HARVARD | BUSINESS | SCHOOL

9-117-027

REV: 1 0 DE ENERO DE 2 01 9

SOBRE AJ SRINIV COMO UN

LINDA NN PAI NO

NEGRO RAJ Gol

Violación cibernética en Target

En noviembre de 2013, Target Corporation fue objeto de uno de los mayores ciberataques de la historia. En vísperas de Navidad, la temporada más activa del año para el sector minorista, los piratas informáticos robaron información de tarjetas de crédito y débito de 40 millones de clientes de Target y nombres, así como direcciones de correo electrónico y domicilio de otros 70 millones. El ataque y la respuesta de Target expusieron a la empresa a intensas críticas y plantearon preguntas sobre la rendición de cuentas de la junta directiva de Target y del Comité de Auditoría y del Comité de Responsabilidad Corporativa, responsables de la supervisión de los riesgos operativos y de reputación. La firma líder en asesoramiento sobre representación, Institutional Shareholder Services (ISS), recomendó que los accionistas de Target votaran en contra de la reelección de 7 de los 10 miembros de la junta directiva de Target, incluido el presidente del Comité de Auditoría. Los inversores presentaron demandas derivadas acusando a la junta directiva de incumplimiento del deber fiduciario y de desperdicio de activos corporativos, de falta de diligencia en la protección de información confidencial de los clientes y de no supervisar los riesgos para el valor de la marca. Aunque el directorio de Target defendió vigorosamente su desempeño, los observadores se preguntaron hasta qué punto debía rendir cuentas el directorio por una violación de tan gran magnitud.

Antecedentes de la empresa

Los orígenes de Target se remontan a la fundación de una tienda departamental en Minneapolis por parte de George Dayton en 1902. En 1909, Dayton abrió una tienda de descuento, centrándose en los clientes que no podían permitirse pagar los precios más elevados de la tienda departamental.[1]En la década de 1950, las tiendas de descuento comenzaron a ganar participación de mercado a los grandes almacenes al ofrecer productos de marca y calidad a precios más bajos. En 1962, la Dayton Company abrió sus tiendas de descuento con la marca Target al mismo tiempo que Sam Walton fundaba Walmart y Sebastian Kresge iniciaba Kmart. Target creó su imagen de marca única vendiendo productos de calidad a precios bajos en un entorno de lujo, cuando sus competidores se centraban en vender productos lo más baratos posible. Antes de la apertura de Target, Douglas Dayton había declarado en 1961: "[Target] combinará lo mejor del mundo de la moda con lo mejor del mundo de los descuentos, una tienda de calidad con productos de calidad a precios de descuento y un supermercado de descuento... una tienda en la que pueda estar orgulloso de comprar, una tienda en la que pueda confiar, una tienda en la que sea divertido comprar y emocionante visitarla".[2]

Target adoptó este enfoque como la tienda que ofrecía a los consumidores comunes productos de alta calidad a precios de tienda de descuento, plasmados en su eslogan, "Pague menos, espere más", publicitado por primera vez en 1994.[3]Este espíritu permitió a Target diferenciarse de competidores como Walmart. Target apeló a las últimas novedades

Los profesores Suraj Srinivasan y Lynn Paine y el investigador asociado Neeraj Goyal prepararon este caso. Este caso se desarrolló a partir de fuentes publicadas. La financiación para el desarrollo de este caso fue proporcionada por la Escuela de Negocios de Harvard y no por la empresa. Los casos de HBS se desarrollan únicamente como base para el debate en clase. Los casos no tienen como objetivo servir como avales, fuentes de datos primarios o ilustraciones de gestión eficaz o ineficaz.

gustos de los consumidores ofreciendo nuevas modas y tendencias frescas e incluso colaboró con marcas de diseñadores como Maternity, Jason Wu y Liz Lange.[4]

En 2004, Dayton Company vendió sus tiendas Mervyn's y Marshall Field's y se centró exclusivamente en Target, que representaba casi el 80% de las ventas de la empresa matriz.[5]Durante el año fiscal 2013, Target tuvo ingresos de más de 72 mil millones de dólares, lo que refleja una tasa de crecimiento anual compuesta del 2,8% respecto de los cinco años anteriores.[6](Ver **Anexos 1–3** (Para conocer los estados financieros recientes y el desempeño de las acciones de Target). En noviembre de 2013, Target operaba 1.919 tiendas, 1.797 en los EE. UU. y 122 en Canadá, lo que representa más de 254 millones de pies cuadrados de venta minorista. Target competía con los minoristas estadounidenses más grandes, como Walmart, Sears, y Kohl's.[7,8] Incluso esto Target estaba orgullosa de su ciudadanía corporativa. En cada comunicado de prensa financiero de 2013 se afirmaba: "Desde 1946, Target ha donado el 5 por ciento de sus ganancias a programas y subvenciones comunitarias; hoy, esa donación equivale a más de 4 millones de dólares por semana".[9]

Una tienda Target típica tenía alrededor de 80.000 unidades de mantenimiento de existencias (SKU)[a] ofreciendo una amplia variedad de productos electrónicos, productos para el hogar, ropa e incluso comestibles en sus sucursales SuperTarget.[10]Target también ofreció a sus clientes crédito a través de su programa REDcard. Como ocurre con todos los minoristas, la temporada de compras del Día de Acción de Gracias a Navidad fue el período de mayor actividad para Target; para la temporada navideña de 2013, la empresa había aumentado su plantilla en 50.000 personas, frente a su base habitual de alrededor de 366.000.[11,12]Cada año entre 2010 y 2013, la empresa obtuvo alrededor del 30% de sus ingresos en el cuarto trimestre.[13]

Los piratas informáticos atacan el objetivo

En septiembre de 2013, piratas informáticos de una ubicación desconocida iniciaron una campaña de correo electrónico de phishing.[b] contra uno de los proveedores de calefacción y ventilación externa de Target, Fazio Mechanical Services.[14,15]La información sobre los proveedores de Target estaba disponible públicamente en línea y, por lo tanto, era accesible para cualquiera que la buscara. Cuando un empleado de Fazio abrió el correo electrónico malicioso, los piratas informáticos pudieron robar todas las contraseñas de Fazio.[16] El principal método de Fazio para detectar malware era una versión gratuita de un producto de seguridad llamado "Malwarebytes Anti-Malware", cuya licencia prohibía explícitamente su uso por parte de empresas. Pero Fazio lo había utilizado de todos modos y Target no supervisaba las medidas de seguridad del proveedor. Además, ese mismo mes, el equipo de seguridad de Target identificó vulnerabilidades en los sistemas de tarjetas de pago y cajas registradoras de la empresa, pero los funcionarios de Target no realizaron ni ordenaron más investigaciones.[17]

El 15 de noviembre de 2013, utilizando las credenciales de Fazio, los piratas informáticos obtuvieron acceso a la red de Target para facturación electrónica, gestión de proyectos y presentación de contratos.[18]Para evitar tal intrusión, Target podría haber exigido una autenticación de dos factores (una contraseña normal, mejorada con un código de verificación enviado al teléfono móvil del vendedor), que era un estándar de la industria de tarjetas de pago (PCI) para el acceso remoto por parte de terceros, pero Target no lo exigía.[19,20]Según un analista de la industria que gestionó algunas de las relaciones con proveedores de Target:[21]

> Solo los proveedores del grupo de mayor seguridad (aquellos que deben acceder directamente a la información confidencial) recibirían un token, y las instrucciones sobre cómo acceder a esa parte de la red. Target habría prestado muy poca atención a proveedores como

a Un SKU identifica cada artículo distinto ofrecido en el catálogo de productos de un minorista y puede variar según el fabricante, el material, el tamaño, el color y otras características.

b Las campañas de correo electrónico de phishing son intentos de los estafadores de Internet de obtener información personal confidencial, como nombres de usuario y contraseñas, información de tarjetas de crédito y otros datos, mediante el envío de correos electrónicos con enlaces maliciosos. Estos correos electrónicos suelen pedir a los usuarios desprevenidos que visiten un sitio web fraudulento e ingresen información en un sitio web aparentemente apropiado, pero permiten a los estafadores robar y hacer un uso indebido de los datos recopilados.

> Fazio, y a mí me sorprendería mucho que alguna vez Target hiciera una evaluación de seguridad básica de ese tipo de proveedores.

Además, como la red de Target no estaba segmentada adecuadamente, los piratas informáticos obtuvieron acceso a pagos confidenciales y datos personales de clientes.[22] Según un experto del sector, "nunca debería existir una ruta entre una red para un contratista externo (como Fazio) y la red para los datos de pago. En el caso de Target, la había y los piratas informáticos la encontraron y la explotaron".[23]

Según los investigadores, el ataque comenzó en un pequeño número de sistemas de punto de venta (POS) entre el 15 y el 28 de noviembre, en vísperas de la temporada de compras navideñas más activa para los minoristas estadounidenses. Para el 30 de noviembre, la mayoría del sistema POS de Target se había visto afectado. Los piratas informáticos instalaron malware[c] llamado "Citadel" en sistemas POS específicos en las tiendas minoristas de Target.[24,25] Una vez que los piratas informáticos instalaron el malware, utilizaron un método de ataque de "extracción de RAM";[d] Esto permitió a los piratas informáticos recopilar datos cifrados a medida que pasaban de los sistemas POS a los proveedores de procesamiento de pagos Visa y MasterCard.[26] El malware recopilaba información de tarjetas de crédito y débito cifrada en las bandas magnéticas de las tarjetas cada vez que un cliente las pasaba por la tienda.[27]

El diseño de la red de Target permitió a los piratas informáticos moverse por las redes internas de Target e incluso actualizar el malware para otra ola de ataques.[28] Según un informe de seguridad, "los atacantes habrían instalado primero tres variantes de este malware el 30 de noviembre y lo actualizaron dos veces más, justo antes de la medianoche del 2 de diciembre y justo después de la medianoche del 3 de diciembre".[29] El 2 de diciembre y durante las siguientes dos semanas, el malware comenzó a exportar los datos recopilados a través de otro servidor Target comprometido, a un servidor externo ubicado en Rusia.[30] (Referirse a **Anexo 4** (para una cronología del ciberataque).

En total, los piratas informáticos reunieron 11 gigabytes (GB) de datos robados, lo que representa alrededor de 40 millones de cuentas de tarjetas de débito y crédito.[mi] y podrían venderse en el mercado negro por hasta 100 dólares por número de tarjeta de crédito o débito.[31,32,33] Según las demandas presentadas por los clientes afectados, "el 11 de diciembre, una semana después de que los piratas informáticos violaran los sistemas de Target, Easy Solutions, una empresa que rastrea el fraude, notó un aumento de diez a veinte veces en el número de tarjetas de alto valor robadas en sitios web del mercado negro, de casi todos los bancos y cooperativas de crédito".[34]

Advertencias de seguridad ignoradas inicialmente

Target encargó la supervisión de su ciberseguridad a FireEye, Inc., una empresa que proporcionaba herramientas de detección de malware y un equipo de especialistas en seguridad en Bangalore, India. Estos especialistas en seguridad debían supervisar los sistemas de Target las 24 horas del día.[35] El equipo de FireEye inicialmente lanzó una alerta de ataque justo después del Viernes Negro.[f] Temporada de compras, el 30 de noviembre.[36,37,38] El equipo de FireEye en India envió una alerta electrónica al equipo de seguridad interno de Target en Minnesota indicando que el

---

c El malware (o "software malicioso") es cualquier programa o archivo que sea dañino para el usuario de una computadora. Esto incluye virus informáticos, gusanos, caballos de Troya y también spyware, programación que recopila información sobre el usuario de una computadora sin permiso.

El malware de extracción de memoria o RAM scraping tiene como objetivo los datos cifrados en la memoria del sistema informático, donde los datos están en formato de texto simple. Según los expertos en seguridad, para procesar datos o códigos, la información debe descifrarse en la memoria, lo que hace que el sistema sea vulnerable. El malware de extracción de memoria RAM intercepta los datos cuando el código ve 16 caracteres que terminan en un cero o un carácter especial, como es el caso de los datos de tarjetas de crédito.

Posteriormente, Target revisó sus estimaciones de clientes afectados de 70 millones a 110 millones, e incluyó otros tipos de datos como direcciones postales y de correo electrónico y números de teléfono, datos que Target había recopilado a lo largo del tiempo.

El Viernes Negro es el viernes después del Día de Acción de Gracias (el Día de Acción de Gracias es el cuarto jueves de noviembre) y marca el comienzo del período de compras navideñas en los EE. UU. En la década de 2000, se volvió cada vez más común que los minoristas estadounidenses abrieran más temprano en el día, a las 5 o 6 a. m. el Viernes Negro, y en 2014, Target abrió sus puertas a las 6 p. m. el jueves de Acción de Gracias.

El software de monitoreo había detectado intrusiones de malware pero la instalación aún no se había activado. Sin embargo, el equipo estadounidense no respondió a la alerta. Según la investigación posterior, el equipo estadounidense podría haber visto la alerta de FireEye como un falso positivo, ya que se estaban generando múltiples alertas con nombres genéricos como "malware.binary".[39]

Una vez que el malware comenzó a extraer datos de los piratas informáticos el 2 de diciembre, el equipo de seguridad en India alertó nuevamente al equipo de seguridad de Target en Minneapolis, pero no obtuvo respuesta.[40,41]Del 2 al 15 de diciembre, los piratas informáticos recopilaron datos de tarjetas de crédito de los clientes en tiempo real. Cada vez que un cliente pasaba una tarjeta por la caja registradora, los datos financieros vinculados a la tarjeta se enviaban a uno de los tres "puntos de almacenamiento" creados dentro de las redes de Target. Para evitar que saltaran las alarmas, los datos se almacenaban en las redes de Target durante seis días y luego se transmitían a través de una serie de servidores falsos antes de ser enviados a los servidores personales de los piratas informáticos.

Según dos expertos que auditaron la brecha, "la brecha podría haberse detenido allí sin intervención humana. El sistema tiene una opción para eliminar automáticamente el malware cuando se detecta. El equipo de seguridad de Target desactivó esa función".[42]No estaba claro por qué se creó esta función.
apagado. (Consulte**Anexo 5**para una representación gráfica de las oportunidades perdidas de Target, y **Anexo 6**(para un resumen del análisis realizado por un subcomité del Senado de EE. UU. sobre la violación de datos de Target).

Antes del ataque, las funciones de seguridad de la información estaban divididas entre el Director Financiero, el Director de Información y el Asesor Jurídico General (consulte**Anexo 7**Beth Jacob era la directora de información de Target durante el ataque y supervisaba equipos en India y Estados Unidos.[43]Aunque el ciberataque a través del sistema POS no estaba necesariamente bajo la responsabilidad directa del CIO, según los analistas, detectar la violación parecía caer dentro de las responsabilidades del CIO.[44]

Target descubre la brecha (semana del 12 al 19 de diciembre)

El 12 de diciembre de 2013, el Departamento de Justicia de EE. UU. (DOJ) se comunicó con Target para informarle sobre la violación, lo que hizo que el equipo ejecutivo estadounidense de la empresa fuera consciente de su gravedad.[45]Ese mismo día, JP Morgan Chase comenzó a alertar a las compañías de tarjetas de crédito sobre un patrón de cargos fraudulentos con tarjetas de crédito iniciados en Target.[46]
Al día siguiente, los ejecutivos de Target se reunieron con el Departamento de Justicia y el Servicio Secreto de Estados Unidos, y el 14 de diciembre, Target contrató a un equipo forense externo para investigar la violación.[47]

En una entrevista posterior con CNBC, el director ejecutivo de Target, Gregg Steinhafel, explicó que se enteró de la violación de datos la mañana del 15 de diciembre, después de que el equipo de seguridad interna confirmara el ataque. El 15 de diciembre, Target comenzó a eliminar el malware de sus sistemas y los atacantes comenzaron a perder el acceso a la red de Target, pero Target quería evitar interrupciones en las operaciones de las tiendas y no cerró sus tiendas.[48]La empresa tardó hasta las 6 de la tarde del 15 de diciembre en eliminar el malware.[g,49]El día 16[El]Target inició una investigación y comenzó el trabajo forense, y el 17 de diciembre, la compañía comenzó a preparar sus tiendas y centros de llamadas para responder las preguntas de los clientes.[50]

La primera indicación pública de la violación se produjo el 18 de diciembre, desde*Krebs sobre seguridad*, un popular blog de seguridad en línea dirigido por David Krebs.[51,52]Fuentes de las empresas emisoras de tarjetas de crédito informaron a Krebs que la violación de seguridad se extendió a casi todas las sucursales de Target en los EE. UU. y se produjo desde el Día de Acción de Gracias hasta el 15 de diciembre. No estaba claro si los clientes en línea se habían visto afectados. Krebs informó que más de un millón de tarjetas se habían visto comprometidas y advirtió que si los piratas informáticos lograban robar los datos PIN de las tarjetas de débito,

g El 15 de diciembre, Target eliminó la mayor parte del malware de sus redes. Sin embargo, se robaron los datos de las tarjetas de otros 56 clientes que compraron en Target el 16 y el 17 de diciembre, ya que un pequeño número de sistemas POS que se habían desconectado de la red durante la limpieza inicial seguían infectados hasta entonces.

Potencialmente podrían robar dinero directamente de las cuentas de los clientes y de los cajeros automáticos.[53]Los medios de comunicación se hicieron eco de la noticia y obtuvieron la confirmación del Servicio Secreto de que estaba investigando el incidente. Un medio de comunicación, citando a una fuente anónima, afirmó: "Cuando todo esté dicho y hecho, este caso se pondrá a la altura de algunas de las mayores infracciones de seguridad en el comercio minorista hasta la fecha".[54]Target se negó a confirmar el incidente ese día.

Target anuncia la violación

El 19 de diciembre, una semana después de que el Departamento de Justicia se puso en contacto con ellos por primera vez, Target publicó en su sitio web corporativo (y no en el sitio web para consumidores más frecuentado) y distribuyó a través de los medios de comunicación habituales un comunicado de prensa en el que afirmaba que estaba "al tanto" de un acceso no autorizado a los datos de las tarjetas de pago.[55]El comunicado de prensa explicó que entre el 27 de noviembre y el 15 de diciembre de 2013, aproximadamente 40 millones de cuentas de tarjetas de crédito y débito pertenecientes a clientes de Target se vieron afectadas.[56]"Target alertó a las autoridades e instituciones financieras inmediatamente después de tener conocimiento del acceso no autorizado y está poniendo todos los recursos apropiados para respaldar estos esfuerzos", afirma el comunicado de prensa.[57]

Los clientes de Target comenzaron a notar inmediatamente transacciones fraudulentas en sus cuentas. Un cliente afirmó: "Efectivamente, había cargos de varios minoristas en línea que ni yo ni mi esposo habíamos realizado".[58]Otro cliente llamó a la línea directa de Target "al menos 40 veces" el 20 de diciembre, el día después del anuncio, y "cuando finalmente logró comunicarse, el mensaje pregrabado la remitió a una dirección web: http... barra, barra... y así sucesivamente". Los clientes se quejaron del mal servicio cuando intentaron recabar más información sobre la violación de seguridad y cómo podría afectarles.[59]
A los clientes les resultó difícil navegar por el sitio web de Target y la falta de información los dejó mal preparados para planificar.[60]

El 20 de diciembre, el director ejecutivo Steinhafel explicó en una carta publicada en el sitio web de Target y enviada a los clientes por correo electrónico y correo postal de EE. UU. que "no hay indicios de que los números PIN se hayan visto comprometidos".[61,62]El CEO también explicó que el simple hecho de haber comprado en Target durante ese período no implicaba que fueran víctimas de fraude, y que el nivel de fraude había sido bajo en situaciones similares.[63]Target ofreció monitoreo gratuito de crédito y robo para los clientes afectados durante un año y les aseguró que no serían responsables de ningún cargo fraudulento que resultara de la violación.[64](Ver **Anexo 8a**para el anuncio de Target y**Anexo 8b**(para la carta de Steinhafel.) Target también declaró que no era probable que se hubiera accedido a fechas de nacimiento y números de Seguro Social.[65]

En una disculpa en video publicada en el sitio web corporativo de Target el mismo día, Steinhafel explicó que los tiempos de espera en los centros de llamadas de Target eran "inaceptables" y que su equipo estaba "trabajando las 24 horas" para acortarlos. Steinhafel ofreció el descuento del 10 % para empleados a los clientes que compraran en las tiendas Target el 21 y el 22 de diciembre.[66,67]El CEO destacó tres pasos que sus clientes preocupados deben seguir, a saber, verificar la actividad de la tarjeta de crédito para ver si hubo cargos sospechosos, comunicarse con el proveedor de la tarjeta o con el propio Target si un cliente encuentra cargos sospechosos y verificar su informe de servicios de crédito.[68]Sin embargo, los clientes no se sentían preparados para protegerse. Un cliente afirmó: "¿Cómo diablos se supone que voy a controlar mi cuenta si no puedo acceder a ella? No hay excusa que me sirva".[69]La presión sobre la gerencia de Target para gestionar de manera eficiente la respuesta a la violación continuó aumentando.

El 20 de diciembre,*Krebs sobre seguridad*se enteró de que los mercados negros clandestinos se habían inundado de tarjetas de crédito y débito robadas que se vendían en lotes de un millón de tarjetas a un precio que oscilaba entre 20 y 100 dólares cada una.[70] Estos lotes de tarjetas se consideraron de alta "calidad", ya que se habían robado datos de las bandas magnéticas de las tarjetas y podían clonarse más fácilmente. Krebs habló con un banco de Nueva Inglaterra y descubrió que, aunque los funcionarios del banco habían identificado hasta el momento a 6.000 clientes (el 5% de su cartera de tarjetas) que habían sido clonados,

Habían comprado en Target durante el período de la infracción, pero no habían recibido ninguna notificación de Target ni de las fuerzas del orden. El representante del banco afirmó: “Nadie nos ha notificado. Las fuerzas del orden no han dicho nada, nuestras asociaciones bancarias estatales no han enviado nada... nada”.[71]

El 25 de diciembre, un ejecutivo de pagos familiarizado con la violación de seguridad de Target declaró que se había robado información del PIN, y el 27 de diciembre, Target revirtió su posición anterior para confirmar que, de hecho, se había robado información del PIN.[72,73]Además de los datos PIN, se habían visto comprometidos los números CVV y las fechas de caducidad, y los clientes ni siquiera tenían que haber pasado sus tarjetas en una tienda Target. Target había conservado datos a lo largo del tiempo, que ahora habían sido robados.[74]Target explicó que, aunque se había robado la información del PIN, esta permanecía cifrada y que no se había robado la clave de descifrado, necesaria para desbloquear y descifrar el código PIN, ya que nunca se almacenó en la red de Target. Solo el procesador de pagos independiente podía descifrar este código.[75]

El 10 de enero, Target anunció que, además de datos de tarjetas de pago, también se había robado información personal, incluidos nombres y direcciones postales y de correo electrónico, de 70 millones de clientes, 30 millones más de los que Target había informado inicialmente.[76,77,78]Esta revelación planteó interrogantes sobre a qué otros datos podrían haber accedido los piratas informáticos. Un analista del sector explicó: “Es bastante difícil que alguien salga a solicitar un crédito a tu nombre si no tiene tu número de seguridad social. Pero si tiene tu número de seguridad social y todos estos otros datos también, el problema se agrava”.[79]
Target recopiló los números de la Seguridad Social de los clientes que solicitaron su tarjeta de crédito estrella, la REDcard. Un experto de la marca captó el sombrío sentimiento de los clientes:

> El minorista ha llegado a su punto más bajo de percepción por parte de los consumidores desde al menos junio de 2007. Si bien muchos dicen que pueden entender que una tienda haya sido atacada por piratas informáticos, están teniendo problemas para comprender lo que un cliente llamó una respuesta "desalentadora" a la violación de seguridad. Muchos están prometiendo evitar comprar en Target, mientras que otros han cancelado sus tarjetas REDcard... o están planeando demandar.[80]

Steinhafel explicó en una entrevista el 12 de enero de 2014: “La experiencia del centro de llamadas inicialmente fue inaceptable y por eso me disculpo. A partir del viernes [10 de enero], nuestros tiempos de espera fueron de solo 8 segundos”.[81]

Los piratas informáticos apuntaron a un gran número de clientes, lo que permitió realizar pequeños cargos que fácilmente podrían pasar desapercibidos para un ojo desprevenido.[82]“Es muy frustrante”, explicó una clienta afectada que había examinado sus estados de cuenta con gran detalle y había encontrado dos cargos no autorizados: uno de iTunes y un extraño cargo de 14 dólares que no había realizado. Otra clienta descubrió que su cuenta bancaria había perdido 3.643,53 dólares y ahora solo 5,86, lo que la obligó a pedir préstamos para comida y para la matrícula de su hijo.[83]

Autopsia: ¿Qué salió mal?

Una investigación del Senado descubrió que al menos dos meses antes de estos ataques, el equipo de seguridad de Target había destacado vulnerabilidades en el sistema POS de Target y solicitó revisar la red de pagos de Target.[84]Según un ex empleado, Target estaba actualizando sus terminales de pago, lo que dejó a los analistas de seguridad con menos tiempo para encontrar fallas en el sistema. Pero el informe del Senado concluyó que la solicitud de revisión fue ignorada, ya que Target se estaba preparando para un ajetreado fin de semana de Black Friday. No quedó claro quién dentro de la gerencia de Target tomó esta decisión, pero según un empleado:

> La gran cantidad de advertencias que reciben los minoristas hace que sea difícil saber cuáles tomar en serio. Target cuenta con un amplio equipo de inteligencia de ciberseguridad, que detecta numerosas amenazas cada semana y solo puede priorizar una cierta cantidad de problemas.[85,86]

Target había recibido una certificación de cumplimiento de los Estándares de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) en septiembre de 2013, de Trustwave Holdings, una empresa de seguridad de la información.[87,88]Las compañías de tarjetas exigían a los comerciantes que recibieran esta certificación antes de procesar transacciones. A finales de 2013, la industria de las tarjetas de pago se disponía a adoptar el último conjunto de normas, PCI DSS 3.0. Las grandes organizaciones como Target estaban sujetas a auditorías anuales de sus redes de seguridad.[89]
Trustwave era considerado líder en la industria de la seguridad, habiendo realizado miles de estas certificaciones y auditorías para minoristas y procesadores de pagos.[90]

Sin embargo, algunos clientes certificados por Trustwave sufrieron grandes ciberataques poco después de recibir sus certificaciones.[91]Según los observadores de la industria, "[los recientes ciberataques] también plantearon preguntas importantes sobre la responsabilidad de las empresas de terceros que auditan y certifican la confiabilidad de los restaurantes, minoristas y otros que aceptan pagos con tarjetas bancarias".[92]Además, los estándares en sí no se consideraban dinámicos. Según los analistas, las necesidades de seguridad evolucionaban a un ritmo más rápido: una empresa que cumplía con las normas podía dejar de cumplirlas al mes siguiente si se instalaban y configuraban cortafuegos de forma incorrecta o si se conectaban sistemas segregados porque se habían abusado de las restricciones de acceso.[93]Además, podrían surgir nuevas vulnerabilidades si una empresa cambiara sus servidores o su arquitectura de software, o incluso instalara nuevos programas. Por ello, los analistas del sector consideraron que los estándares PCI son un "piso y no un techo".[94]

Según un experto de la industria tecnológica, era poco probable que Target cumpliera con PCI. 2.0 en el momento de la violación, porque el ataque que afectó a millones de clientes pasó desapercibido durante 18 días.[95]Para interrumpir el ataque, Target debería haber tomado las medidas exigidas en el PCI DSS 2.1, la versión del PCI DSS vigente en el momento de la infracción. Target debería haber eliminado las cuentas predeterminadas innecesarias, que los piratas informáticos utilizaban para acceder a las partes más sensibles de la red de Target. Además, Target debería haber exigido a los proveedores que vigilaran de cerca la integridad de sus archivos críticos del sistema, lo que habría puesto a Fazio sobre aviso de que los piratas informáticos habían robado sus credenciales de Target. Por último, Target podría haber creado cortafuegos más fuertes entre sus sistemas internos e Internet externo; haber comprobado la ubicación de los inicios de sesión con credenciales; y haber creado una lista de servidores aprobados y conexiones a Internet con los que la red de Target podía comunicarse.[96,97]

Las secuelas

Las ventas totales de Target cayeron un 6,6% en el cuarto trimestre de 2013 y, en comparación con el año anterior, las ganancias netas del cuarto trimestre cayeron un 46% a 520 millones de dólares.[98,99]El 1 de febrero de 2014, seis semanas después de la fecha del anuncio de la violación, el precio de las acciones de la empresa cayó un 8,8% a 56,7 dólares por acción.[100]
Target también pronosticó una reducción de aproximadamente el 20% en las ganancias por acción (EPS) después del episodio. A fines de 2014, Target había incurrido en costos de 162 millones de dólares debido a la filtración de datos, y se esperaba que la cantidad aumentara como resultado de litigios pendientes.[101,102]

Aunque Target hizo un esfuerzo concertado para controlar el daño del ataque, enfrentó un amplio escrutinio de los medios, investigaciones del Congreso, la Comisión de Bolsa y Valores (SEC), el Departamento de Justicia y la Comisión Federal de Comercio (FTC), así como litigios de clientes, bancos y accionistas afectados.

Investigaciones del Congreso

Los ejecutivos de Target fueron llamados a testificar sobre la violación ante el Comité Judicial del Senado y el Comité de Comercio, Ciencia y Transporte del Senado. El día antes de la audiencia del 27 de marzo, la oficina del senador John D. Rockefeller IV, presidente del Comité de Comercio, Ciencia y Transporte, publicó un informe que detalla cómo ocurrió la violación y cómo Target pasó por alto numerosos datos confidenciales.

oportunidades para detener el ataque.[103](Ver**Anexo 6**(Para obtener un resumen del análisis del comité). En la audiencia, el senador Richard Blumenthal, miembro del comité, declaró:

> [El informe de investigación] explica cómo Target podría haber evitado la violación si hubiera impedido que los atacantes completaran incluso uno solo de los pasos [descritos en el informe]. La mejor tecnología del mundo es inútil a menos que haya una buena gestión y, para ser franco, hubo múltiples advertencias del software anti-intrusión de la empresa. La dirección las pasó por alto. Si Target no protegió adecuadamente la información de los clientes, les negó la protección que esperan con razón cuando una empresa recopila su información personal.[104,105,106]

El senador Blumenthal continuó: "En el futuro, en algún momento, el director ejecutivo y la junta directiva tendrán que asumir la responsabilidad".[107,108]

Litigio

Target se enfrentó a demandas de clientes particulares, bancos que brindaban servicios de tarjetas de crédito e inversores. Al 7 de mayo de 2014, Target tenía 81 casos de consumidores, 28 casos de bancos y 4 casos de accionistas presentados y pendientes ante varios tribunales.[109]

Demandas de clientes

Los piratas informáticos eligieron un momento oportuno para atacar. La temporada de compras de Acción de Gracias y Navidad marcó uno de los períodos de compras más importantes para los consumidores estadounidenses. En 2014, solo durante el Día de Acción de Gracias y el día siguiente (Viernes Negro), los estadounidenses gastaron más de 12 mil millones de dólares, y la mayor parte de estas ventas, más de 9 mil millones de dólares, se realizaron durante el Viernes Negro.[110]

Los datos de la pista[yo]Los datos robados por los hackers permitieron falsificar la información codificada en la banda magnética de una tarjeta y, con los datos del PIN, retirar dinero directamente de las cuentas de los clientes.[111, 112] Si hubieran sabido que los números PIN habían sido comprometidos, los clientes podrían haber solicitado tarjetas de reemplazo y haberse protegido. Sin embargo, hasta el 27 de diciembre, Target afirmó que no había indicios de que los PIN de las tarjetas de débito estuvieran afectados y sostuvo que los culpables no podían retirar dinero de las cuentas de los clientes. Una demanda dio el ejemplo de una clienta, madre de cinco hijos, cuya tarjeta fue rechazada cuando intentó realizar un retiro:[113]

> La Sra. [Brystal] Keller tuvo un cargo fraudulento de $434.15... otro por un monto de $276... El banco de la Sra. Keller no reembolsó ninguno de los cargos fraudulentos hasta el 7 de enero de 2014, más de dos semanas después de que ocurrió el fraude... Su cuenta estuvo bloqueada desde el 26 de diciembre de 2013 hasta el 21 de enero de 2014... La Sra. Keller no pagó el alquiler, pagó el préstamo de un automóvil... tuvo dificultades para poner comida en la mesa para su familia durante las vacaciones.

Además del dinero robado directamente, los clientes afectados tuvieron que hacer frente a tasas de interés más altas debido a los pagos atrasados, los costos de reemplazar la identificación emitida por el gobierno y la contratación de asistencia legal. Un cliente tuvo 35 consultas fraudulentas en su historial crediticio y su "puntaje crediticio bajó aproximadamente entre 25 y 50 puntos", lo que retrasó la compra de un automóvil nuevo que necesitaba desesperadamente.[114]

Los datos de seguimiento son una cadena de caracteres codificados en la banda magnética de una tarjeta de crédito que incluye el nombre del titular de la tarjeta, la fecha de vencimiento de la tarjeta y el número de valor de verificación de la tarjeta (CVV).

Los demandantes en demandas interpuestas por consumidores afirmaron que Target tenía la responsabilidad de cumplir con los estándares de la industria en la construcción y mantenimiento de cortafuegos, la protección de los datos de los titulares de tarjetas y la supervisión de los controles y los sistemas de red. Las demandas de los consumidores alegaron que Target no cumplía con todas las regulaciones aplicables a los minoristas. Además, las demoras de Target en descubrir la violación de seguridad, del 30 de noviembre al 12 de diciembre, y en detenerla, del 12 al 15 de diciembre, permitieron que los piratas informáticos siguieran robando información de tarjetas de crédito y débito.

Como resultado, los clientes afectados solicitaron una indemnización por las violaciones de las leyes estatales de protección al consumidor, la negligencia y el incumplimiento del contrato. En noviembre de 2015, Target aceptó un acuerdo para cubrir las pérdidas de los consumidores.[115]Sesenta y un millones de personas fueron notificadas directamente sobre el acuerdo, y los clientes que documentaron sus gastos podrían recuperar hasta $10,000.[yo,116]

Bancos

Visa, MasterCard y otras instituciones financieras también presentaron demandas contra Target. Al menos siete meses antes de los ataques, en abril y nuevamente en agosto de 2013, Visa había publicado alertas para los minoristas en las que detallaba las vulnerabilidades de seguridad del malware que extraía datos de RAM.[117,118]Visa detalló los métodos que los piratas informáticos podrían utilizar y recomendó pasos como "configurar el firewall", "garantizar que solo los puertos, servicios y direcciones IP permitidos se comuniquen con la red", "segregar la red de procesamiento de pagos de otras redes que no procesan pagos" e "implementar cifrado punto a punto basado en hardware".[119]El equipo de seguridad interno de Target escaló las alertas y solicitó una revisión más a fondo de la infraestructura de seguridad de Target, pero no se atendió la solicitud.[120]

Los bancos afirmaron que Target había actuado de manera negligente al no proporcionar la seguridad suficiente para los datos. Los demandantes también acusaron a Target de violar la Ley de Seguridad de Tarjetas Plásticas de Minnesota al proteger los datos de manera inadecuada, tergiversar los hechos sobre la seguridad de los datos y retener los datos de las tarjetas de pago.[121]

Además, debido a que Target procesaba tarjetas de crédito, estaba sujeto a las Reglas de Bandera Roja de FACTA.[yo,122] Estas normas exigían a los minoristas que desarrollaran y administraran protocolos para identificar el robo de datos y las vulnerabilidades, supervisar las transacciones de crédito y responder cuando se robaban las identidades de los consumidores. Los bancos argumentaron que Target no había implementado ni respetado las "Reglas de alerta", lo que violaba la ley federal.[123]

"Las instituciones financieras no deberían tener que soportar la carga de costos elevados relacionados con violaciones de datos de comerciantes sobre las que no tienen control", argumentaron los abogados del demandante.[124]Un banco afectado afirmó que los sistemas de Target eran vulnerables, ya que Target conservaba los datos de las transacciones de los clientes en sus propios servidores. Como resultado, los bancos tuvieron que hacer frente a costes adicionales por la reemisión de tarjetas, el reembolso a los clientes que habían incurrido en cargos no autorizados y la contratación de personal para prestar atención al cliente.[125]Estos costes resultaron especialmente caros para los bancos más pequeños, como explicó el director ejecutivo de la Asociación de Banqueros de Estados Unidos. En una carta al Congreso del 16 de enero de 2014, explicó:[126,127]

> Los bancos con menos de mil millones de dólares en activos gastaron un promedio de 11,02 dólares para reemitir una tarjeta de débito y 12,75 dólares para reemitir una tarjeta de crédito. Eso se compara con los 2,70 y 2,99 dólares respectivamente que gastaron los bancos con más de 50 mil millones de dólares en activos. Cuando un minorista como Target

---

i Aquellos clientes que no documentaron sus pérdidas tenían derecho a una porción igual del fondo de liquidación restante.

La Sección 114 de la Ley de Transacciones Crediticias Justas y Precisas de 2003 ("FACTA"), conocida como las "Reglas de Bandera Roja", exige que las organizaciones que gestionan o extienden crédito detecten, prevengan y mitiguen el robo de identidad mediante el desarrollo de un "Programa de Prevención del Robo de Identidad" escrito. Esta definición abarca no solo a las instituciones financieras, sino también a las empresas no financieras, como las empresas de servicios públicos, los concesionarios de automóviles, las empresas de atención médica y los minoristas.

> habla de que sus clientes tienen “cero responsabilidad” por transacciones fraudulentas, es porque los bancos de nuestra nación son los que brindan ese alivio, no el minorista que sufrió la violación.

Target resolvió su demanda con Visa por 67 millones de dólares en agosto de 2015, y por aproximadamente 40 millones de dólares con MasterCard y otros bancos en diciembre de 2015.[128,129]Para entonces, Target había gastado aproximadamente 290 millones de dólares en costos relacionados con la violación y esperaba un reembolso de 90 millones de dólares de las aseguradoras.[130]

Responsabilidad de la Junta Directiva

Los accionistas de Target presentaron demandas derivadas contra todos los directores del directorio de la empresa y contra el director financiero y el director de informática.[131]En particular, los accionistas identificaron al director ejecutivo Gregg W. Steinhafel, a la directora de informática Beth M. Jacob, al director independiente principal James A. Johnson y a los presidentes y miembros de los comités de auditoría y responsabilidad corporativa del directorio como líderes cuyo “imprudente desprecio por sus deberes... planteaba un riesgo de daño grave a la empresa”.[132](Referirse a**Anexo 9**(para obtener información biográfica sobre los directores de Target).

En las demandas se afirmaba que, en virtud de sus deberes fiduciarios, los directores estaban obligados a crear y mantener un sistema para proteger la información personal y financiera de los clientes, así como a investigar y corregir las prácticas indebidas. Además, los directores estaban obligados a informar a los clientes de cualquier infracción de forma precisa y oportuna.[133]

Las demandas derivadas afirmaron que los directores incumplieron su deber fiduciario al no implementar controles internos para proteger los datos de los consumidores.[134]Además, los accionistas alegaron que la negligencia de los directores provocó un desperdicio de activos corporativos, ya que la empresa perdió ingresos, tuvo que ofrecer un descuento del 10% para atraer clientes nuevamente a la tienda y enfrentó futuros gastos de litigio.[135]Los demandantes también afirmaron que los directores malgastaron y administraron mal los activos corporativos al proporcionar compensaciones y estructuras de bonificación inadecuadas a ciertos funcionarios ejecutivos.[136]

Los demandantes alegaron además que los directores y los miembros del Comité de Auditoría no tomaban en serio sus responsabilidades de información financiera y que no supervisaban los controles internos y los sistemas de seguridad cibernética.[137]Los accionistas enumeraron una serie de costos en los que incurrieron debido a la inacción de los directores: acuerdos de demanda colectiva, investigaciones del Departamento de Justicia y del Servicio Secreto y posibles multas, aumento del costo del capital debido a una rebaja de calificación, honorarios legales y de consultoría, y costos de los esfuerzos de retención de clientes como monitoreo de crédito y descuento del 10% para compradores estadounidenses, todo lo cual erosionó el valor para los accionistas.[138]

En respuesta, los abogados de Target afirmaron que los directores no eran responsables, ya que estaban protegidos por los estatutos de la empresa, que los protegían de toda responsabilidad, excepto en casos de mala conducta intencional. Además, el equipo legal respondió que los accionistas no habían presentado "afirmaciones plausibles" de que los directores no habían cumplido con sus obligaciones y que la ocurrencia de la filtración de datos en sí misma no implicaba que los directores no hubieran cumplido con sus obligaciones.[139]

Riesgos reconocidos por Target

El estatuto del Comité de Auditoría del directorio de Target destacó la responsabilidad de supervisión del comité para revisar y discutir el enfoque de la evaluación de riesgos, incluido el riesgo de fraude, con el jefe de auditoría interna de la empresa.[140]Esta responsabilidad colaborativa también incluyó dedicar recursos para mitigar los riesgos identificados.[141,142]La declaración de poder de Target también destacó la responsabilidad del Comité de Responsabilidad Corporativa de “evaluar y gestionar el riesgo reputacional”.[143.144]De hecho, en su presentación 10-K de 2012, Target había identificado la violación de la seguridad de los datos como un riesgo al que estaba expuesta la empresa:

> Si sufrimos una importante violación de la seguridad de los datos o no logramos detectarla ni responder adecuadamente a ella, podríamos estar expuestos a acciones de cumplimiento de la ley por parte del gobierno y a litigios privados. Además, nuestros clientes podrían perder la confianza en nuestra capacidad para proteger su información personal, lo que podría hacer que dejen de usar las tarjetas REDcard, se nieguen a utilizar nuestros servicios de farmacia o dejen de comprar con nosotros por completo. La pérdida de confianza a causa de una importante violación de la seguridad de los datos que involucre a miembros del equipo podría dañar nuestra reputación, generar desafíos en la contratación y retención de miembros del equipo, aumentar nuestros costos laborales y afectar la forma en que operamos nuestro negocio.[145]

Las instituciones de gobernanza opinan

En mayo de 2014, la importante firma de asesoramiento en materia de representación de accionistas ISS publicó un informe en el que afirmaba que las fallas del Comité de Auditoría, del Comité de Responsabilidad Corporativa y del directorio habían provocado pérdidas significativas para la empresa y sus accionistas. ISS expresó su preocupación por el "fracaso de estos comités y, posiblemente, por extensión, del directorio en pleno, en reconocer la amenaza potencial que enfrentaba la empresa".[146]ISS recomendó a los accionistas que 7 de los 10 miembros de la junta directiva deberían ser removidos por negligencia. ISS recomendó la remoción de todo el Comité de Auditoría, incluida la presidenta, Roxanne Austin; el director independiente principal, James Johnson, quien también formaba parte del Comité de Compensación; y otros dos directores.[147]

La ISS argumentó que, al no vigilar de cerca la posibilidad de robo, los directores permitieron que sus clientes y comunidades se enfrentaran a riesgos indebidos y a un daño insuperable a la marca y la reputación de la empresa. El informe de la ISS afirmaba:[148]

> Parece que el fracaso de los comités [de Auditoría y Responsabilidad Corporativa] a la hora de garantizar una gestión adecuada de estos riesgos preparó el terreno para la filtración de datos, que ha provocado pérdidas significativas para la empresa y sus accionistas. Se justifica un voto EN CONTRA de los directores que forman parte de los Comités de Auditoría y Responsabilidad Corporativa por no proporcionar una supervisión suficiente de los riesgos.

ISS también afirmó que la junta directiva mostró un desprecio por los procedimientos de divulgación y los procesos de evaluación de riesgos al no comunicar un programa sólido a los accionistas antes de la violación.[149]La respuesta de la junta directiva a la violación fue reactiva, sugiriendo que la empresa no estaba preparada para prevenir y manejar una violación de esta magnitud.[150]ISS también afirmó que tanto el comité de Auditoría como el de Responsabilidad Corporativa deberían haber monitoreado más de cerca el riesgo al valor de la marca y la reputación de la empresa y, por lo tanto, estos comités fueron responsables de las pérdidas debidas a la violación de datos.[151]

La ISS cuestionó si el CIO estaba calificado para el cargo. El informe afirmaba:

> Según una biografía disponible públicamente, la ex CIO se incorporó a Target en 1984, donde pasó dos años como asistente de compras en la división de tiendas departamentales Dayton's de la empresa. Dejó la empresa en 1986, pero regresó en 2002 como directora de centros de contacto con los clientes. Se convirtió en vicepresidenta de operaciones para clientes en 2006, y luego fue nombrada vicepresidenta sénior y CIO en 2008. Fue ascendida a vicepresidenta ejecutiva y CIO en 2010. En comparación, la nueva CIO tiene "más de 40 años de experiencia y es una líder reconocida en tecnología de la información, seguridad de datos y operaciones comerciales", según el comunicado de prensa de Target que anuncia su nombramiento.[152]

Sin embargo, Glass Lewis, otro asesor de votos, sugirió que no había suficiente información para concluir que la junta había sido negligente.[153]Glass Lewis reconoció varias fallas: Target no había requerido la autenticación adecuada de sus proveedores, sus empleados no habían actuado ante las advertencias de seguridad y el sistema permitía la transmisión de datos robados sin detección y no detectaba

que los servidores internos habían sido comprometidos. Sin embargo, Glass Lewis no recomendó reemplazar a ningún director debido a la filtración de datos.[154]En cambio, Glass Lewis recomendó votar “no” contra Johnson y Anne M. Mulcahy por cuestiones no relacionadas en Fannie Mae y Citigroup, respectivamente.

La junta directiva de Target se defiende

Después de que ISS publicara su informe, el directorio de Target emitió una carta asegurando a los accionistas que tomaba en serio sus "responsabilidades de supervisión" y que antes de la filtración había autorizado a la compañía a gastar "cientos de millones de dólares" en seguridad de la red, había duplicado el personal de seguridad de la información en cinco años y había tomado otras medidas de seguridad.[155](Ver**Anexo 10**Target también explicó que la empresa tenía “300 empleados dedicados a la seguridad de la información, había capacitado a 350.000 empleados en seguridad de datos y tenía personal en un centro de operaciones de seguridad abierto las 24 horas para revisar la actividad sospechosa en la red”.[156]Otros también defendieron al consejo. Un experto en gobernanza explicó: “El papel de los directores es de supervisión, no de gestión diaria. No se puede esperar que los directores gestionen al personal de seguridad para garantizar que esté haciendo su trabajo; este papel es clara y directamente una función de gestión... Target identificó la ciberseguridad como un riesgo y estableció controles para monitorear este riesgo; la supervisión fue el resultado de un error humano”.[157]

Según algunos analistas del sector, las infracciones cibernéticas en las redes corporativas eran riesgos que se podían gestionar, pero no prevenir. (Consulte**Anexos 11**y**12a, 12b**,y**12c**Según estos analistas, era importante que la dirección respondiera rápidamente una vez que se descubrió la infracción y, en su opinión, la dirección de Target reaccionó rápidamente en este caso. Por ello, estos analistas creían que el argumento para culpar a los miembros de la junta directiva no era particularmente sólido en comparación con infracciones anteriores que pasaron desapercibidas durante años.[158]

Conclusión

En los últimos años, las violaciones de datos y los delitos cibernéticos se han convertido en un problema cada vez mayor para las empresas estadounidenses. Ante estas tendencias, los observadores y los expertos en gobernanza se preguntaron qué papel debería desempeñar el consejo de administración en la supervisión de la ciberseguridad y cómo podrían cumplir con sus responsabilidades en este ámbito de la manera más eficaz.

Anexo 1 Estado de resultados seleccionados de Target Corporation (millones de USD)

Año fiscal que termina en febrero de 2001	2010	2011	2012	2013	2014
Ganancia	63.435	65.786	68.466	71.960	71,279
Beneficio bruto	19.031	20.703	21,559	22,427	21.240
Lngresos netos	2.488	2.920	2.929	2.999	1.971
EPS básico	3.31	4.04	4.31	4.57	3.1
Promedio ponderado de acciones básicas fuera.	752	724	679	657	635

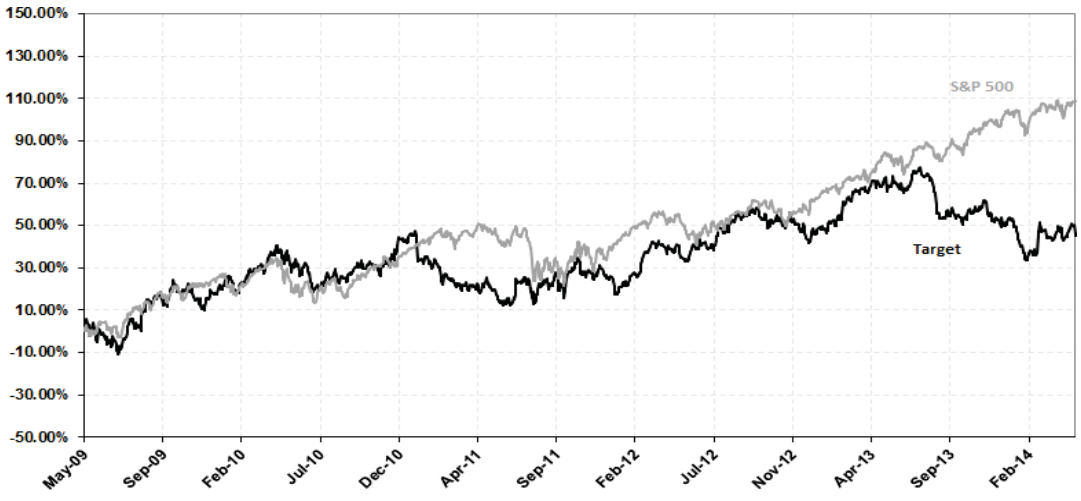
Fuente: Capital IQ, consultado el 8 de junio de 2016.

Anexo 2 Balance general seleccionado de la corporación objetivo (millones de USD)

Año fiscal que termina en febrero de 2001	2010	2011	2012	2013	2014
Activos corrientes totales	18.424	17.213	16.449	16.388	11,573
Buena voluntad	59	59	59	59	151
Activos totales	44.533	43.705	46.630	48.163	44.553
Pasivo corriente total	11,327	10.070	14.287	14.031	12.777
Pasivo total	29,186	28,218	30.809	31.605	28.322
Patrimonio total	15.347	15,487	15.821	16.558	16.231
Pasivos y patrimonio totales	44.533	43.705	46.630	48.163	44.553

Fuente: Capital IQ, consultado el 8 de junio de 2016.

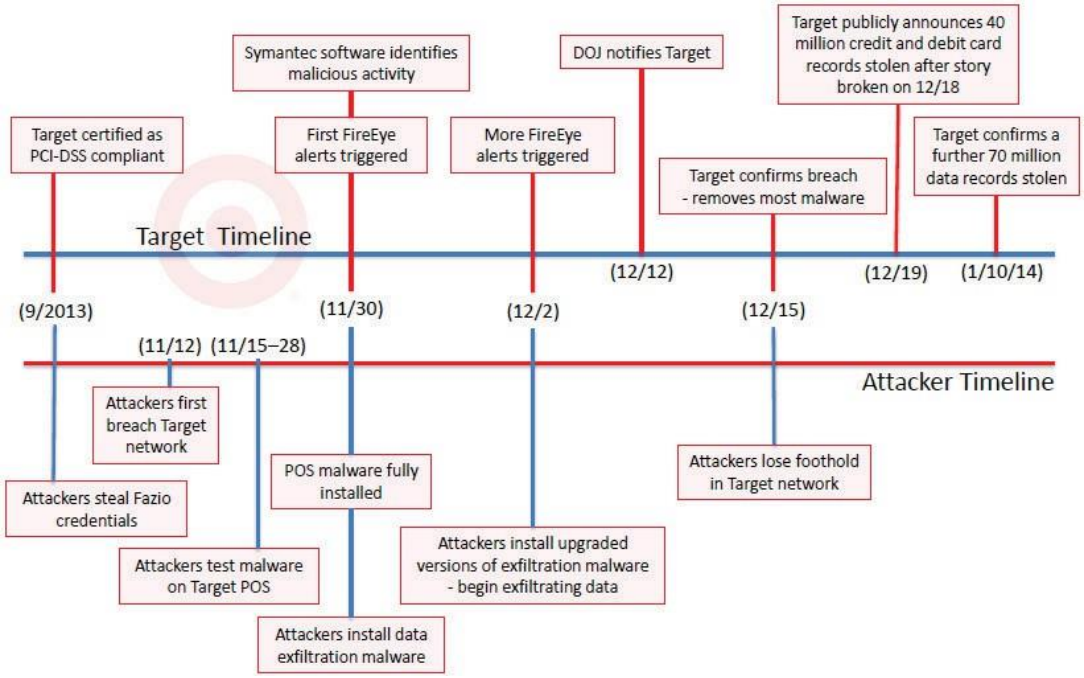
Anexo 3 Rendimiento de las acciones de Target Corporation en comparación con el S&P 500 (5 de mayo de 2009–5 de mayo de 2014)



Fuente: Capital IQ, consultado el 2 de mayo de 2016.

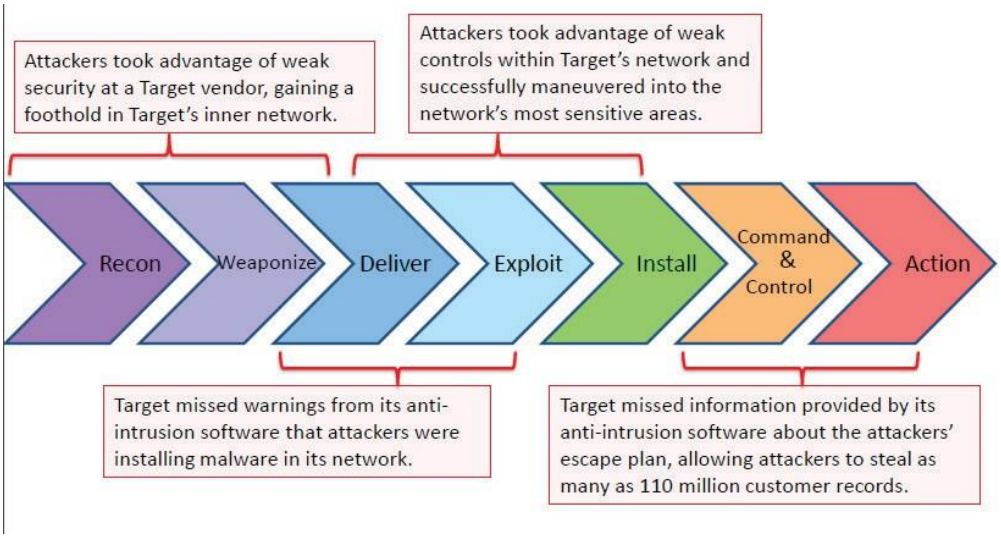
Nota: Ambas series están indexadas al 5 de mayo de 2009.

Anexo 4 Cronología de la filtración de datos de Target



Fuente: Comité Senatorial de Comercio, Ciencia y Transporte, *Un análisis de la "cadena de muerte" de la filtración de datos de Target en 2013* 113ei Congreso, 2Dakota del Nortesesión, 2014.

Anexo 5 Posibles oportunidades perdidas del objetivo



Fuente: Comité Senatorial de Comercio, Ciencia y Transporte, *Un análisis de la "cadena de muerte" de la filtración de datos de Target en 2013* 113ei Congreso, 2Dakota del Nortesesión, 2014.

Anexo 6 Resumen del análisis del Comité del Senado sobre la filtración de datos de Target

El siguiente resumen describe el análisis de "Kill Chain" realizado por el Comité del Senado y describe los pasos que Target y Fazio Mechanical Services podrían haber tomado para prevenir el ciberataque.

1)**"Reconocimiento"**—Información sobre las víctimas recopilada discretamente por el atacante

Los atacantes podrían haber enviado correos electrónicos con malware a Fazio, el proveedor externo de Target. Unas simples búsquedas en Internet permitieron a los piratas informáticos encontrar el portal de proveedores y las páginas de gestión de instalaciones de Target, así como trazar un mapa de la red interna de Target. Target podría tener información públicamente disponible limitada.

2)**"'Armas"**—El hacker prepara el malware para enviarlo a la víctima

Es probable que el hacker haya utilizado su malware como arma mediante un simple archivo adjunto en un correo electrónico, como un PDF o un documento de Microsoft Office. Fazio utilizó indebidamente una versión gratuita de su software antimalware, que no ofrecía protección en tiempo real y estaba destinada a uso individual y no corporativo.

3)**"Entrega"**—Malware enviado a la víctima

El atacante inició el ataque de phishing y el malware proporcionó a los piratas informáticos las contraseñas de Fazio para los sistemas de Target (Target podría haber requerido una autenticación de dos pasos en esta etapa, una contraseña y una confirmación móvil, como medida de protección). Los estándares PCI-DSS requieren una autenticación de dos pasos para el acceso remoto a las redes de pago, pero esto técnicamente no era parte del sistema POS de Target. Los atacantes cargaron el malware que extraía RAM en los terminales POS de Target.

4)**"Explotación"**—Malware distribuido en las redes de las víctimas

El malware que extrae la memoria RAM comenzó a registrar datos de millones de tarjetas a medida que se pasaban por las cajas registradoras. En ese momento, Target podría haber verificado cualquiera de las alertas enviadas por su software FireEye, o podría haber habilitado el software para que eliminara automáticamente el malware. Target también podría haber prestado mayor atención a una de las muchas alertas de la industria y el gobierno sobre el aumento de las amenazas cibernéticas.

5)**"Instalación"**—El atacante gana terreno en las redes de las víctimas

Los piratas informáticos utilizaron los sistemas de Fazio para seguir violando las redes de Target, aunque no está claro cómo. Una medida de protección en esta etapa habría sido eliminar las cuentas predeterminadas innecesarias.

6) "**Mando y Control (C2)"**—El atacante obtiene acceso remoto a las redes de la víctima

Los piratas informáticos mantuvieron una línea de comunicación entre Internet exterior y la red de Target; Target podría haber verificado por qué se estaba utilizando el inicio de sesión de Fazio para acceder a partes no relacionadas de la red de Target y podría haber desarrollado firewalls más fuertes.

7)**"'Acciones sobre objetivos"**—El atacante inicia la extracción de datos

Los piratas informáticos extrajeron los datos a servidores en Rusia, que deberían haber sido marcados como sospechosos. El sistema FireEye de Target detectó el malware de extracción y Target podría haber tomado medidas al respecto.

Fuente: Comité Senatorial de Comercio, Ciencia y Transporte, *Un análisis de la "cadena de muerte" de la filtración de datos de Target en 2013* 113El Congreso, 2Dakota del Nortesesión, 2014.

Nota: Un análisis de "cadena de muerte" es un marco desarrollado por investigadores de seguridad de Lockheed Martin y es una herramienta estándar de la industria utilizada por la industria de seguridad de la información.

Anexo 7 Estructura de seguridad de la información del objetivo antes de la violación

En Target había tres equipos que tenían responsabilidades interrelacionadas en materia de seguridad de datos: Target Information Protection (TIP), Target Technology Services (TTS) y Corporate Security.

Protección de la información de destino (TIP)

El papel de TIP incluía: (1) establecer e implementar políticas y estándares de seguridad de la información; (2) trabajar con evaluadores externos para gestionar el cumplimiento de estándares externos; (3) gestionar la respuesta a incidentes de seguridad de red no rutinarios; (4) priorizar las inversiones relacionadas con la seguridad de la información.

Desde 2010 hasta la filtración, TIP estaba dirigida por un ejecutivo de alto nivel que, además de ser responsable de aspectos relacionados con la seguridad de los datos, también era el director de privacidad y responsable del cumplimiento de la HIPAA. El director de alto nivel de TIP reportaba al presidente de la división Target Financial and Retail Services (FRS), quien a su vez reportaba al director financiero de la empresa. TIP tenía equipos relacionados con aspectos de seguridad, en particular:

(a) Equipo de evaluación y gestión de proveedores, que era responsable de evaluar si los proveedores Podría acceder a la red de Target en función del riesgo del proveedor. El equipo realizó alrededor de 300 evaluaciones de proveedores cada año.

(b) Comité de Revisión de Riesgos (RRC), que era un equipo multifuncional que servía como recurso que Brindó orientación a los equipos comerciales y tecnológicos sobre la mitigación de riesgos. RRC no gestionó la mitigación, pero sirvió como fuente de información.

(c) Equipo de admisión, que proporcionó un lugar para que los empleados de Target pudieran dirigir preguntas relacionadas con la seguridad, Por ejemplo, ¿qué hacer si un empleado pierde una computadora portátil?

Servicios de tecnología de destino (TTS)

TTS era el equipo de tecnología de la información dirigido por el director de información (CIO), que a su vez reportaba al director ejecutivo de la empresa. TTS planificó, construyó y dirigió los sistemas informáticos de Target y administró la red corporativa, los centros de datos, las redes de tiendas, los registros de puntos de venta y el sitio web Target.com. TTS empleaba a unas 9.000 personas en el momento de la filtración. TTS tenía un equipo de ciberseguridad dirigido por un director sénior que reportaba al CIO. Además, Target tenía otros dos equipos relacionados con la seguridad de la información dentro de TTS: el Centro de Operaciones de Seguridad (SOC) y el equipo Red.

(a) El SOC era un centro de gestión de alertas las 24 horas que monitoreaba la red para detectar anomalías. actividad y trabajó con TIP para abordar los problemas de seguridad identificados. En el momento de la vulneración, los sistemas de Target generaban alrededor de 200 alertas por día, que eran analizadas por humanos dentro de un sistema predefinido de análisis y escalamiento. Si una alerta se consideraba grave, se escalaba a TIP para su resolución.

(b) El equipo rojo era un equipo interno de piratas informáticos de “sombrero blanco” que realizaban tareas de seguridad de la red. pruebas y simulaciones de ataques encubiertos y abiertos para probar las respuestas del objetivo.

Investigaciones de seguridad corporativa y de seguridad de la información (ISI)

El brazo de investigación del programa de seguridad de datos y el equipo de inteligencia cibernética formaban parte del departamento de Seguridad Corporativa, encabezado por un vicepresidente que reportaba al asesor general. Los analistas de ISI investigaban los incidentes en coordinación con el SOC y el TIP.

Gobernanza del programa de ciberseguridad

La gobernanza general de la seguridad cibernética estaba bajo la supervisión del Comité Ejecutivo de Seguridad Cibernética de Target, que se reunía trimestralmente. El comité estaba formado por altos directivos de Seguridad Corporativa, la unidad de negocios FRS y TTS. El siguiente nivel era el Comité Directivo de Seguridad Cibernética, que se encargaba de reunir a las personas para planificar el futuro del programa de seguridad cibernética, revisar la estrategia de seguridad cibernética y preparar las agendas para las reuniones del Comité Ejecutivo de Seguridad Cibernética. Estaba formado por líderes de TTP, TTS y Seguridad Corporativa. Por último, el Grupo de Trabajo de Seguridad Cibernética reunía información relevante de fuentes internas y externas e informaba al Comité Directivo de Seguridad Cibernética sobre las tendencias de amenazas y vulnerabilidades. Los miembros de este grupo provenían de TIP, TTS y Seguridad Corporativa.

Auditores internos y externos

El departamento de Aseguramiento, Riesgo y Cumplimiento (ARC) desempeñaba la función de auditoría interna de la empresa y reportaba al director financiero y al comité de auditoría. La función de auditoría interna incluía un equipo que era responsable de auditar la eficacia de los controles para las funciones de soporte, incluida la tecnología de la información. Ernst & Young (E&Y), los auditores externos de Target, probaron y auditaron los controles internos relacionados con la tecnología de la información. Antes de la filtración, E&Y no había encontrado debilidades materiales en los controles internos de Target.

Comités de la Junta Directiva

Antes de la violación de datos, la responsabilidad de supervisión de la seguridad de los datos recaía principalmente en el Comité de Auditoría, como parte de su responsabilidad general de supervisar la integridad de los estados financieros de Target, supervisar la auditoría interna y supervisar el cumplimiento de los requisitos legales y reglamentarios por parte de Target. El Comité de Responsabilidad Corporativa tenía funciones de supervisión relacionadas con la privacidad de los clientes y el impacto de una violación de datos en la reputación de Target.

Fuente: Elaborado por el autor del caso con base en la información del Informe del Comité de Litigios Especiales de Target Corporación de fecha 30 de marzo de 2016.

Anexo 8a Comunicado de prensa inicial de Target, fechado el 19 de diciembre de 2013

Target confirma acceso no autorizado a datos de tarjetas de pago en tiendas de EE.UU.

Target confirmó hoy que tiene conocimiento de un acceso no autorizado a los datos de tarjetas de pago que puede haber afectado a ciertos clientes que realizan compras con tarjeta de crédito y débito en sus tiendas de Estados Unidos. Target está trabajando en estrecha colaboración con las autoridades y las instituciones financieras, y ha identificado y resuelto el problema.

"La primera prioridad de Target es preservar la confianza de nuestros clientes y hemos actuado con rapidez para solucionar este problema, de modo que los clientes puedan comprar con confianza. Lamentamos cualquier inconveniente que esto pueda causar", afirmó Gregg Steinhafel, presidente y director ejecutivo de Target. "Tomamos este asunto muy en serio y estamos trabajando con las autoridades para llevar a los responsables ante la justicia".

Es posible que aproximadamente 40 millones de cuentas de tarjetas de crédito y débito se hayan visto afectadas entre el 27 de noviembre y el 15 de diciembre de 2013. Target alertó a las autoridades y a las instituciones financieras inmediatamente después de enterarse del acceso no autorizado y está poniendo todos los recursos necesarios para respaldar estas iniciativas. Entre otras acciones, Target se está asociando con una importante empresa forense externa para realizar una investigación exhaustiva del incidente.

Hay más información disponible en el sitio web corporativo de Target. Los clientes que sospechen de alguna actividad no autorizada deben comunicarse con Target al: 866-852-8680.

Fuente: "Target confirma acceso no autorizado a datos de tarjetas de pago en tiendas de EE. UU.", sitio web de Target Corporation, https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car consultado el 7 de julio de 2016.

Anexo 8b El director ejecutivo de Target informa a sus clientes sobre una filtración de datos, fechada el 20 de diciembre de 2013

Estimado huésped de Target:

Como probablemente ya hayas oído, Target sufrió un acceso no autorizado a los datos de tarjetas de pago de las tiendas Target de EE. UU. Nos tomamos este delito muy en serio. Fue un delito contra Target, contra los miembros de nuestro equipo y, lo más importante, contra ti, nuestro valioso cliente.

Entendemos que una situación como esta genera estrés y ansiedad sobre la seguridad de los datos de su tarjeta de pago en Target. Nuestra marca se ha construido sobre una base de 50 años de confianza con nuestros clientes y queremos asegurarle que se ha abordado la causa de este problema y que puede comprar con confianza en Target.

Queremos que sepas algunas cosas importantes:

El acceso no autorizado tuvo lugar en las tiendas Target de Estados Unidos entre el 27 de noviembre y el 15 de diciembre de 2013. Las tiendas canadienses y target.com no se vieron afectadas.

Incluso si compraste en Target durante este período, no significa que seas víctima de un fraude. De hecho, en otras situaciones similares, los niveles de fraude real suelen ser bajos.

No hay indicios de que los números PIN se hayan visto comprometidos en las tarjetas de débito con PIN emitidas por los bancos afectados o en las tarjetas de débito Target. Alguien no puede visitar un cajero automático con una tarjeta de débito fraudulenta y retirar dinero en efectivo.

Usted no será responsable de cargos fraudulentos; ni su banco ni Target tienen esa responsabilidad.

Estamos trabajando lo más rápido posible para brindarle la información que necesita. Nuestros huéspedes son siempre nuestra prioridad.

Para mayor seguridad, ofreceremos servicios gratuitos de monitoreo de crédito para todos los afectados. Nos comunicaremos con usted pronto para informarle cómo y dónde acceder al servicio.

Lea el aviso completo a continuación. En los próximos días y semanas, nos apoyaremos en target.com, abullseyeview.com, corporate.target.com y nuestros diversos canales sociales para responder preguntas y mantenerlo informado.

¡Gracias por su paciencia, comprensión y lealtad a Target!

Gregg Steinhafel Presidente, director general y director ejecutivo de Target

Fuente: Target Corporation, “Un mensaje del director ejecutivo Gregg Steinhafel sobre los problemas de las tarjetas de pago de Target”, Target Sitio web de la corporación, https://corporate.target.com/article/2013/12/important-notice-unauthorized-access-topayment-ca, consultado el 4 de mayo de 2016.

Anexo 9 Junta Directiva de Target Corporation en 2013

Roxanne S. Austin, 52 años. Presidenta de Austin Investment Advisors. Directora desde 2002.

Comités: Auditoría (Presidencia), Finanzas.

La Sra. Austin aporta al Directorio su experiencia en gestión financiera, operativa y de riesgos, así como un conocimiento sustancial de las nuevas tecnologías de medios, que desarrolló durante su anterior servicio como Presidenta y Directora de Operaciones de DirecTV, Vicepresidenta Ejecutiva y Directora Financiera de Hughes Electronics Corporation y Socia de Deloitte & Touche.

Douglas M. Baker, Jr., 53 años. Presidente y director ejecutivo de Ecolab Inc. Director desde 2013.

Comités: Auditoría, Nominaciones y Gobernanza.

El Sr. Baker aporta al Directorio una valiosa experiencia global en marketing, ventas y gestión general, así como perspectivas operativas y de gobernanza. Su función actual como director ejecutivo de una gran empresa que cotiza en bolsa proporciona al Directorio una perspectiva adicional de alto nivel en gestión organizacional.

Henrique De Castro, 47 años. Director de operaciones de Yahoo! Inc. Director desde 2013.

Comités: Responsabilidad Corporativa, Nominaciones y Gobernanza.

El Sr. De Castro aporta a la Junta Directiva una valiosa perspectiva sobre plataformas de medios, móviles y tecnológicas. Su experiencia en Yahoo! y Google, así como su experiencia previa en Dell Inc., le proporcionan perspectivas globales sobre la dirección de operaciones, estrategia, gestión de socios y generación de ingresos en las industrias de la tecnología y los medios.

Calvin Darden, 63 años. Presidente de Darden Development Group, LLC. Director desde 2003.

Comités: Compensación, Nominaciones y Gobernanza.

El Sr. Darden aporta a la Junta una experiencia significativa en redes de cadena de suministro, logística, servicio al cliente y gestión de una fuerza laboral a gran escala obtenida durante sus 33 años de carrera en United Parcel Service of America, Inc., y más recientemente ha desarrollado experiencia en relaciones comunitarias y desarrollo inmobiliario.

James A. Johnson, 69 años. Fundador de Johnson Capital Partners. Director desde 1996.

Comités: Compensación (Presidencia), Responsabilidad Corporativa.

El Sr. Johnson cuenta con más de 40 años de experiencia en los sectores público y empresarial. El Sr. Johnson aporta a la Junta Directiva una sólida capacidad de liderazgo y de creación de consenso, así como un sólido conocimiento de la dinámica de las políticas públicas, la gobernanza corporativa y las cuestiones de gestión de la reputación.

Mary E. Minnick, 53 años. Socia de Lion Capital. Directora desde 2005.

Comités: Auditoría, Responsabilidad Corporativa.

La Sra. Minnick aporta al Directorio una importante experiencia en la creación de conciencia de marca, gestión general, desarrollo de productos, marketing, distribución y ventas a escala mundial, adquirida a lo largo de sus 23 años de carrera en The Coca-Cola Company. Su puesto actual en Lion Capital proporciona al Directorio una visión adicional del negocio minorista y las tendencias de marketing de consumo fuera de los Estados Unidos.

Anne M. Mulcahy, 60 años. Presidenta del Consejo de Administración de Save The Children Federation, Inc. Director desde 1997.

Comités: Nominaciones y Gobernanza (Presidente), Finanzas.

La Sra. Mulcahy obtuvo una amplia experiencia en todas las áreas de gestión empresarial mientras dirigía a Xerox a través de un cambio radical. Esta experiencia, combinada con sus funciones de liderazgo en asociaciones comerciales y actividades de políticas públicas, proporciona al Directorio experiencia adicional en las áreas de eficacia organizacional, gestión financiera y gobierno corporativo.

Derica W. Rice, 48 años. Vicepresidenta ejecutiva de servicios globales y directora financiera de Eli Lilly and Company. Director desde 2008.

Comités: Finanzas (Presidencia), Auditoría.

La carrera del Sr. Rice en Eli Lilly le ha proporcionado una importante experiencia en la gestión de operaciones financieras a nivel mundial. Su experiencia aporta al Directorio habilidades adicionales en las áreas de supervisión financiera, gestión de riesgos y alineación de iniciativas financieras y estratégicas.

Gregg W. Steinhafel, 58 años. Presidente del Consejo de Administración, Director Ejecutivo y Presidente de Target. Director desde 2007.

Comités: Ninguno

En sus más de 30 años en Target, el Sr. Steinhafel ha adquirido una importante experiencia de liderazgo y conocimiento del sector minorista. Como director ejecutivo, es responsable de determinar la estrategia de Target y articular claramente las prioridades, así como de alinear y motivar a la organización para que se ejecute de manera eficaz y se garantice un éxito continuo. Estas capacidades, combinadas con el profundo conocimiento que tiene el Sr. Steinhafel de los clientes de Target y su compromiso inquebrantable con la marca Target, lo hacen excepcionalmente calificado para formar parte de la Junta Directiva.

John G. Stumpf, 59 años. Presidente del directorio, presidente y director ejecutivo de Wells Fargo & Company. Director desde 2010.

Comités: Compensación, Finanzas.

El papel actual del Sr. Stumpf como presidente, director general y director ejecutivo de Wells Fargo, y su larga trayectoria en el sector bancario, proporcionan al Consejo experiencia en gestión de marca, supervisión financiera y administración del capital.

Solomon D. Trujillo, 61 años. Director ejecutivo y director de Telstra Corporation Limited. Director desde 1994.

Comités: Responsabilidad Corporativa (Presidencia), Nominaciones y Gobernanza.

El Sr. Trujillo es un ejecutivo de negocios internacionales con tres décadas de experiencia como director general de grandes empresas globales de capitalización bursátil en las industrias de telecomunicaciones, medios y cable con sede en los Estados Unidos, la Unión Europea y la región de Asia y el Pacífico. Tiene experiencia en operaciones globales y aporta al Directorio una importante experiencia y conocimientos internacionales en las industrias de venta minorista, tecnología, medios y comunicaciones.

Fuente: Declaración de representación de Target 2013, consultada el 4 de mayo de 2016.

Anexo 10 Roxanne Austin, presidenta interina de Target, defiende a la junta directiva

A nuestros accionistas,

Al tomar sus decisiones de votación para nuestra Reunión Anual de 2014, queríamos que tuviera información sobre la supervisión de las prácticas de seguridad de la información en Target por parte de su Junta Directiva.

El cibercrimen es una amenaza real y persistente, ya que los delincuentes sofisticados buscan constantemente vulnerar las redes de información y robar datos. Las vulneraciones se producen en toda la economía y afectan a una amplia gama de víctimas, entre ellas el gobierno de los EE. UU., las industrias de tecnología y defensa y empresas más tradicionales, como los minoristas.

Su Junta Directiva reconoce plenamente la importancia de sus responsabilidades de supervisión en esta área. Bajo el liderazgo y la supervisión de la Junta Directiva, Target tomó medidas importantes para abordar los riesgos cambiantes de delitos cibernéticos antes de la filtración, mediante:

- Invertir cientos de millones de dólares en personal, procesos, tecnología y recursos relacionados de seguridad de red
- Dedicando más de 300 empleados a la seguridad de la información (más del doble que hace cinco años)
- Exigir capacitación anual sobre seguridad de datos para todos los empleados de Target (más de 350.000)
- Operar un Centro de Operaciones de Seguridad (SOC) con personal capacitado las 24 horas del día para revisar la actividad sospechosa en la red.
- Invertir en tecnología de monitoreo de red para mejorar la capacidad de Target de detectar posibles ciberataques
- Convertirse en miembro fundador de la National Cyber-Forensics & Training Alliance (NCFTA), una asociación de participantes públicos, privados y académicos enfocada en identificar, mitigar y neutralizar las ciberamenazas.

A pesar de estos esfuerzos, Target sufrió un sofisticado ataque criminal que condujo a la violación de datos en 2013. Desde entonces, su Junta ha monitoreado activamente la respuesta de Target a la situación. Después de la violación, la Junta ha supervisado esfuerzos sustanciales para proteger a los clientes de Target. Target está realizando una revisión integral de la seguridad de su red y está avanzando hacia la tecnología de chip y PIN para el procesamiento de tarjetas de crédito. La Junta está realizando un examen amplio de la estructura de supervisión de riesgos de Target, que incluirá un examen del papel de la alta gerencia, las estructuras de informes y la supervisión de la Junta.

Target ya ha hecho lo siguiente:

- Anunciamos que estamos acelerando la adopción de la tecnología de tarjetas de pago inteligentes con “chip y PIN” y fijamos objetivos importantes para 2015, entre ellos:
  - Conversión de todas nuestras tarjetas REDcard a tarjetas con chip
  - Equipar nuestras tiendas con lectores de tarjetas con chip
- Se contrató a un nuevo Director de Información
- Elevó los roles de Director de Seguridad de la Información y Director de Cumplimiento y comenzó búsquedas para cubrir esos puestos.

- Procesos mejorados de toma de decisiones sobre seguridad de la información
- Trabajó con otros minoristas líderes para establecer el Centro de análisis e intercambio de información minorista (Retail-ISAC) y se unió al Centro de análisis e intercambio de información de servicios financieros (FSISAC) como el primer miembro minorista del grupo.

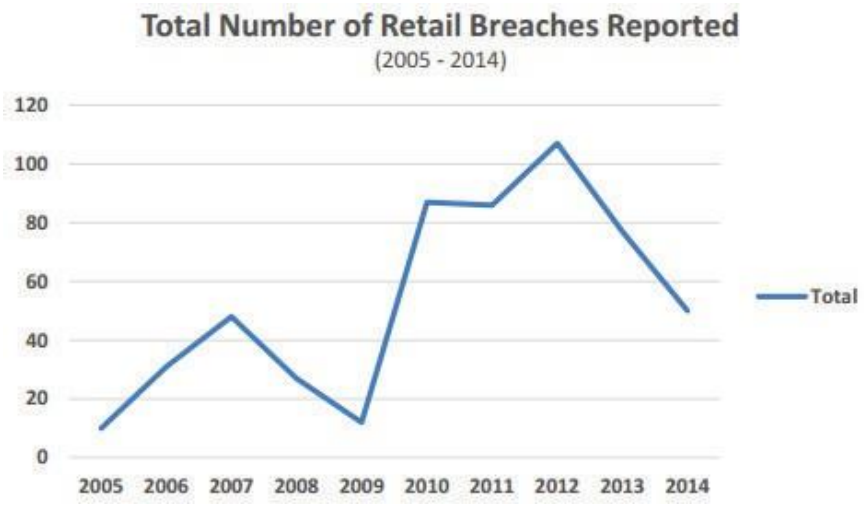
Nuevamente, queremos asegurarle que la Junta Directiva toma en serio sus responsabilidades de supervisión y reconocemos la importancia de que Target aborde estos problemas de seguridad de la información de la manera más eficaz posible. Agradeceríamos sus comentarios sobre este importante tema. Si desea compartir sus opiniones y comentarios, envíe un mensaje a BoardOfDirectors@target.com . También valoramos su apoyo y le pedimos que vote a favor de la reelección de todos los directores de Target en nuestra Reunión Anual de 2014.

Roxanne Austin, presidenta interina de la junta directiva

Fuente: Target Def 14A presentado el 2 de junio de 2014, consultado el 12 de mayo de 2016.

Anexo 11 Grandes ciberataques a minoristas

Según informes del sector, los ciberataques en el sector minorista han aumentado drásticamente desde 2009, y en 2012 se registraron más de 100 infracciones en el sector minorista:



Durante este período, los piratas informáticos atacaron a menos minoristas, pero de mayor tamaño, con acceso a grandes porciones de la población estadounidense: TJX Companies (2007, 100 millones), The Home Depot (2014, 56 millones), The Valve Corporation (2011, 35 millones) y Sony PlayStation Network (2011, 12 millones).

Los expertos del sector descubrieron que más del 99 % de los ataques explotaban directamente un punto final objetivo o implementaban malware con éxito. Una de las razones por las que estas estrategias habían tenido éxito era la falta de validación de datos por parte de los administradores de seguridad y la complejidad innata de protegerse contra un gran volumen de ataques. Como resultado, la piratería y el malware se convirtieron en el método de ataque más popular y, entre 2005 y 2014, se perdieron más de 300 millones de registros únicamente por estos métodos.

Fuente: David McMillen, IBM Research and Intelligence Report, IBM Corporation, 6 de enero de 2015.

Anexo 12a Industrias que fueron blanco de ataques cibernéticos, 2011-2013

Sector industrial	# de Infracciones 2011	% de Total Infracciones 2011	# de Infracciones 2012	% de Total Infracciones 2012	# de Infracciones 2013	% de Total Infracciones 2013
Negocio	177	42%	162	34%	195	32%
Educativo	57	14%	63	13%	54	9%
Gobierno/Militar	54	13%	55	12%	60	10%
Salud/Medicina	102	24%	167	36%	271	44%
Financiero/Crédito	31	7%	24	5%	34	6%
Total	**421**		**471**		**614**	

Anexo 12bTécnicas utilizadas por los ciberdelincuentes, 2011-2013

Tipo de incidente	# de Infracciones 2011	% de Total Infracciones 2011	# de Infracciones 2012	% de Total Infracciones 2012	# de Infracciones 2013	% de Total Infracciones 2013
Robo interno	56	13%	40	9%	72	12%
Seco	110	26%	128	27%	160	26%
Datos en movimiento	78	19%	57	12%	79	13%
Exposición accidental	45	11%	41	9%	46	8%
Subcontratista	32	8%	54	12%	89	15%
Negligencia del empleado			34	7%	58	10%

Anexo 12cPérdida de datos de consumidores, 2011-2013

Categoría	# de Infracciones 2011	% de Total Infracciones 2011	# de Infracciones 2012	% de Total Infracciones 2012	# de Infracciones 2013	% de Total Infracciones 2013
Papel	68	16%	72	15%	73	12%
Totales desconocidos	172	41%	237	50%	243	40%
Números de Seguro Social Expuestos	260	62%	226	48%	295	48%
Tarjetas de Crédito/Débito Expuestas	111	26%	68	14%	96	16%
Atributos Desconocidos	133	32%	163	35%	176	29%

Fuente: Centro de recursos sobre robo de identidad, http://www.idtheftcenter.org/images/breach/2005to2015multiyear.pdf, Consultado el 4 de mayo de 2016.

Anexo 13 Resultados de la elección de la junta directiva de Target, 2014 (en miles)

	Para		Contra	
Candidato	**Acciones**	**%**	**Acciones**	**%**
Roxanne S. Austin	382.077	78.0	107.814	22.0
Douglas M. Baker, Jr.	467.403	95,5	22.107	4.5
Calvin Darden	389.118	79,5	100.313	20.5
Henrique De Castro	396.684	81.0	93.130	19.0
James A. Johnson	307.783	62.9	181.383	37.1
María E. Minnick	391.561	80.0	97.848	20.0
Anne M. Mulcahy	310.851	63.6	177.938	36.4
Derica W. Rice	393.117	80.3	96.243	19.7
Kenneth L. Salazar	475.251	97.1	14.167	2.9
Juan G. Stumpf	464.751	94.9	24.829	5.1

Fuente: Objetivo, Formulario 8-K 2014, consultado el 4 de mayo de 2016.

Notas finales

1 Corporación Target, Formulario 10-K de 2013.

2 Target Corporation, "Target a través de los años", sitio web de Target Corporation, https://corporate.target.com/about/history/Target-through-the-years, consultado el 1 de mayo de 2016.

3 K. Palepu, S. Srinivasan y J. Weber, "Target Corporation: Ackman versus la Junta Directiva", HBS No. 109-010 (Boston: Harvard Business School Publishing, 2011).

4 "Informe sobre acciones de Target Corp.", S&P Capital IQ, 25 de marzo de 2014.

5 Ibíd.

6 Ibíd. (CAGR son cálculos de los autores).

7. Corporación objetivo, 2013 10-K.

8 Target Corporation, "Target Reports Third Quarter 2013 Earnings", sitio web de Target Corporation, http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1878983, consultado el 26 de mayo de 2016.

9 Target Corporation, "Target Corporation aumenta el dividendo trimestral regular en un 19 por ciento", sitio web de Target Corporation, http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1829310, consultado el 26 de mayo de 2016.

10 Brad Dorfman, "El director ejecutivo de Target ve resurgir a los compradores", Reuters, 7 de mayo de 2010.

11 Corporación Target, 2013 10-Q.

12 Corporación Target, 2013 10-K.

13 Target Corp., 2010 10-K; Target Corp., 2011 10-K; Target Corp., 2012 10-K; Target Corp., 2013 10-K; y cálculos del autor.

14 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

15 SearchSecurity, "phishing", sitio web de SearchSecurity,http://searchsecurity.techtarget.com/definition/phishing, consultado el 2 de mayo de 2016.

16 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

17 Ibíd.

18 Ibíd.

19 Brian Krebs, "Ataque por correo electrónico a un proveedor que configura una brecha en Target",*Krebs sobre seguridad*(blog), 14 de febrero de 2014.

20 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

21 Brian Krebs, "Ataque por correo electrónico a proveedor configura brecha en Target".

22 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

23 Ibíd.

24 Ibíd.

25 SearchSecurity, "malware (software malicioso)", sitio web SearchSecurity, http://searchmidmarketsecurity.techtarget.com/definition/malware, consultado el 2 de mayo de 2016.

26 Matthew J. Schwartz, "Target Breach: 8 datos sobre malware de extracción de memoria",*Lectura oscura*14 de enero de 2014.

27 Comité Senatorial de Comercio, Ciencia y Transporte,*Un análisis de la "cadena de muerte" de la filtración de datos de Target en 2013*113El Congreso, 2Dakota del Nortesesión, 2014.

28 N. Perlroth, "Investigación sobre robo de datos de tarjetas de crédito en Target",*El New York Times*, 19 de diciembre de 2013.

29 Comité Senatorial de Comercio, Ciencia y Transporte,*Un análisis de la "cadena de muerte" de la filtración de datos de Target en 2013*113El Congreso, 2Dakota del Nortesesión, 2014.

30 Ibíd.

31 Ibíd.

32 Corporación Target, 2013 10-K.

33 Elizabeth A. Harris y Nicole Perlroth, "Para Target, las cifras de infracciones aumentan", *El New York Times* 10 de enero de 2014.

34 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

35 Ibíd.

36 Ibíd.

37 Mellisa Tolentino, "¿Qué tiendas abren temprano el Día de Acción de Gracias? Vencer al Viernes Negro", *Ángulo de silicio* 26 de noviembre de 2014.

38 Emily J. Fox, "Los trabajadores de Wal-Mart planean una huelga el Viernes Negro", CNN Money, 15 de noviembre de 2012.

39 Comité Senatorial de Comercio, Ciencia y Transporte, *Un análisis de la "cadena de muerte" de la filtración de datos de Target en 2013* 113 El Congreso, 2 Dakota del Norte sesión, 2014.

40 Kevin Fogarty, "Informe: los jefes de Target ignoraron la alerta de TI sobre una violación inminente", *Dados* 13 de marzo de 2014.

41 Robert Lemos, "La violación de un objetivo implicó un ciberataque en dos etapas: investigadores de seguridad", *Semana electrónica*, 21 de enero de 2014.

42 Kevin Fogarty, "Informe: los jefes de Target ignoraron la alerta de TI sobre una violación inminente".

43 Mary Shacklett, "La opinión de un ex CIO sobre la renuncia del CIO de Target después de una filtración masiva de datos", *República tecnológica* 13 de marzo de 2014.

44 Ibíd.

45 Target Corporation, "Testimonio de John Mulligan", sitio web de Target Corporation, https://corporate.target.com/_media/TargetCorp/global/PDF/Target-SJC-020414.pdf, consultado el 26 de mayo de 2016.

46 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

47 Meagan Clark, "Cronología de la violación de datos de Target y sus consecuencias: cómo el robo cibernético se convirtió en una bola de nieve para el gigante minorista", *Tiempos de negocios internacionales* 5 de mayo de 2014.

48 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

49 Ibíd.

50 Becky Quick y Matthew J. Belvedere, "El director ejecutivo de Target 'todavía conmocionado' por la filtración de datos, promete 'hacerlo bien'", CNBC, 12 de enero de 2014.

51 Natalie Burg, "Cinco lecciones para todas las empresas a partir de la filtración de datos de Target", *Forbes Negocios* 17 de enero de 2014.

52 Comité Senatorial de Comercio, Ciencia y Transporte, *Un análisis de la "cadena de muerte" de la filtración de datos de Target en 2013* 113 El Congreso, 2 Dakota del Norte sesión, 2014.

53 Brian Krebs, "Fuentes: objetivo que investiga una violación de datos", *Krebs sobre seguridad* (blog), 18 de diciembre de 2013.

54 Ibíd.

55 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

56 Servicios de investigación del Congreso, El objetivo y otras violaciones de datos financieros: preguntas frecuentes, 114 El Congreso, 1 calle sesión. 2015.

57 Target Corporation, "Target confirma acceso no autorizado a datos de tarjetas de pago en tiendas de EE. UU.", sitio web de Target Corporation, https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-paid-car, consultado el 4 de mayo de 2016.

58 Tim Feran, "Una mujer de Delaware entre las víctimas de la violación de datos de Target", *Despacho de Colón*, 20 de diciembre de 2013.

59 Beth Pinsker, "Los consumidores expresan su frustración y enojo por la violación de datos de Target", Reuters, 13 de enero de 2014.

60 Target Corporation, "Target invierte $5 millones en una coalición de ciberseguridad", sitio web de Target Corporation, https://corporate.target.com/article/2014/02/target-to-invest-5-million-in-cybersecurity-coalit, consultado el 4 de mayo de 2016.

61 Target Corporation, "Un mensaje del director ejecutivo Gregg Steinhafel sobre los problemas con las tarjetas de pago de Target", sitio web de Target Corporation,https://corporate.target.com/article/2013/12/important-notice-unauthorized-access-to-paid-ca, consultado el 4 de mayo de 2016.

62 Eric Weibel, "La violación de datos de Target destaca la necesidad de que las empresas adquieran un seguro cibernético",*Examinador*, 21 de diciembre de 2013.

63 Target Corporation, "Un mensaje del director ejecutivo Gregg Steinhafel sobre los problemas con las tarjetas de pago de Target".

64 Ibíd.

65 Meagan Clark, "Cronología de la violación de datos de Target y sus consecuencias: cómo el robo cibernético se convirtió en una bola de nieve para el gigante minorista".

66 Target Corporation, "Un mensaje del director ejecutivo Gregg Steinhafel sobre los problemas con las tarjetas de pago de Target".

67 Ibíd.

68 Ibíd.

69 Aimee Picchi, "Los clientes se ponen furiosos por la respuesta de Target al hackeo",*Reloj de dinero*, 20 de diciembre de 2013.

70 Brian Krebs, "Las tarjetas robadas en la filtración de Target inundan los mercados clandestinos",*Krebs sobre seguridad*(blog), 20 de diciembre de 2013.

71 Ibíd.

72 Jim Finkle y David Henry, "Exclusivo: Los piratas informáticos objetivo robaron PIN bancarios encriptados—fuente", Reuters, 25 de diciembre de 2013.

73 David Goldman, "Target confirma que los datos del PIN fueron robados en una violación de seguridad", CNN Money, 27 de diciembre de 2013.

74*Banco Amalgamated contra Corporación Target*, No. 14-cv-00263-DWF-SER, Queja (D. Minn. presentada el 28 de enero de 2014).

75 David Goldman, "Target confirma que los datos del PIN fueron robados en una violación de seguridad".

76 Meagan Clark, "Cronología de la violación de datos de Target y sus consecuencias: cómo el robo cibernético se convirtió en una bola de nieve para el gigante minorista".

77 Maggie McGrath, "La filtración de datos de Target reveló información sobre hasta 70 millones de clientes",*Forbes*10 de enero de 2014.

78*Kulla contra Steinhafel*, No 0:14-cv-00203, Queja (D. Minn. presentada el 21 de enero de 2014).

79 Hadley Malcolm, "Objetivo: Datos robados de hasta 70 millones de clientes",*EE.UU. hoy*10 de enero de 2014.

80 Aimee Picchi, "Tras una violación de seguridad, la marca Target sufre un duro golpe",*Observatorio de dinero de CBS*, 27 de diciembre de 2013.

81 Becky Quick y Matthew J. Belvedere, "El director ejecutivo de Target 'aún está conmocionado' por la filtración de datos y promete 'remediarlo'".

82 Sara Germano, Robin Sidel y Danny Yadron, "Target enfrenta una reacción violenta después de una violación de seguridad de 20 días",*El diario Wall Street* En línea, 19 de diciembre de 2013.

83 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

84 Danny Yadron, Paul Ziobro y Devlin Barrett, "Se advirtió al objetivo de vulnerabilidades antes de la filtración de datos",*El diario Wall Street*14 de febrero de 2014.

85 Comité Senatorial de Comercio, Ciencia y Transporte,*Un análisis de la "cadena de muerte" de la filtración de datos de Target en 2013*113El Congreso, 2Dakota del Nortesesión, 2014.

86 Danny Yadron et al., "Se advirtió al objetivo sobre vulnerabilidades antes de la filtración de datos".

87 Target Corporation, "Testimonio de John Mulligan", sitio web de Target Corporation, https://corporate.target.com/_media/TargetCorp/global/PDF/Target-SJC-020414.pdf, consultado el 26 de mayo de 2016.

88 Jennifer Bjorhus, "Las reseñas limpias precedieron a la filtración de datos de Target y otras",*Tribuna estelar*31 de marzo de 2014.

89 Kim Zetter, "¿La demanda de Target finalmente expondrá las fallas de las auditorías de seguridad?"*Con cable*28 de marzo de 2014.

90 Ibíd.

91 Ibíd.

92 Ibíd.

93 Ibíd.

94 Jennifer Bjorhus, "Las reseñas limpias precedieron a la filtración de datos de Target y otras".

95 Ibíd.

96 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

97 Comité Senatorial de Comercio, Ciencia y Transporte, *Un análisis de la "cadena de muerte" de la filtración de datos de Target en 2013* 113 El Congreso, 2 Dakota del Norte sesión, 2014.

98 Target Corporation, "Ventas totales del segmento: cambio porcentual respecto del año anterior", sitio web de Target Corporation, http://investors.target.com/phoenix.zhtml?c=65828&p=irol-summaryfinancial, consultado el 26 de mayo de 2016.

99 Elizabeth A. Harris, "La filtración de datos perjudica las ganancias de Target", *El New York Times* 26 de febrero de 2014.

100 datos de Capital IQ.

101 Kevin M. McGinty, "El precio de la filtración de datos de Target: 252 millones de dólares y sigue aumentando", *Cuestiones de privacidad y seguridad* 26 de febrero de 2015.

102 Kaleigh Simmons, "Todo lo que necesita saber sobre las demandas por violación de datos de Target", *Onda de choque* 4 de febrero de 2015.

103 Jay Rockefeller IV, "Rockefeller: Informe del personal detalla las oportunidades perdidas de Target para detener la filtración masiva de datos", *Voto inteligente* 25 de marzo de 2014.

104 TGB Security, "El director financiero de Target interrogado en una audiencia del Senado", sitio web de TGB Security, https://tbgsecurity.com/target-cfo-grilledin-senate-hearing-bankinfosecurity/, consultado el 6 de mayo de 2016.

105 Elizabeth A. Harris, "El objetivo tuvo la oportunidad de detener la violación, dicen los senadores", *El New York Times* 26 de marzo de 2014.

106 D. Skariachan y J. Finkle, "Target se reúne con fiscales estatales mientras se acumulan demandas", Reuters, 23 de diciembre de 2013.

107 Jeffrey Roman, "El director financiero de Target interrogado en una audiencia del Senado", *Seguridad de la información bancaria* 27 de marzo de 2014.

108 Jim Spencer y Jennifer Bjorhus, "Target pasó por alto múltiples advertencias sobre violaciones de datos, según un informe del Senado", *Tribuna estelar* 27 de marzo de 2014.

109 *Davis contra Steinhafel*, No. 0:14-cv-00203, Brief (D. Minn. presentado el 8 de mayo de 2014).

110 Gregory Wallace y Gabrielle Solomon, "Black Thursday? Thanksgiving sales numbers growing", CNN Money, 30 de noviembre de 2014.

111 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

112 Fundamentos de criptografía, "Target", sitio web Fundamentos de criptografía, http://cryptofundamentals.com/target, consultado el 27 de mayo de 2016.

113 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

114 Ibíd.

115 Keller Rohrback, "Target Data Breach", sitio web de Keller Rohrback, http://krcomplexlit.com/currentcases/target-databreach/, consultado el 7 de mayo de 2016.

116 Y. Peter Kang, "El acuerdo de 10 millones de dólares de Target por la violación de datos obtiene la aprobación final", *Ley360* 17 de noviembre de 2015.

117 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522, Queja (D. Minn. presentada el 25 de agosto de 2014).

118 Jim Finkle y Mark Hosenball, "Exclusivo: Más minoristas estadounidenses conocidos víctimas de ataques cibernéticos (fuentes)".

119 Ibíd.

120 Ibíd.

121 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522-PAM, Declaración de Charles S. Zimmerman (D. Minn. presentada el 2 de diciembre de 2015).

122 *Banco Amalgamated contra Corporación Target*, No. 14-cv-00263-DWF-SER, Queja (D. Minn. presentada el 28 de enero de 2014).

123 Ibíd.

124 Jonathan Stempel y Nandita Bose, "Target llega a un acuerdo por 39,4 millones de dólares con bancos por violación de datos", Reuters, 2 de diciembre de 2015.

125 En re: Litigio por violación de seguridad de datos de clientes de Target Corp., No 0:14-md-02522-PAM, Declaración de Charles S. Zimmerman (D. Minn. presentada el 2 de diciembre de 2015).

126 *Banco Amalgamated contra Corporación Target*, No. 14-cv-00263-DWF-SER, Queja (D. Minn. presentada el 28 de enero de 2014).

127 Matthew Heller, "Encuesta muestra el costo de las violaciones de Target en los bancos", *director de Finanzas* sitio web, http://ww2.cfo.com/fraud/2014/09/survey-shows-toll-target-breach-banks/, consultado el 7 de mayo de 2016.

128 Tracy Kitten, "Violación de Target: MasterCard evalúa un nuevo acuerdo", *Seguridad de la información bancaria* 20 de agosto de 2015.

129 Jonathan Stempel y Nandita Bose, "Target llega a un acuerdo de 39,4 millones de dólares con los bancos por la filtración de datos".

130 Ibíd.

131 *Davis contra Steinhafel*, No. 0:14-cv-00203, Brief (D. Minn. presentado el 8 de mayo de 2014).

132 *Kulla V. Steinhafel*, No 0:14-cv-00203, Queja (D. Minn. presentada el 21 de enero de 2014).

133 Ibíd.

134 Ibíd.

135 Ibíd.

136 Ibíd.

137 *Davis V. Steinhafel*, No 0:14-cv-00261, Queja (D. Minn. presentada el 28 de enero de 2014).

138 Ibíd.

139 *Davis contra Steinhafel*, No. 0:14-cv-00203, Brief (D. Minn. presentado el 8 de mayo de 2014).

140 Target Corporation, "Estatuto del Comité de Auditoría y Finanzas", sitio web de Target Corporation, http://investors.target.com/phoenix.zhtml?c=65828&p=irol-govcommittees, consultado el 11 de mayo de 2016.

141 Ibíd.

142 Donna Dabney, "¿Acertó ISS al recomendar un voto en contra de los directores de Target?", sitio web de The Conference Board, http://tcbblogs.org/governance/2014/06/04/did-iss-get-it-right-in-recommending-a-vote-against-targets-directors/, consultado el 7 de mayo de 2016.

143 Ibíd.

144 "Target Corporation Proxy Statement and Notice of Annual Meeting of Shareholders", Presentación ante la SEC, 19 de mayo de 2014, consultado el 7 de mayo de 2016.

145 Target Corp., 2012 10-K, pág. 7, https://corporate.target.com/_media/TargetCorp/annualreports/content/download/pdf/Annual-Report.pdf?ext=.pdf.

146 "Target Corporation", ISS Proxy Advisory Services, 27 de mayo de 2014.

147 Ibíd.

148 Ibíd.

149 Ibíd.

150 Ibíd.

151 Ibíd.

152 Ibíd.

153 "Documento de representación—Target Corporation", Glass Lewis & Co., 27 de mayo de 2014.

154 Ibíd.

155 Nick Halter, "La presidenta de Target defiende el manejo de la violación de datos por parte de la junta directiva",*Revista de negocios de Minneapolis/St. Paul*En línea el 2 de junio de 2014.

156 Ibíd.

157 Donna Dabney, "¿ISS hizo lo correcto al recomendar un voto en contra de los directores de Target?"

158 Wayne Hood y Shannon Coyne, "Target: Comentarios tras reunión de analistas del lado vendedor", BMO Capital Markets, 2 de junio de 2014.