad. Si las personas tienen acceso elevado que no necesitan, usted se abre ante un riesgo. De manera que hemos intentado abordar esto mediante [implementar] el monitoreo-en-red, controles de compensación para prevenir el error. Si usted tiene error humano, esos [tipos de controles] pueden reducir el riesgo.

A pesar de las preocupaciones alrededor de las amenazas internas, la frecuencia con la cual las organizaciones entrenan a contratistas, ejecutivos, y empleados en seguridad cibernética permanece relativamente baja (figura 15), apoyando nuestro punto de vista de que a menudo es el vínculo débil en el panorama de la seguridad cibernética.

Figura 15. Frecuencia del entrenamiento en seguridad cibernética recibido por empleados, ejecutivos y terceros proveedores



Fuente: Análisis de Deloitte

El empleo de terceros proveedores puede incrementar el riesgo cibernético

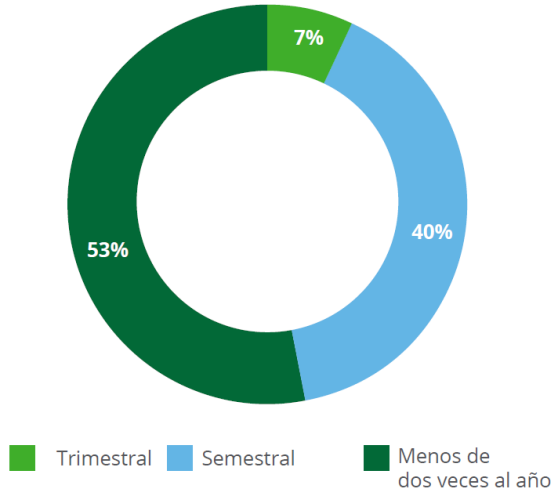
Con las dificultades que las compañías experimentan para contratar y entrenar profesionales cibernéticos internos, la tercerización con terceros proveedores puede ayudar a las compañías a integrar en sus negocios tecnologías nuevas tales como nube, pago móvil, y soluciones de comercio electrónico. Sin embargo, esto puede abrir nuevas posibilidades de riesgo cibernético si las relaciones no son administradas correctamente, desde el proceso de integración mediante valoraciones frecuentes. Esta es un área de preocupación, entonces, dado que la valoración del riesgo de terceros es infrecuente, con solo el 7 por ciento de los encuestados realizando trimestralmente valoraciones del riesgo de terceros (figura 16).

Enfoques creativos para la seguridad cibernética

Además de los esfuerzos formales de preparación centrados en la seguridad interna, las compañías comúnmente entrenan a sus empleados en cómo asegurar su información personal, con base en la racionalidad de que, si los empleados entienden las amenazas personales para sí mismos, estarán más vigilantes en el trabajo. Los temas abordados tienden a ser más básicos, pero son algunos de los fundamentos de la seguridad cibernética, tales como protección de la identidad y de las claves, uso de redes seguras de Wi-Fi, identificación y eliminación de correos electrónicos sospechosos, fraude W-2. Y uso seguro de dispositivos móviles. Tal y como un ejecutivo comentó:

> Solo hay muchas[herramientas de seguridad y entrenamiento] que lo pueden hacer. Usted puede implementar controles y procesos de IP, pero usted es solo tan exitoso como los usuarios. Son el vínculo débil. De manera que [nosotros estamos] intentando elevar la consciencia y la madurez de la base de usuarios y también trasladarla a la organización a lo largo del camino.

Figura 16. Frecuencia de las valoraciones del riesgo de terceros



Q37(c) ¿Qué tan a menudo su organización realiza una valoración del riesgo alto de terceros?

Fuente: Análisis de Deloitte

En nuestras discusiones en profundidad con ejecutivos cibernéticos, ellos hablaron acerca de eventos informales de trabajo en red a los cuales asisten con otros profesionales cibernéticos para mantenerse informados de los desarrollos en el riesgo cibernético. Muchos participantes en grupos locales de discusión de CISO comparten el aprendizaje relacionado con las violaciones cibernéticas. Las reuniones también incluyen presentaciones realizadas por invitados sobre temas clave tales como presentaciones de expertos del FBI en seguridad cibernética. Los participantes son anónimos, como también lo son los ejemplos que comparten.

Reconociendo la necesidad de desarrollar talento cibernético superior, China lanzó en septiembre de 2016 el entrenamiento del talento en seguridad cibernética a nivel de toda la nación.[16] Esto podría servir como modelo para los Estados Unidos y otros países que esperen avanzar en la administración del riesgo cibernético. Un funcionario de educación en la 4th China Internet Security Conference realizada en agosto de 2016 señaló que el país necesita al menos 500,000 expertos en seguridad cibernética, pero que solo cerca de 8,000 de tales se gradúan cada año. Las autoridades de Wuhan, la capital de la Provincia de Hubei de China, anunciaron planes tanto para doblar el número de becas para estudiantes que busquen estudiar seguridad cibernética, así como también operar reclutamiento especial para "genios disidentes," como parte del esfuerzo nacional para entrenar talento en seguridad cibernética. El gobierno de la China no solo ha establecido un innovador sistema de evaluación que prioriza el entrenamiento práctico y emprendedor, sino que también ofrece el doble de salario y de fondos de investigación para los mejores expertos en seguridad cibernética.

Libro de juegos de talento y capital humano

¿QUÉ PUEDEN LOS NEGOCIOS HACER PARA OPTIMIZAR EL TALENTO Y EL CAPITAL HUMANO?

El liderazgo puede establecer el tono desde lo alto para promover una cultura de seguridad, haciéndolo mediante compromiso proactivo, a nivel de la organización, implementando programas medibles de aprendizaje y conciencia sobre la seguridad cibernética, y fomentando comportamientos de sus empleados que protejan a la organización y a sus gentes de una violación generalizada de la seguridad. Más específicamente, esto lo puede lograr mediante:

- **Establezca una función dedicada de seguridad cibernética** liderada por el CISO con personal de seguridad cibernética calificado en funcionamiento para proteger los activos sensibles, monitorear las amenazas a la seguridad, y estar preparado para responder a las violaciones que puedan ocurrir. Desarrolle estrategias de la fuerza de trabajo de la seguridad cibernética, lo cual puede ser logrado mediante la valoración de las necesidades y brechas de habilidades de la fuerza de trabajo, reclute talento calificado para roles bien definidos de administración de la seguridad cibernética, proporcione entrenamiento especializado cuando sea necesario para mejorar adicionalmente los conjuntos de habilidades del empleado, y cree un entorno productivo, orientado-a-resultados, para retener el talento.

- **Establezca un equipo multidisciplinar de *stakeholders* clave**, que incluya tecnología de la información, tecnología de operaciones, investigación y desarrollo, finanzas, mercadeo, y riesgo. Identifique y socialice con este equipo la estructura del riesgo para definir las estrategias clave de mitigación y de manera clara identifique la propiedad para la implementación.

- **Realice pruebas internas regulares de suplantación de identidad** como una herramienta de valoración y conciencia para ayudar a los empleados a que identifiquen de mejor manera esos ataques cuando ocurran.

- **Asegure que la organización regularmente reconoce los comportamientos relacionados con el riesgo cibernético**, las tendencias y las amenazas cibernéticas para la organización.

- **Proporcione oportunidades de aprendizaje y sensibilización** en la forma de bits pequeños, frecuentes, de información al tiempo que aprovecha los múltiples canales de entrega (digital, basado en el salón de clase, y similares).

- **Estimule escenarios de amenazas de la vida real** con una sección transversal del equipo de liderazgo ejecutivo para realizar periódicamente verificaciones del conocimiento y valore la preparación de la administración para la amenaza real. Evalúe los resultados de las diversas pruebas de simulación para ganar efectividad, y para incorporar las lecciones aprendidas en los programas interactivos de conciencia y aprendizaje.

- **Desarrolle e implemente un programa comprensivo de riesgo de terceros**. A la luz de la dependencia de terceros proveedores para implementar programas avanzados de seguridad cibernética e incrementar la descentralización de las unidades de operación, es prudente obligar estándares consistentes de gobierno de los terceros. El centro de atención del compromiso de los terceros progresivamente está cambiando hacia el valor, reflejando el reconocimiento que las organizaciones hacen de la oportunidad estratégicas que los terceros pueden crear para ellas.

- **Defina por anticipado los requerimientos para los terceros proveedores de seguridad cibernética** en contratos clave, y asegure que las compañías tengan el derecho a auditar el uso de esos requerimientos.

- **Incremente la actividad de monitoreo y aseguramiento relacionada con terceros**. Los negocios de consumo se beneficiarían de programas de administración del riesgo de terceros que también ayuden a asegurar que el acceso del tercero a la red, a los sistemas, o a los datos de la compañía cumplen plenamente los requerimientos de seguridad cibernética.

- **Visite las localizaciones de los terceros** para ganar aseguramiento acerca de la administración de los terceros.

Conclusión

A TRAVÉS DE este reporte, hemos resaltado los desafíos y las potenciales oportunidades que los negocios de consumo enfrentan en relación con la seguridad cibernética. En orden a capturar el valor del negocio asociado con las tecnologías innovadoras y las iniciativas de seguridad cibernética que muchas compañías están siguiendo, los negocios deben permanecer seguros, vigilantes, y con capacidad de recuperación. Algunas ideas sobre dónde potencialmente comenzar incluyen:

- **Establezca el tono**: Establezca el correcto tono desde lo alto para la administración de la seguridad cibernética en la organización. Las iniciativas de seguridad cibernética deben ser apropiadamente respaldadas por el equipo de liderazgo y la administración a nivel ejecutivo para lograr los objetivos clave del riesgo cibernético.

- **Valore el riesgo de manera amplia**: Realice valoraciones del riesgo cibernético que cubra toda la empresa y los productos conectados. Si las valoraciones anteriores han sido realizadas, revise el alcance para confirmar que incluyó todos los riesgos posibles. Asegure que la valoración del riesgo aborde los principios alrededor de estar seguro, vigilante, y con capacidad de recuperación.

- **Socialice el perfil del riesgo**: Comparta, con el liderazgo ejecutivo, los resultados de la valoración del riesgo junto con la estrategia recomendada y la hoja de ruta. Participe en un diálogo como un equipo acerca de los impactos de negocio (incluyendo la potencial pérdida en dólares, así como también el daño a la reputación de la marca y la confianza del consumidor) de los riesgos cibernéticos clave. Para abordar esos riesgos, discuta cómo priorizar las asignaciones de recursos a través de las áreas de seguro, vigilante, y con capacidad de recuperación, acorde con la tolerancia, la postura, y las capacidades que frente al riesgo tiene su organización.

- **Construya en seguridad**: Evalúe las inversiones superiores del negocio en tecnologías emergentes y productos conectados. Confirme si esos proyectos están alineados con el programa de riesgo cibernético. Determine si el talento cibernético hace parte de los equipos del proyecto para ayudarlos a construir en la administración del riesgo cibernético y estrategias a prueba de fallos en la parte delantera.

- **Recuerde que los datos son un activo**. En los negocios de consumo, los datos son un activo estratégico; las formulaciones del producto, los datos del consumidor, y tales son valiosos para las compañías que tengan que construir relaciones con sus clientes. Esto probablemente necesita una conexión más estrecha entre el valor de negocio asociado con los datos y las estrategias para protegerlos.

- **Valore el riesgo de terceros**: Haga inventario de las relaciones con terceros que sean críticas para la misión. Evalúe las estrategias para abordar los riesgos de terceros que coincidan con esas relaciones.

- **Esté vigilante con el monitoreo**: Esté vigilante al evaluar, desarrollar, e implementar sus capacidades de monitoreo de la amenaza cibernética de su compañía. Determine si y qué tan rápidamente sería detectada una violación en áreas clave de la compañía. Recuerde extender, a los productos conectados, la detección de la amenaza cibernética.

- **Siempre esté preparado**: Incremente la capacidad de recuperación organizacional mediante centrarse en la preparación para el incidente y la violación mediante ejercicios de juegos de azar. Comprometa en esos ejercicios a TI así como también a los líderes clave del negocio.

- **Aclare las responsabilidades organizacionales**: Sea tan claro como el cristal, con el equipo de liderazgo ejecutivo, sobre las responsabilidades de la propiedad organizacional por los componentes clave del programa de riesgo cibernético. Asegure que en el equipo haya un líder claro con la responsabilidad para reunir todo.

- **Oriente la conciencia incrementada**: Asegure que los empleados son apropiadamente conscientes de sus responsabilidades para ayudar a mitigar los riesgos cibernéticos relacionados con suplantación de identidad o ingeniería social, protección de IP y datos sensibles, y patrones adecuados de escalado para reportar la actividad inusual u otras áreas de preocupación.

NOTAS FINALES

[1] Deloitte, *Cyber risk in advanced manufacturing: Getting ahead of cyber risk*, 2016, https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html#.

[2] Deloitte, "An introduction to cyber war games," *Wall Street Journal—CIO Journal*, September 22, 2014, http://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/.

[3] Deloitte, SSI, and JD Power, consumer privacy study presented at Next2017 Conference, May 9-10, 2017, New York.

[4] Zion Market Research, "Global smart home market will reach USD 53.45 billion by 2022," *Global Newswire*, January 20, 2017, https://globenewswire.com/news-release/2017/01/20/909668/0/en/Global-Smart-Home-Market-willreach-USD-53-45-Billion-by-2022-Zion-Market-Research.html.

[5] Associated Press, "U.S. warns of security flaw that could allow hackers control of heart devices," *CBS News*, January 10, 2017, http://www.cbsnews.com/news/cybersecurity-flaw-that-could-allow-hackers-control-of-heartdevices-united-states-warns/.

[6] Amy Nordrum, "Popular Internet of Things forecast of 50 billion devices by 2020 is outdated," *IEEE Spectrum*, August 18, 2016, http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.

[7] Kyle Wiggers, "Google partnered with H&M-backed fashion startup Ivyrevel to build customised 'data dresses,'" *Business Insider*, February 7, 2017, http://www.businessinsider.com/google-partners-with-hm-ivyrevel-forcoded-couture-project-2017-2?IR=T.

[8] Robert Williams and Jeremy Kahn, "Inside the retail store of the future: Online retailer Farfetch is bringing technology to the shop floor to blend internet and in-store experiences," *Bloomberg*, April 24, 2017, https://www.bloomberg.com/news/articles/2017-04-24/online-retailer-farfetch-and-the-retail-store-of-the-future.

[9] Blake Morgan, "Five easy to understand examples of The Internet of Things," *Forbes*, January 27, 2016, https://www.forbes.com/sites/blakemorgan/2016/01/27/5-easy-to-understand-examples-of-iot-and-customerexperience/#4841b95b366c.

[10] Ellie Burns, "The IoT era: A connected world where even teddy bears pose a threat," *Computer Business Review*, February 28, 2017, http://www.cbronline.com/news/cybersecurity/breaches/IoT-era-connected-world-whereeven-teddy-bears-pose-a-threat/.

[11] Zion Market Research, "Global mobile wallet market will reach USD 3,142.17 billion by 2022," *Global Newswire*, January 19, 2017, https://globenewswire.com/news-release/2017/01/19/909307/0/en/Global-Mobile-Wallet-Marketwill-reach-USD-3-142-17-billion-by-2022-Zion-Market-Research.html.

[12] Ocean Tomo, "2015 annual study of intangible asset market value," March 5, 2015.

[13] Deloitte, *Cyber risk in advanced manufacturing*.

[14] Deloitte, *Intellectual property theft expected to rise*, 2016, https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/intellectual-property-expected-to-rise-deloitte-poll.html.

[15] Deloitte, *Cyber risk in an Internet of Things world*, 2015, https://www2.deloitte.com/us/en/pages/technologymedia-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html.

[16] Cao Siqi, "China launches cyber security talent training nationwide," *Global Times*, September 20, 2016, http://www.globaltimes.cn/content/1007158.shtml.

ACERCA DE LOS AUTORES

Sean Peasley

Sean Peasley es socio de Deloitte & Touche LLP y sirve como el líder de Consumer and Industrial Products para la práctica de Cyber Risk Services. Tiene más de 30 años de experiencia en ayudar a que los clientes se vuelvan Secure.Vigilant.Resilient.™ mediante ayudar a las organizaciones a abordar los desafíos del riesgo cibernético. Está experimentado en administración del riesgo cibernético, inteligencia de amenaza cibernética, juegos de azar cibernéticos, administración de identidad y acceso, privacidad y protección de datos, y capacidad de recuperación del negocio.

Kiran Mantha

Kiran Mantha es directive en Deloitte Advisory y lidera los Cyber Risk Services para el sector de Retail and
Distribution. Con cerca de 17 años de experiencia, ayuda a las corporaciones a administrar riesgos complejos de negocios y de información. Mantha está involucrado en varios grupos de industria desde una perspectiva de eminencia y promueve la conciencia del riesgo cibernético entre minoristas.

Vikram Rao

Vikram Rao es gerente senior de Advisory Business de Deloitte con cerca de 15 años de experiencia. Es líder de la práctica de Cyber Risk Services de Deloitte, la cual ayuda a que los clientes sean Secure. Vigilant. Resilient.TM. Ha ayudado a compañías *Fortune* 100 en varios sectores de negocios de consume con la evaluación de sus riesgos cibernéticos y ha asesorado ejecutivos en estrategias de inversión para reforzar su postura ante la seguridad cibernética.

Curt Fedder

Curt Fedder es gerente senior del Deloitte Services LP's Center for Industry Insights y lidera la investigación de mercado para productos de consumo. Con experticia en investigación del consumidor, y centro de atención puesto en patrimonio de marca, satisfacción del cliente, y publicidad, Fedder ha liderado grupos de investigación del consumidor en organizaciones de productos de consumo y minoristas. Ha publicado artículos en el *Journal of Advertising Research* and *Quirks Marketing Research*, y ha realizado presentaciones en conferencias de la industria de investigación de mercado.

Marcello Gasdia

Marcello Gasdia es gerente en el Deloitte Services LP's Center for Industry Insights, y es el líder de investigación para Travel, Hospitality, and Services. Aprovecha la experiencia primaria de investigación para estudiar el comportamiento del consumidor y las tendencias del mercado a través de varios sectores de viajes – incluyendo hoteles, aerolíneas, transporte terrestre, y restaurantes.

ASISTENTES

Rob Goldberg, Directivo asesor, Deloitte & Touche LLP

Gregg Schmidtetter, Líder Consumer Products Cyber Risk Services, Deloitte & Touche LLP

Vikram Kunchala, Director administrativo asesoría, Deloitte & Touche LLP

Gina Pingitore, Director administrativo, Deloitte Center for Industry Insights

Ryan Robinson, Líder de investigación para Industrial Products and Services, Deloitte Center for Industry Insights

ACERCA DEL DELOITTE CENTER FOR INDUSTRY INSIGHTS

El Deloitte Center for Industry Insights es la division de investigación de la práctica Deloitte LLP's Consumer and Industrial Products, de Deloitte LLP. La meta del centro es informar, a los *stakeholders* a través del ecosistema de negocios de consumo y fabricación, sobre los problemas críticos de negocios, incluyendo tendencias emergentes, desafíos, y oportunidades. Usando investigación primaria y análisis riguroso, el centro proporciona perspectivas únicas y busca ser una fuente de confianza para conocimientos relevantes, oportunos, y confiables.

Para conocer más, visite www.deloitte.com/us/cb and www.deloitte.com/us/manufacturing.

AGRADECIMIENTOS

Los autores también desean dar las gracias a los siguientes profesionales que han contribuido a la publicación de este estudio:

Leslie Ament, Líder de investigación sobre minoristas, Deloitte Center for Industry Insights, Deloitte Services LP

Linda Chen, Profesional de Mercadeo estratégico, Deloitte Center for Industry Insights, Deloitte Services LP

Linda Clemmer, Líder de mercadeo de Travel, Hospitality, and Services, Deloitte Services LP

Joanna Wrobel Cullinan, Profesional asesor de Mercadeo estratégico, Deloitte Services LP

Ashley Dunham, Líder de mercadeo minorista, Deloitte Services LP

Shweta Joshi, Analista senior, Deloitte Center for Industry Insights, Deloitte Support Services India Pvt.
Ltd.

Sarah Katz, Profesional asesor de mercadeo estratégico, Deloitte Services LP

Charlie Kirby, Gerente de asesoría, Deloitte and Touche, LLP

Robert Libbey, Investigación de mercados, Deloitte Center for Industry Insights, Deloitte Services LP

Beth Ruck, Gerente senior de comunicaciones, Deloitte Services LP

Paula Spoto, Líder de mercadeo de Consumer Products, Deloitte Services LP

Jagadish Upadhyaya, Gerente asistente, Deloitte Center for Industry Insights, Deloitte Support Services
India Pvt. Ltd.

CONTACTOS

Sean Peasley
Consumer and Industrial Products leader for Cyber Risk Services
Partner
Deloitte & Touche LLP
+1 714.334.6600
speasley@deloitte.com

Kiran Mantha
Retail & Distribution leader for Cyber Risk Services
Principal
Deloitte & Touche LLP
+1.212.436.6155
kmantha@deloitte.com

Vikram Rao
Senior manager
Deloitte & Touche LLP
+1.617.437.3950
vikrao@deloitte.com

Curt Fedder
Consumer Products research leader
Deloitte Center for Industry Insights
Senior manager
Deloitte Services LP
+1.773.680.4952
cfedder@deloitte.com

Marcello Gasdia
Travel, Hospitality, and Services research leader
Deloitte Center for Industry Insights
Manager
Deloitte Services LP
+1.212.436.3839
mgasdia@deloitte.com

 Siga @DU_Press
Inscríbase en DUPress.com para las actualizaciones de Deloitte University Press.

Acerca de Deloitte University Press
Deloitte University Press publica artículos originales, reportes y publicaciones periódicas que proporcionan conocimientos para los negocios, el sector público y ONG. Nuestra meta es aprovechar la investigación y la experiencia de nuestra organización de servicios profesionales, y la de co-autores en la academia y negocios, para avanzar la conversación sobre el espectro amplio de temas de interés para ejecutivos y líderes del gobierno.

Deloitte University Press es una huella de Deloitte Development LLC.

Acerca de esta publicación

Acerca de Deloitte