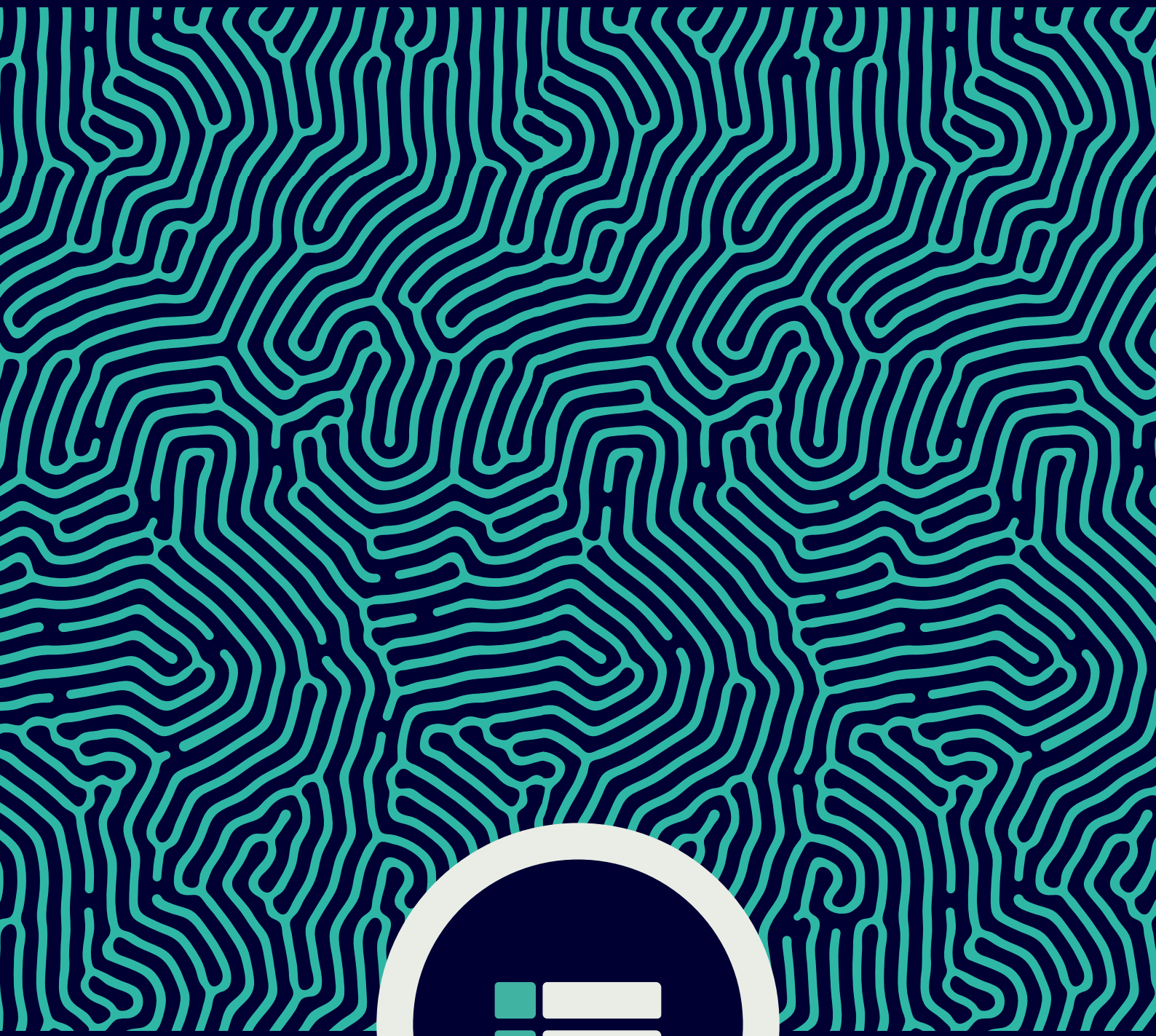
INFORME GLOBAL DE INTERNET PARA 2016



Resumen Ejecutivo

Introducción

Los casos de infracciones de datos están aumentando. Sus efectos sobre los usuarios (consumidores, empleados y organizaciones) son profundos y duraderos, y conllevan importantes costos financieros y no financieros. Lo peor es que, en muchos casos, la infracción de datos podría haberse prevenido. Y aunque este no fuera el caso, podría al menos haberse mitigado el daño.

Así que el tema central de este informe es, en cierto modo, simple.

¿Por qué las organizaciones no toman todas las medidas disponibles para proteger a quienes les confían su información personal? ¿Es porque no se hacen cargo de todos los costos de las infracciones de datos? ¿Es porque proteger mejor los datos de los usuarios no les ofrece beneficios suficientes? En ambos casos, la respuesta es afirmativa.

Si bien los usuarios corren con los costos a largo plazo de cada infracción, la más perjudicada es la confianza en Internet. Internet Society tiene la visión de que Internet es para todos, en todas partes. La confianza en Internet es la base de esa visión. Sin confianza, quienes están en línea se encuentran menos predispuestos a confiar su información personal a Internet y quienes aún no lo están tienen una razón para permanecer desconectados. La economía de Internet no crecerá tan rápido como podría hacerlo y será mucho más difícil alcanzar los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas.[1]

Con este informe, Internet Society busca incrementar el conocimiento sobre las infracciones de datos y sobre nuestra responsabilidad colectiva en lo que respecta a la protección del ecosistema de datos. Ofrecemos recomendaciones para reducir tanto la cantidad como los efectos de las infracciones de datos. El debate se centrará fundamentalmente en los usuarios, ya que son las principales víctimas. Es necesario ganar y mantener su confianza para que la promesa de Internet sea realidad para todos.

¿Qué es una infracción de datos?

"Una infracción a la seguridad que ocasiona la destrucción, pérdida, alteración, divulgación no autorizada o acceso de manera accidental o ilícita a datos personales transmitidos, almacenados o procesados de algún modo en relación con la prestación de un servicio público de comunicaciones electrónicas"

Oficina del Comisionado de Información (ICO) del Reino Unido[2]

[1] Como se ha señalado, los datos, al igual que el petróleo, tienen sus inconvenientes; en este sentido, las infracciones de datos son los nuevos derrames de petróleo. Vea el siguiente artículo de Robin Wilton, director de divulgación técnica de identidad y privacidad de Internet Society, en https://www.internetsociety.org/blog/tech-matters/2014/10/they-say-"personal-data-new-oil"-thats-good-thing.

[2] Vea https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/.

Datos y tendencias

Las infracciones de datos tienden a aumentar:

- Cada vez son más las personas afectadas por las infracciones de datos. Las infracciones informadas están aumentando: hay una creciente cantidad de registros conocidos vulnerados y una cantidad aún mayor de registros cuya cifra se desconoce. La principal causa son los ataques externos, en general, para obtener beneficios financieros. La mayoría de las filtraciones parecen ocurrir en los EE. UU., pero es probable que esto se deba a que allí existen reglas de notificación de filtraciones que conducen a la divulgación de más casos.

- Las encuestas aún no indican que las filtraciones de datos informadas repercutan significativamente en la predisposición a conectarse de las personas que aún no son usuarias de Internet. Sin embargo, a medida que crece la cantidad de usuarios afectados, por ejemplo, por robos de identidad con ánimo de lucro, son más los usuarios que dudan en utilizar servicios en línea que requieran información personal. Los usuarios también pueden dejar de hacer negocios con una compañía que ha sufrido una infracción de datos. A su vez, la creciente falta de confianza entre los usuarios podría ser una buena excusa para impedir que quienes aún no usan Internet decidan conectarse.

- Las organizaciones están gastando más en prevención, pero esto aún no ha disminuido perceptiblemente la cantidad de infracciones ni el impacto y el costo de las que se producen. Por otra parte, el costo de las infracciones, cuando se calcula, generalmente incluye solo el costo para la organización y no tiene en cuenta el costo que implica para los usuarios, que son las principales víctimas.

Estas tendencias no pueden continuar sin dañar significativamente la privacidad de los individuos y la confianza de los usuarios en Internet, con la consecuencia de un uso más selectivo de Internet.

Estudios de casos prácticos

El informe destaca algunas de las principales causas de las infracciones de datos y sus efectos sobre las organizaciones y los usuarios. Las cifras son abrumadoras: a Target le robaron los números de tarjetas de crédito de 40 millones de clientes y los ofrecieron a la venta en línea; a Ashley Madison le quitaron los registros de las aventuras personales de 37 millones de usuarios casados y los publicaron en línea; y a la Oficina de Gestión de Personal (OPM) de Estados Unidos le robaron los registros de 21,5 millones de exempleados, empleados y posibles empleados.

El efecto de estas infracciones sobre consumidores, usuarios, empleados y terceros que ni siquiera sabían que estas organizaciones tenían sus datos es profundo y duradero. Algunos usuarios perdieron tiempo y dinero en proteger sus finanzas y su identidad contra los robos, algunos vieron desmoronarse sus matrimonios y hasta cometieron suicidio, y otros pueden ser objeto de chantajes y quedar expuestos.

Los casos de estudio muestran lo sencillos que son algunos ataques, pero también lo difícil que es para las organizaciones protegerse de todas las amenazas. Para los usuarios, los casos de estudio ponen de relieve la creciente sensación de inseguridad en línea, donde deben depositar su confianza en organizaciones cuya seguridad no pueden evaluar. Cada vez es mayor la cantidad de usuarios afectados de manera directa o indirecta por una infracción de datos. Los casos de estudio especifican el efecto real y final que estas infracciones tienen sobre los usuarios que ven defraudada la confianza depositada, como consumidores o como empleados, en las organizaciones.

Problemas

Frente a los costos financieros y no financieros que ponen de relieve los casos de estudio y los datos, es desconcertante que muchas de las infracciones hayan aprovechado vulnerabilidades conocidas y fueran evitables. En algunos casos, había parches disponibles que no se utilizaron. Algunos ataques se perpetraron mediante ingeniería social, es decir, los empleados fueron engañados para ceder su contraseña o introducir una infección, generalmente de maneras que podrían haberse prevenido.

Por supuesto, no todas las infracciones se deben a ataques ni todos los ataques son prevenibles. Algunos utilizan vulnerabilidades de día cero que antes de su empleo no se conocían. Otros se deben a la divulgación accidental de datos, por ejemplo, cuando se pierde un dispositivo que contiene datos confidenciales. Aunque no son prevenibles, estas infracciones son al menos previsibles, dada la frecuencia con que ocurren. Es posible mitigar sus efectos, minimizando la cantidad de datos recopilados y cifrando los datos que se almacenan y se envían.

Queda pendiente responder por qué, dado el costo de las infracciones, las organizaciones no hacen más por abordar las prevenibles y disminuir el costo y los efectos de las previsibles. Esto nos lleva a la cuestión de la economía de la confianza.

La inversión en ciberseguridad está regida por una deficiencia del mercado. En primer lugar, las infracciones de datos tienen externalidades; costos que las organizaciones no tienen en cuenta. En segundo lugar, aún en los casos en que se realizan inversiones, debido a las asimetrías en la información, las organizaciones tienen dificultades para transmitir el nivel de ciberseguridad resultante al resto del ecosistema. En consecuencia, el incentivo de invertir en ciberseguridad es limitado; las organizaciones no se hacen cargo de todos los costos de la falta de inversión y no pueden beneficiarse por haber invertido.

La organización que sufre una infracción no corre con todos los costos. El costo que enfrentan otros es una externalidad que no se tiene necesariamente en cuenta a la hora de tomar decisiones relativas a la protección contra las infracciones de datos. Además, el peso de las infracciones de datos afecta la confianza futura, que es una externalidad y, desde una perspectiva económica, no existe un motivo racional para que las organizaciones lo tengan en cuenta. Sin embargo, no es un efecto que la sociedad pueda ignorar.

Los actores no tienen información completa acerca de los riesgos que pueden enfrentar en línea, lo que les dificulta tomar decisiones fundamentadas. Concretamente, es difícil que las organizaciones se beneficien al dar los pasos adecuados para evitar las infracciones de datos porque no pueden transmitirles a sus clientes cuál es su nivel de seguridad de datos. Esto limita el incentivo a la inversión en seguridad de datos.

Recomendaciones

El informe destaca cinco recomendaciones para abordar los asuntos relacionados con los aspectos económicos de las infracciones de datos.

R1 Colocar a los usuarios en el centro de las soluciones; e incluir tanto a usuarios como a organizaciones al evaluar los costos de las infracciones de datos.

R2 Aumentar la transparencia a través de la divulgación y la notificación de las infracciones de datos.

R3 La seguridad de los datos debe ser una prioridad. Deben ponerse a disposición mejores herramientas y enfoques. Cuando se trata de seguridad, las organizaciones deben ajustarse a normas basadas en las prácticas recomendadas.

R4 Las organizaciones deben ser responsables de sus infracciones. Se deben establecer de antemano reglas generales respecto a la asignación de obligaciones y reparaciones en caso de infracción de datos.

R5 Aumentar los incentivos a la inversión en seguridad catalizando un mercado para la evaluación confiable e independiente de las medidas de protección de los datos.

La *primera recomendación* es poner a los usuarios en el centro de las soluciones. Para implementar este enfoque centrado en el usuario, la *segunda recomendación* es crear mayor transparencia respecto al riesgo, la incidencia y el impacto de las infracciones de datos a nivel global.

El mayor conocimiento trae aparejado un aumento en la demanda de mejores herramientas. La *tercera recomendación* es que la seguridad de los datos debe ser una prioridad. Deben ponerse a disposición mejores herramientas y enfoques. Las organizaciones deben ajustarse a normas basadas en prácticas recomendadas.

- **Prevención.** Para evitar las vulnerabilidades conocidas, las herramientas de seguridad (y los parches de seguridad críticos) deben ser más fáciles de utilizar y actualizar. Para prevenir los ataques de ingeniería social, las organizaciones deben aplicar herramientas de confianza y prácticas recomendadas para bloquear los correos electrónicos de suplantación de identidad (*phishing*) y el software malicioso incrustado, y deben capacitar a los empleados para ayudarlos a evitar estos ataques.

- **Mitigación.** Las organizaciones deben recopilar la mínima cantidad de datos necesarios para prestar sus servicios y preservar los derechos y las expectativas de los individuos. Las organizaciones también deben cifrar los datos recopilados y almacenados que se encuentran en tránsito y en reposo. El cifrado debe ser fácil de utilizar e, idealmente, debe implementarse de manera predeterminada, en especial para los individuos.

Por supuesto, independientemente de lo sencillas que puedan volverse las herramientas, su implementación sigue requiriendo tiempo y dinero, y no todas las organizaciones están dispuestas a gastar para prevenir las infracciones de datos y mitigar el impacto de las que no pueden prevenirse. Las últimas dos recomendaciones se centran en cómo abordar estas deficiencias del mercado a través de incentivos económicos relacionados tanto con los costos como con los beneficios.

- *Cuarta recomendación.* Mayor responsabilidad. Al atribuir una mayor proporción de las externalidades de las infracciones de datos a las organizaciones que tienen los datos, sus costos aumentarán y deberán esforzarse más por prevenirlas y mitigar sus efectos.

- *Quinta recomendación.* Señales de seguridad. Al permitir que las organizaciones señalen que son menos vulnerables y, de este modo, reducir la asimetría de la información, las organizaciones podrán competir mejor por los negocios y aumentará el beneficio de invertir en la prevención de las infracciones de datos.

Las cinco recomendaciones están resumidas en el círculo de la seguridad.

Estas cinco recomendaciones se basan en dos principios importantes: administración de los datos y responsabilidad colectiva.

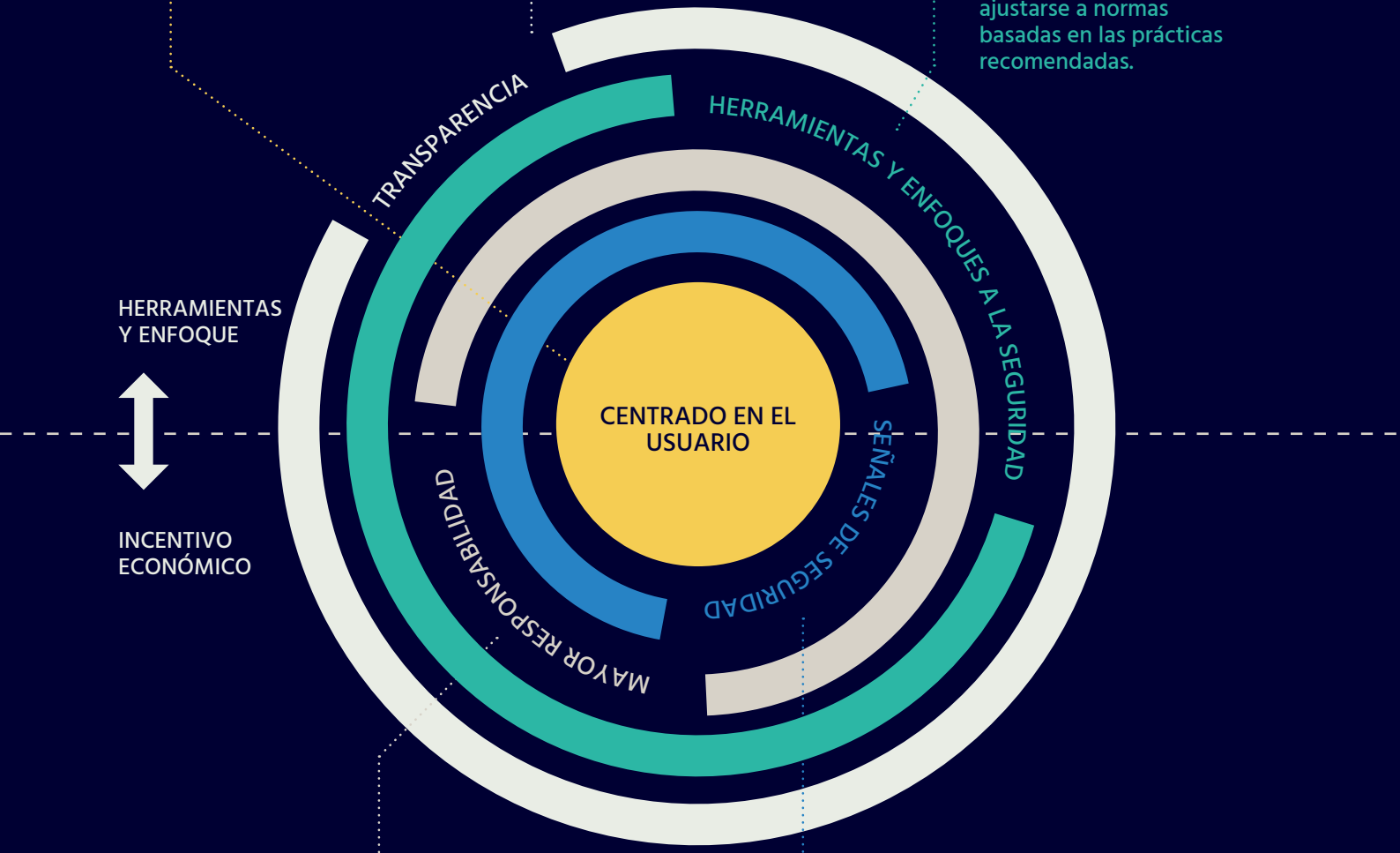
Administración de los datos. Las organizaciones deben verse a sí mismas como custodias de los datos de sus usuarios, y protegerlos no solo como una necesidad empresarial sino también en nombre de los propios individuos. Las organizaciones deben adoptar un enfoque ético para el manejo de los datos y comprender que pueden prosperar haciendo el bien: proteger a los usuarios debe ser una meta por mérito propio, que además protege a la organización.

Círculo de la seguridad

1. Colocar a los usuarios en el centro de las soluciones; al evaluar los costos de las infracciones de datos, incluir tanto a usuarios como a organizaciones.

2. Aumentar la transparencia a través de la divulgación y la notificación de las infracciones de datos.

3. La seguridad de los datos debe ser una prioridad. Deben ponerse a disposición mejores herramientas y enfoques. Cuando se trata de seguridad, las organizaciones deben ajustarse a normas basadas en las prácticas recomendadas.



4. Las organizaciones deben ser responsables de sus infracciones. Se deben establecer de antemano reglas generales respecto a la asignación de obligaciones y reparaciones en caso de infracción de datos.

5. Aumentar los incentivos a la inversión en seguridad catalizando un mercado para la evaluación confiable e independiente de las medidas de protección de los datos.

Responsabilidad colectiva. En Internet, todos están conectados. Una infracción puede conducir a otra (en otras palabras, "su infracción podría ser la mía"). Las organizaciones tienen la responsabilidad de proteger los datos que están en su poder. También comparten la responsabilidad colectiva de proteger el ecosistema de datos como un todo con otros actores, incluidos proveedores, empleados, gobiernos, entre otros. Si alguno de estos eslabones no funciona, podría romperse toda la cadena de confianza.

En resumen, nuestro mensaje para las organizaciones es:

- Los datos personales son preciosos y preciados. ¡Protéjanlos!
- Recopilen únicamente los datos que sean absolutamente necesarios y cifren los que conserven.
- Restrinjan el acceso a los datos a quienes necesitan conocerlos.
- Señalen el nivel de seguridad que proporcionan.
- Destruyan los datos cuando ya no se utilicen.
- Sean más transparentes respecto a los incidentes de infracción de datos.
- Estén alerta a las infracciones; prepárense, notifiquen y actúen de inmediato.

Conclusión

Las infracciones de datos son una preocupación creciente en todo el mundo. Para mitigar este problema y su efecto económico, el informe propone cambiar el abordaje de las infracciones de datos y hacer participar a todos los actores.

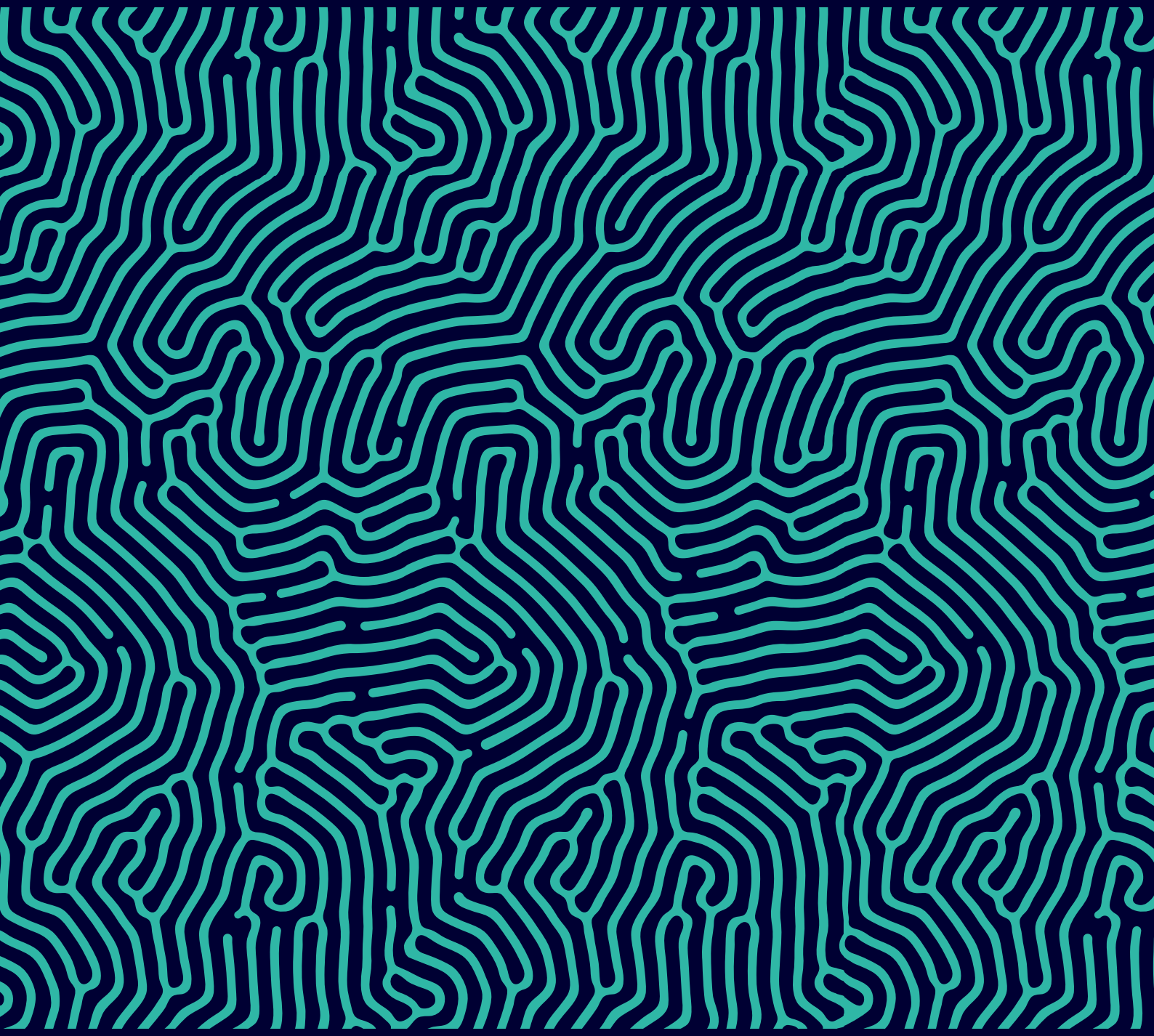
A medida que los usuarios trasladan su vida a las redes, es necesario ganar su confianza para hacer realidad todos los beneficios de Internet en todo el mundo. Esa confianza depende de cómo se protegen los datos de los usuarios contra las infracciones. Cada infracción de datos crea un nuevo grupo de usuarios que cuya confianza puede haber sido traicionada; esta situación se difunde oralmente entre las personas conocidas y más ampliamente a través de la prensa, lo que genera dudas y socava la confianza de los usuarios en general.

Con este informe, Internet Society se propone ofrecer recomendaciones que ayuden a proporcionar una mejor seguridad de datos. Esto, a su vez, tiene el potencial de aumentar el uso de Internet y de elevar el impacto económico y social de Internet en la economía y la sociedad general. En definitiva, esto ayudará a hacer realidad la visión de Internet Society de que Internet es para todos, en todas partes.

Internet de las cosas

Ante la perspectiva de un mundo donde la Internet de las cosas (IoT) esté omnipresente, las vulnerabilidades que ocasionan infracciones de datos también pueden aplicarse a los dispositivos IoT, tal vez con un impacto aún mayor sobre los usuarios. En primer lugar, los dispositivos conectados, como monitores de niños, pueden contener sensores, incluso para video y audio, que pueden ofrecer información acerca de sus propietarios. Sin embargo, más allá de las infracciones de datos, las personas pueden poner su seguridad personal bajo el control de dispositivos conectados, como dispositivos médicos o vehículos conectados. El robo y la venta de los expedientes médicos generan una angustia increíble. Pero la piratería y la anulación de los dispositivos médicos personales son potencialmente fatales.

En general, muchas de nuestras recomendaciones son válidas para prevenir o mitigar las infracciones en toda la gama de dispositivos IoT, no solo para proteger los datos que recopilan con sus sensores sino también para abordar aquellas infracciones que podrían acarrear riesgos para la seguridad personal o pública. Por lo tanto, Internet Society alienta la aplicación de estos hallazgos a todos los asuntos relevantes derivados de la incipiente IoT. Aunque es un tema que va mucho más allá de las infracciones de datos, las causas pueden ser similares y es preciso considerarlas como cuestión prioritaria al abordar la seguridad general de estos dispositivos.



Internet Society