FORESCOUT

EL PAPEL DE LA CIBERSEGURIDAD EN LA DILIGENCIA DE FUSIONES Y ADQUISICIONES

Un estudio de investigación para comprender mejor los riesgos de ciberseguridad a los que se enfrentan las empresas al adquirir otra empresa.

OBJETIVO DE ESTE ESTUDIO

Este estudio fue diseñado para analizar la creciente preocupación por los ciberriesgos y la importancia de la evaluación de la ciberseguridad durante fusiones y adquisiciones (M&A, Mergers and Acquisitions), así como para determinar el nivel de preparación de las empresas para gestionar el ciberriesgo durante M&A desde el punto de vista de los responsables de la toma de decisiones de IT (ITDM, IT Decision Makers) y los responsables de la toma de decisiones empresariales (BDM, Business Decision Makers).

¿Están preocupados los principales responsables de la toma de decisiones por la ciberseguridad durante una adquisición? ¿Qué factores se consideran parte de la diligencia debida y el proceso de evaluación antes, durante y después de la adquisición? ¿Generan los ciberincidentes retrasos en la adquisición? ¿Qué significa el ciberriesgo para las empresas que buscan adquirir otras empresas? ¿Qué pueden hacer para protegerse mejor durante este importante proceso para minimizar el riesgo y proteger sus empresas? Este informe analiza estas y otras cuestiones, y ofrece recomendaciones para gestionar de forma eficaz los riesgos de ciberseguridad durante una adquisición.

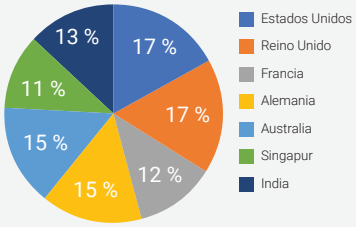
Este estudio e informe fue encargado por Forescout Technologies con encuestados procedentes de Quest Mindshare.

ACERCA DEL ESTUDIO

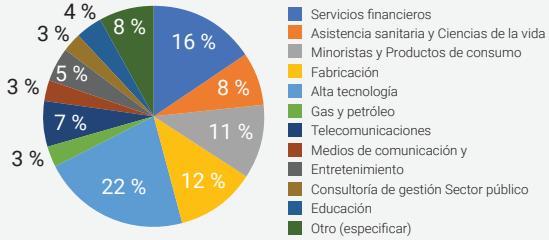
Este informe se basa en una encuesta llevada a cabo entre el 20 de febrero y 10 de marzo de 2019, y fue encargada por Forescout Technologies con encuestados procedentes de Quest Mindshare, con el fin de comprender el ciberriesgo dentro del ciclo de vida de las fusiones y adquisiciones. Participaron un total de 2779 personas de todo el mundo. Para este estudio, se eligieron dos públicos: responsables de la toma de decisiones de IT (ITDM; n=1283) y responsables de la toma de decisiones empresariales (BDM; n=1496). Los datos fueron ponderados para representar equitativamente los públicos y regiones. Para poder participar, los encuestados tenían que ser empleados a tiempo completo, nivel de alta dirección o superior, y principal responsable de la toma de decisiones para compras de IT o implicado en la estrategia de M&A. La encuesta se realizó en Estados Unidos, Francia, Reino Unido, Alemania, Australia, Singapur e India El margen de error es+/- 1,73 puntos porcentuales.

Porcentaje de encuestados

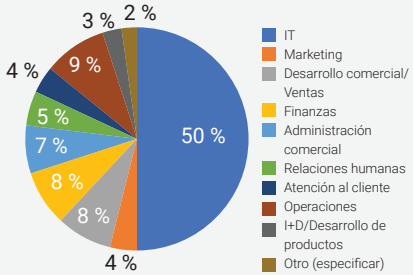
País



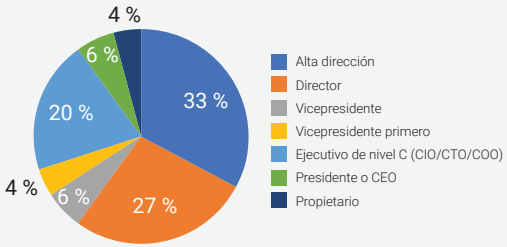
Actividad principal



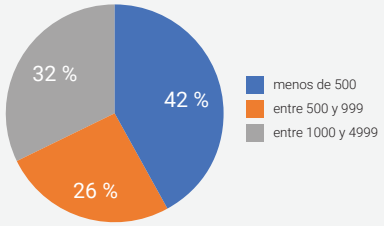
Cargo



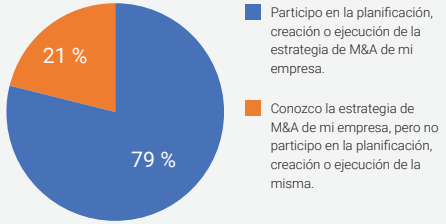
Nivel laboral



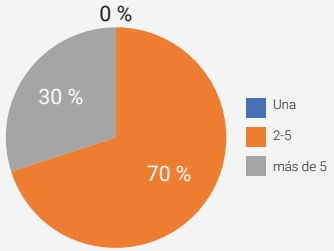
Número de empleados

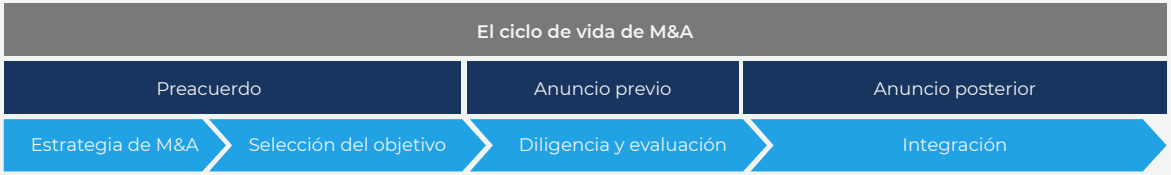


Nivel de implicación



Número de M&A en las que ha participado





RESUMEN EJECUTIVO

Según Gartner, para 2022 el 60 % de las organizaciones que participen en actividades de fusiones y adquisiciones considerará el nivel de ciberseguridad un factor crítico1 en su proceso de diligencia debida, frente a menos del 5 % actual. En nuestra encuesta realizada entre 2779 responsables de la toma de decisiones de IT y empresariales de todo el mundo, el 73 % de los encuestados afirmó que la adquisición de tecnología es su principal prioridad dentro su estrategia de M&A en los próximos 12 meses, y el 62 % que la empresa no solo se enfrenta a un importante riesgo de ciberseguridad al adquirir nuevas empresas, sino que ese ciberriesgo es

Si bien las empresas que forman parte de un acuerdo pueden respetar las cláusulas de limitación, el malware no conoce límites. Una vez que está conectado, los ciberdelincuentes camparán a sus anchas a menos que tome las medidas preceptivas adecuadas.

su principal preocupación tras la adquisición

El riesgo de ciberseguridad es un reto y una preocupación creciente por una serie de razones. El error humano ha sido tradicionalmente señalado como uno de los culpables de los ataques a la red, siendo la negligencia humana y la curiosidad innata mencionadas a menudo como las principales razones2 de un incidente de seguridad o fuga de los datos. Sin embargo, el panorama de las Tecnologías de las Información (IT, Information Technologies) y de la ciberseguridad ha cambiado de manera dramática en las últimas décadas, trayendo tanto avances técnicos como nuevos riesgos. El nacimiento del Internet de las cosas (IoT) ha alterado la forma de vivir y comunicarse de las personas, y con unas previsiones que anticipan que el número de dispositivos IoT sobrepasará los 20 400 millones para 2020[3], también se precisan enfoques innovadores para gestionar los ciberriesgos de IoT. En nuestra encuesta, el 72 % de los participantes consideró los dispositivos IoT (impresoras, iluminación inteligente, teléfonos VoIP, cámaras de seguridad, etc.) como los más vulnerables frente a los actores maliciosos externos. Los dispositivos IoT también juegan un papel en la convergencia actual de la tecnología de IT tradicional con la Tecnología Operativa (OT, Operational Technology), lo que puede exponer potencialmente las redes operativas que anteriormente eran muchos más difíciles de atacar.

Ha habido una gran cantidad de cambios y avances en los últimos años, pero el aumento de la conectividad también ha ofrecido a los adversarios oportunidades de lanzar ataques maliciosos, robar de ámbito limitado puede tener muchas repercusiones financieras reales, tanto para la empresa que se adquiere como para la empresa compradora, tal y como lo prueba la reducción del precio de adquisición de 350 millones de dólares4 como consecuencia de las revelaciones de las violaciones de la seguridad de los datos de Yahoo!, así como la indemnización 1,5 millones de dólares5 por una fuga de datos que los grandes almacenes

Estrategia de fusiones y adquisiciones para los próximos 12 meses

El 73 %

afirma que la adquisición de tecnología es su principal prioridad dentro de su estrategia de M&A para los próximos 12 meses

El 62 %

afirma que su empresa se enfrenta a un riesgo de ciberseguridad importante al adquirir otras empresas, y que esta es su mayor preocupación tras la adquisición.

[1] *Cybersecurity is Critical to the M&A Due Diligence Process, Gartner (La ciberseguridad es esencial para el proceso de diligencia debida de fusiones y adquisiciones), abril de 2018, https://www.gartner.com/en/documents/3873604*

[2] *The biggest cybersecurity risk to US businesses is employee negligence (El mayor riesgo de ciberseguridad para las empresas estadounidenses es la negligencia de los empleados), CNBC, junio de 2018, https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html*

[3] *8.4 Billion Connected "Things" Will be in Use in 2017 (8400 millones de "cosas" conectadas estarán en uso en 2017), Gartner, febrero de 2017, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016*

Neiman Marcus tuvieron que pagar, a pesar de que el cuerdo de adquisición ya se había cerrado.

La diligencia de M&A ha dado prioridad, entre otros, a los departamentos Financiero, Legal, Comercial, Operaciones, Recursos Humanos e IT. Los resultados de la encuesta sugieren que, aunque existe un reconocimiento de los ciberriesgos potenciales durante una adquisición, las empresas que estén estudiando realizar una adquisición podrían beneficiarse de una evaluación de ciberseguridad dedicada mayor. Los resultados también sugieren que la evaluación y la diligencia debida no deberían ser un ejercicio puntual, sino una actividad permanente. Y aunque debe ser así, las empresas compradoras no pueden ir muy lejos en sus investigaciones y procesos de diligencia debida por lo que, intrínsecamente, toda adquisición comporta siempre un cierto riesgo. Nunca sabe realmente lo que tiene hasta que está conectado, y eso hace mucho más importante evaluar tanto como pueda y de la forma más minuciosa posible antes de la integración. Si bien las empresas que forman parte de un acuerdo pueden respetar las cláusulas de limitación, el malware no conoce límites. Una vez que está conectado, los ciberdelincuentes camparán a sus anchas a menos que tome las medidas preceptivas adecuadas.

[4] Verizon cuts Yahoo deal price by $350 million (Verizon recorta el precio del acuerdo de Yahoo en 350 millones de dólares) CNN, febrero de 2017, https://money.cnn.com/2017/02/21/technology/yahoo-verizon-deal/index.html

[5] Neiman Marcus to pay $1.5M settlement over 2013 data breach (Neiman Marcus obligado a pagar una indemnización de 1,5 millones de dólares por una fuga de datos en 2013) RetailDive, enero de 2019, https://www.retaildive.com/news/neiman-marcus-to-pay-15m-settlement-over-2013-data-breach/545641/

RESULTADOS PRINCIPALES

- Los problemas de ciberseguridad son prevalentes y pueden poner en peligro un acuerdo. Más de la mitad de los encuestados (53 %) afirma que su empresa experimentó un problema o incidente de ciberseguridad crítico durante un acuerdo de M&A que puso en peligro la operación.
- Las empresas prestan más atención al nivel de ciberseguridad de una empresa objetivo que lo hacían antes: el 80 % de ITDM y BDM coincidió en que prestan más atención al nivel de ciberseguridad de un objetivo que en el pasado, haciendo hincapié en que es una principal prioridad tanto para responsables de la toma de decisiones de IT como empresariales.
- Una fuga de datos no revelada constituye para la mayoría de las empresas un motivo de ruptura de un acuerdo: el 73 % de los encuestados afirmó que una empresa con un incidente de fuga de datos no revelado es un motivo de ruptura inmediata del acuerdo en la estrategia M&A de la empresa.
- En ocasiones, los responsables de la toma de decisiones sienten que no disponen de tiempo suficiente para llevar a cabo una evaluación de la ciberseguridad. Solo el 36 % afirma con rotundidad que su equipo de IT dispone del tiempo necesario para revisar los estándares, procesos y protocolos de ciberseguridad de la empresa antes de que su empresa adquiera otra.
- Los equipos internos de IT pueden carecer de las competencias necesarias para realizar evaluaciones de ciberseguridad: entre los ITDM, solo el 37 % coincide plenamente en que su equipo de IT que cuenta con los conocimientos necesarios para llevar a cabo una evaluación de ciberseguridad para una adquisición.
- Las empresas asignan recursos externos a sus evaluaciones de ciberseguridad: casi todos los encuestados (97 %) afirmaron que sus empresas gastan dinero en contratistas externos para las auditorías de IT o de evaluación de riesgos de seguridad.
- Los dispositivos conectados y el error humano ponen en riesgo a las empresas: cuando se les preguntó qué es lo que más pone en riesgo a las empresas durante el proceso de información y tecnología, destacaron dos respuestas: el error humano y una configuración deficiente (51 %), y los dispositivos conectados (50 %).
- Durante la integración, a menudo se pasan por alto o se pierden dispositivos: más de la mitad (53 %) de los ITDM afirman que encuentran dispositivos de los que se desconoce su existencia tras finalizar la integración de una nueva adquisición.
- No hacer caso al riesgo de ciberseguridad puede hacer que las empresas se arrepientan de llevar a cabo una adquisición: casi dos terceras partes de los encuestados (65 %) afirmaron que sus empresas lamentaron haber cerrado un acuerdo de fusión y adquisición por cuestiones de ciberseguridad.

PANORAMA DEL CIBERRIESGO ACTUAL EN FUSIONES Y ADQUISICIONES

Los problemas de ciberseguridad son prevalentes y pueden poner en peligro un acuerdo.

53 %

Más de la mitad de los encuestados (53 %) afirma que su empresa experimentó un problema o incidente de ciberseguridad crítico durante un acuerdo de M&A que puso en peligro la operación.

EE. UU.	RU	FR	ALE	AUS	SG	IN
47 %	52 %	61 %	56 %	40 %	50 %	63 %

Las compañías se funden con otras empresas o las adquieren por una gran cantidad de razones: más eficiencias, acceso a un mercado de mayor envergadura, propiedad intelectual o ventajas competitivas, o influencia sobre la cadena de suministro, por nombrar solo algunas. Tanto si la adquisición es un conglomerado, un mercado o producto, o una fusión horizontal o vertical, generalmente hay un proceso de diligencia y evaluación que se extiende a los departamentos Financiero, Legal, Comercial, Operaciones, Recursos Humanos e IT.

Este proceso permite el descubrimiento y evaluación del riesgo. Incluso en las fusiones pequeñas, el número de factores que contribuyen al riesgo y al proceso de toma de decisiones es extraordinario. Y el número creciente de riesgos de ciberseguridad solo viene a complicar todavía más el problema; la evaluación de los activos digitales de una empresa requiere el inventario de materialidad casi invisible con un dudoso historial de ciberseguridad.

Nuestros resultados sugieren que cuanto mayor sea el número de fusiones y adquisiciones en las que haya participado una persona, más probabilidades hay de que admita que su empresa experimentó un problema o incidente de ciberseguridad crítico que puso en peligro el acuerdo de M&A.

Dada la complejidad, no sorprende que más de la mitad de los encuestados (53 %) afirma que su empresa experimentó un problema o incidente de ciberseguridad crítico durante un acuerdo de M&A que puso en peligro la operación. Además, la encuesta ha revelado que:

- Los responsables de la toma de decisiones de IT tenían más probabilidades de afirmar que sus empresas habían experimentado un incidente crítico y comprometedor (57 %) frente a los responsables de la toma de decisiones empresariales (48 %).
- Los encuestados de Francia (61 %) e India (63 %) son los que afirmaron haber experimentado más problemas o incidentes de ciberseguridad.
- Las empresas más grandes (5000 empleados o más) (59 %) y las medianas (entre 1000 y 4999 empleados) (56 %) también experimentaron problemas de ciberseguridad con más frecuencia que las pequeñas de menos de 1000 empleados (49 %).
- Los encuestados pertenecientes a los sectores de la Alta tecnología (57 %) y los Servicios financieros (56 %) también tienen más probabilidades de haber experimentado un problema o incidente de ciberseguridad que otros sectores.
- Las personas que han participado en más de cinco fusiones tenían más probabilidades de contestar que sus empresas habían experimentado un problema o incidente de ciberseguridad crítico que puso en peligro el acuerdo (60 %), frente a los que habían participado en 2-5 fusiones (43 %).
- Los encuestados de organizaciones más maduras que utilizan más controles para mitigar el riesgo de ciberseguridad tenían menos probabilidades de haber experimentado un problema o incidente (46 %), lo que indica que los controles pueden jugar un papel importante a la hora de reducir el riesgo para la ciberseguridad.

Las personas que han participado en más de cinco fusiones tenían más probabilidades de contestar que sus empresas habían experimentado un problema o incidente de ciberseguridad crítico que puso en peligro el acuerdo.

60 %

Personas que habían participado en 2-4 fusiones

43 %

Personas que habían participado en más de 5 fusiones

DILIGENCIA Y EVALUACIÓN

Las empresas prestan más atención al nivel de ciberseguridad de un objetivo que lo hacían antes:

81 %

El ochenta y uno por ciento admitió estar prestando más atención al nivel de ciberseguridad de un objetivo que en el pasado.

EE. UU.	RU	FR	ALE	AUS	SG	IN
84 %	77 %	79 %	72 %	73 %	85 %	94 %

Evaluación del ciberriesgo en la diligencia de fusiones y adquisiciones

Casi todos los encuestados (93 %) indicaron que consideraban las evaluaciones de ciberseguridad tan importantes como la toma de decisiones de M&A de su empresa.

No sorprende que al pedirles que clasificaran una evaluación de ciberseguridad como "muy importante", "importante", "relativamente importante" o "no importante", más ITDM la consideraron muy importante (el 71 % frente al 64 % de BDM). Sin embargo, merece la pena señalar que ambas audiencias consideraron estas evaluaciones como una parte importante del proceso de M&A de sus empresas.

Las empresas están muy preocupadas por la exposición a riesgos de ciberseguridad potenciales y el 83 % coinciden en que se toman muy en serio el nivel de ciberseguridad del objetivo a la hora de llevar a cabo la diligencia debida sobre posibles objetivos de M&A. Y lo que es más importante, el 81 % admitió estar prestando más atención al nivel de ciberseguridad de una empresa objetivo que en el pasado.

A medida que crece la importancia de la transformación digital de las empresas, la estrategia digital y la adquisición de tecnología han ido cobrando cada vez más importancia en la adquisición de empresas. El 79 % de los encuestados indicó que la estrategia digital es una prioridad principal para los próximos 12 meses, mientras que para 77 % lo es la adquisición de tecnología.

La ciberseguridad desempeña un papel más importante en la estrategia de M&A que lo hacía anteriormente, y pueden incluso llegar a ser un motivo de ruptura del acuerdo en determinadas circunstancias.

El 73 % de los encuestados afirmó que una empresa con un incidente de fuga de datos no revelado es un motivo de ruptura inmediata del acuerdo en la estrategia de M&A de la empresa.

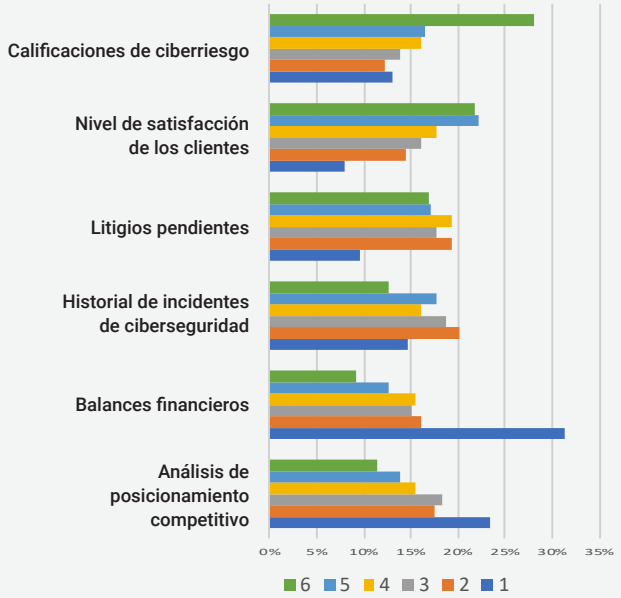
El 73 % de los encuestados afirmó que una empresa con un incidente de fuga de datos no revelado es un motivo de ruptura inmediata del acuerdo en la estrategia M&A de la empresa.

Factores críticos de diligencia debida

Preguntados por los factores más importantes cuando sus empresas realizan su diligencia debida sobre los objetivos de M&A, los encuestados indicaron los balances financieros como el más importante. El segundo factor más importante fue el historial de incidentes de ciberseguridad, como se muestra en el gráfico de la derecha, de más (1) a menos (6) importante. Los incidentes de ciberseguridad son muy importantes para personas que se encargan de cerrar los acuerdos y llevar a cabo el proceso de diligencia debida.

Resultados a la pregunta: ¿Cuáles son los factores más importantes cuando su empresa lleva a cabo la diligencia debida sobre objetivos de fusión o adquisición? (Se enumeran por orden de importancia).

1. Balances financieros
2. Historial de incidentes de seguridad
3. Posicionamiento competitivo
4. Litigios pendientes
5. Nivel de satisfacción de los clientes
6. Calificaciones de ciberriesgo



Sin embargo, mientras que el historial de ciberincidentes se coloca en el segundo puesto de la lista, es importante tener en cuenta cómo se evalúa ese historial y las amenazas potenciales durante el proceso de diligencia debida.

Ejecución de la diligencia debida

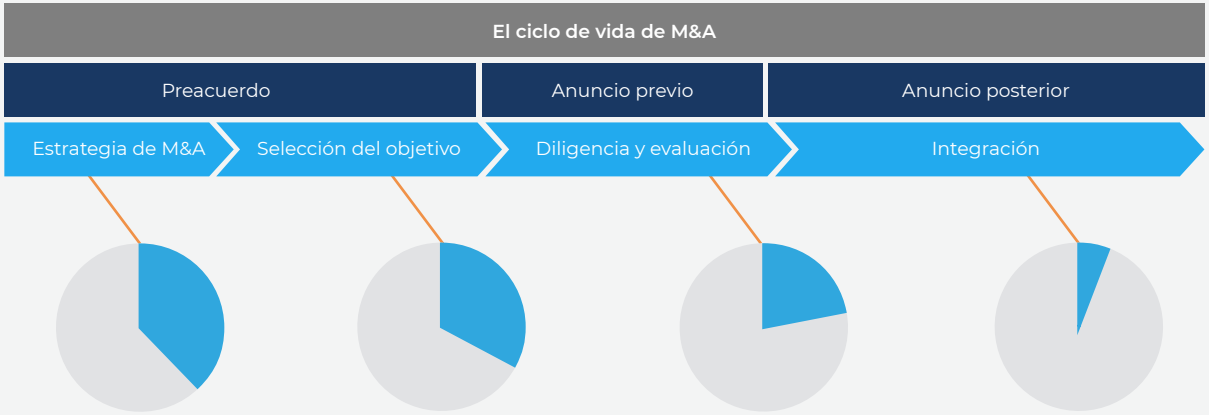
La diligencia debida sobre ciberseguridad de fusiones y adquisiciones normalmente incluye tanto evaluaciones internas como externas. Casi todos los encuestados (97 %) indicaron que sus empresas gastan dinero en contratistas externos y más de la mitad (57 %) que su empresa contrata una de las Big Four para llevar a cabo una evaluación de ciberseguridad. Y, el 80 % de los encuestados indicaron que su empresa realizó una inspección interna en profundidad de los sistemas y dispositivos relacionados con la tecnología de la información antes de completar la adquisición.

Esos resultados sugieren que incluso si no siempre se utilizan una de las 4 grandes empresas de auditoría (las conocidas como Big Four), la mayoría de las empresas llevan a cabo al menos una evaluación interna o utilizan contratistas externos para las evaluaciones. Pero también es importante considerar el enfoque que se utiliza al realizar la diligencia debida y las evaluaciones.

Las evaluaciones de ciberseguridad deberían ser una parte fundamental del proceso de evaluación de adquisiciones, no solo en el momento de la integración, sino durante todo el proceso de adquisición. Sin embargo, el 6 % de los encuestados afirmó que es en la integración (la última fase de la adquisición) cuando comienzan las evaluaciones de ciberseguridad. Otro 22 % afirmó que empezaban durante la diligencia debida, el 33 % dijo que lo hacían durante la selección del objetivo, y solo el 38 % afirmó que empezaban en la creación de la estrategia, es decir, el principio del proceso de adquisición. Estos resultados no solo ponen de relieve puntos de vista muy dispares sobre cuándo debería comenzar la evaluación de ciberseguridad, sino que también sugieren que para muchos no es sino un ejercicio puntual. Es absolutamente primordial que el diagnóstico del nivel de ciberseguridad de una empresa y la evaluación de las vulnerabilidades potenciales empiece desde el mismo inicio del proceso de M&A se prolongue durante la integración y después de la integración. Conviene recordar que incluso si durante la evaluación inicial no se encuentran ciberriesgos importantes, la que se va

Es absolutamente primordial que el diagnóstico del nivel de ciberseguridad de una empresa y la evaluación de las vulnerabilidades potenciales empiece desde el mismo inicio del proceso de M&A se prolongue durante la integración y después de la integración.

A la pregunta sobre la fase en la que realizan la evaluación de ciberseguridad, los encuestados afirmaron:



El 38 % afirmó que empezaba durante la creación de la estrategia

El 33 % afirmó que empezaba durante la selección del objetivo

El 22 % afirmó que empezaba durante la diligencia debida

El 6 % afirmó que empezaba durante la integración

Los responsables de la toma de decisiones piensan que no tienen tiempo suficiente para realizar la evaluación de ciberseguridad:

36 %

Solo el 36 % afirma con rotundidad que su equipo de IT dispone del tiempo necesario para revisar los estándares, procesos y protocolos de ciberseguridad de la empresa antes de que su empresa adquiera otra.

a adquirir seguirá operando (con los empleados actuales, clientes, proveedores y el mundo conectado en general) durante el proceso de M&A.

Y, en cualquier momento, los activos y dispositivos de la compañía objetivo podría convertirse en vulnerables. Además de la evaluación permanente, puede ser muy difícil desarrollar y mantener una vista completa de los ciberriesgos.

Es interesante observar que cuando se pidió a los ITDM y BDM que clasificaran su nivel de preocupación sobre el riesgo de ciberseguridad durante cada fase del proceso del ciclo de vida de M&A (creación de estrategia, selección del objetivo, diligencia y evaluación e integración), en una escala de 1 a 10, indicaron estar más preocupados durante la integración (7,44), y menos por las otras tres áreas: diligencia y evaluación (7,23), selección del objetivo de M&A (6,82), creación de estrategia de M&A (6,58).

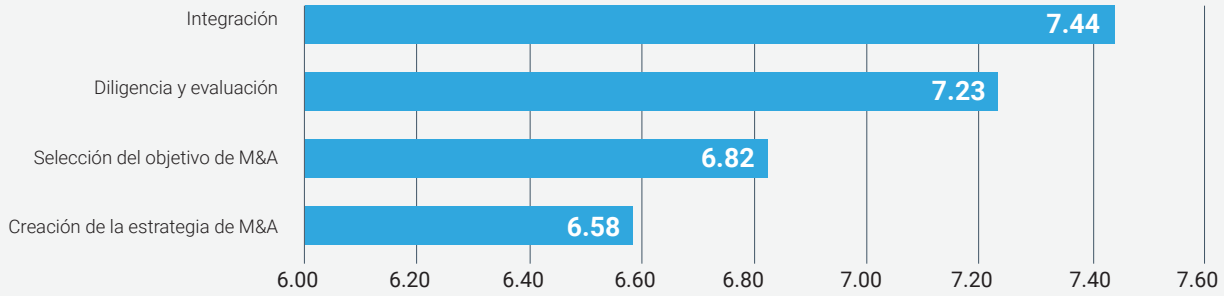
Para este ejercicio, 10 representa el nivel más alto de preocupación y 1 el más bajo. Una vez más, la evaluación de la ciberseguridad debería abarcar toda la duración de la adquisición, dando importancia a cada fase.

desarrolladas que las que solo utilizan uno o dos. Estos controles pueden tener un papel muy importante en la gestión y reducción del riesgo de ciberseguridad.

Una evaluación adecuada lleva tiempo

En un mundo de presión creciente para actuar con rapidez a l ahora de completar una adquisición, el tiempo es oro. Los acuerdos bien ejecutados son aquellos en los que la diligencia y la prudencia dan como resultado una adquisición exitosa donde los problemas son mínimos o inexistentes.

Resultados cuando se les pidió calificar su nivel de preocupación por el riesgo de ciberseguridad durante cada fase del proceso de ciclo de vida de M&A.



En lo que se refiere a los sistemas y procesos que las empresas en proceso M&A utilizan para determinar el nivel de riesgo durante la fase de diligencia y evaluación, los más utilizados generalmente entre ITDM y BDM son la infraestructura y la cadena de suministro de IT (54 %), los resultados de una auditoría interna de ciberseguridad de IT (48 %), y el historial de fugas de datos e incidentes de seguridad (46 %). Los tres sistemas y procesos menos utilizados fueron los sistemas GRC (37 %), las prácticas de aplicación de parches (36 %) y SIEM (27 %). Las organizaciones que utilizan un número mayor de procesos y sistemas cuentan con estrategias de M&A en cuanto a riesgos de ciberseguridad más maduras y

Sin embargo, observamos a menudo un problema cuando los ITDM no creen que cuentan con tiempo suficiente. Solo el 36 % afirma con rotundidad que su equipo de IT dispone del tiempo necesario para revisar los estándares, procesos y protocolos de ciberseguridad de la empresa antes de que su empresa adquiera otra. Aunque durante el proceso la empresa compradora puede necesitar más tiempo para la diligencia de ciberseguridad, una fusión y adquisición que analiza todos los problemas de ciberseguridad por anticipado tiene probabilidades de tener un mejor resultado global y menos sorpresas más adelante.

EVALUACIÓN E INVENTARIO DE ACTIVOS

Los equipos internos de IT pueden carecer de las competencias necesarias para realizar evaluaciones de ciberseguridad:

37 %

Entre los ITDM, solo el 37 % coincide plenamente en que su equipo de IT cuenta con los conocimientos necesarios para llevar a cabo una evaluación de ciberseguridad para una adquisición.

EE. UU.	RU	FR	ALE	AUS	SG	IN
49 %	30 %	36 %	28 %	31 %	31 %	54 %

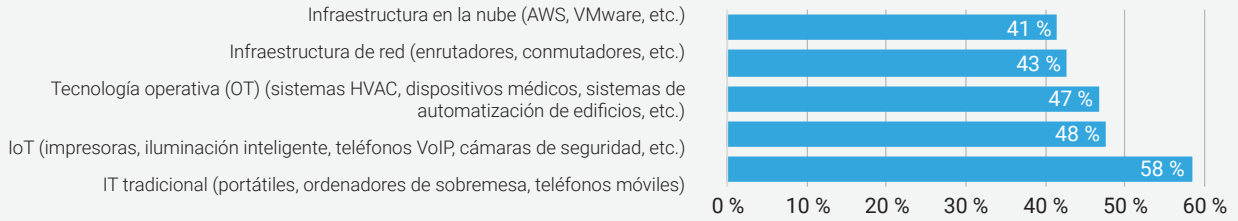
Dispositivos evaluados

Un inventario de activos completo es una parte esencial y una sólida estrategia de defensa, y la capacidad de obtener visibilidad de lo que hay en la red puede permitir acciones y respuestas oportunas capaces de mitigar riesgos operativos y de ciberseguridad. Cuando las empresas buscan activos, deben intentar examinar de forma integral (holística) todo lo que podría convertirse en una vulnerabilidad potencial. Sin embargo, a pesar de la necesidad del inventario de activos y de la evaluación de dispositivos, los resultados de la encuesta indican que los participantes tenían formas distintas de ver la importancia del inventario de activos en las cinco categorías de dispositivos: infraestructura de red, IoT, OT, IT tradicional e infraestructura de nube

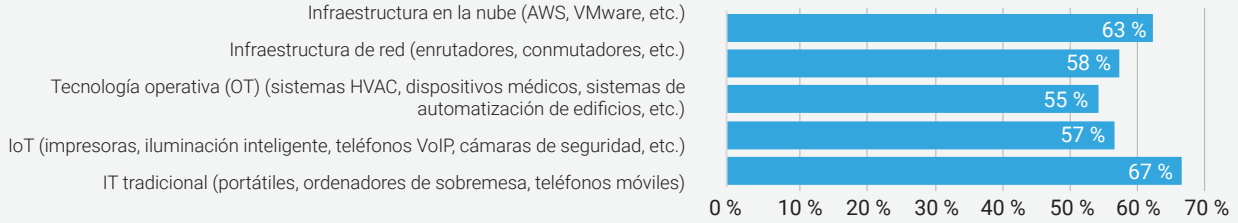
Los resultados de la encuesta apuntan a un desajuste entre dispositivos y activos que se consideran más vulnerables frente a actores maliciosos externos, y los dispositivos y activos que se incluyen realmente como parte de la evaluación de la nueva adquisición. Por ejemplo, el 78 % de los encuestados consideró la infraestructura de red (enrutadores, conmutadores, etc.) el punto más vulnerable frente actores maliciosos externos; sin embargo, solo el 58 % de ITDM afirmó que la infraestructura de red se analizaba como parte de la evaluación de la nueva adquisición. Además, el 43 % de los ITDM, afirmó que durante el inventario de activos, era muy probable que se olvidara la infraestructura de red.

Del mismo modo, el 72 % de los encuestados consideraron los dispositivos IoT (impresoras, iluminación inteligente, teléfonos VoIP, cámaras de seguridad, etc.) el punto más vulnerable frente actores maliciosos externos; sin embargo, solo el 57 % de ITDM afirmó que los dispositivos IoT se analizaban como parte de la evaluación de la nueva adquisición. Además, el 48 % de los ITDM afirmó que durante al inventario de activos, era muy probable que se pasaran por alto los dispositivos IoT.

A la pregunta: ¿qué activos tienen más probabilidades de ser pasados por alto durante el inventario?



A la pregunta: ¿qué tipos de dispositivos son los que busca su empresa a la hora de evaluar el nivel de ciberseguridad de una nueva integración de adquisición?



En lo que respecta a la tecnología operativa, el 73 % de los encuestados la consideró como el punto más vulnerable; el 55 % de los ITDM afirmó que se evaluaba la OT, y el 47 % que era muy probable que los activos de OT se pasaran por alto durante el inventario de activos.

Estos resultados revelan que incluso aunque existe una preocupación considerable sobre la vulnerabilidad de activos y dispositivos en la infraestructura tradicional de IT, OT, IoT, la infraestructura de nube y la infraestructura de red, el grado de preocupación no siempre coincide con la importancia de la acción llevada a cabo; y, por lo tanto, también preocupa enormemente pasar por alto esos dispositivos y activos durante el inventario.

Posible desajuste entre los dispositivos y activos que se consideran más vulnerables y los que en realidad se incluyen como parte de la evaluación:

El 78 % consideraba vulnerable la infraestructura de red

El 58 % afirmaba evaluar la infraestructura de red

El 43 % pensaba que la infraestructura de red podría pasarse por alto

Warum Asset-Erfassung ein Kampf ist

Según estos resultados, parece claro que si bien los responsables de la toma de decisiones consideran el inventario de archivos un paso importante del proceso de evaluación, es a menudo una tarea

Durante la integración, a menudo se pasan por alto o se pierden dispositivos:

53 %

Más de la mitad de los ITDM afirma que encuentran dispositivos de los que se desconocía su existencia tras finalizar la integración de una nueva adquisición.

EE. UU.	RU	FR	ALE	AUS	SG	IN
53 %	49 %	55 %	60 %	44 %	57 %	55 %

complicada para las empresas compradoras durante la M&A.

Por qué es difícil realizar el inventario de activos

A la pregunta de si pensaban que el equipo de IT de su empresa tenía el tiempo suficiente para revisar los estándares de ciberseguridad, los procesos y protocolos de la empresa objetivo antes de la adquisición, solo el 36 % de los ITDM afirmó con rotundidad que sí.

Los responsables de la toma de decisiones no solo piensan que a menudo no se da el tiempo adecuado para llevar a cabo la evaluación de ciberseguridad previa a una adquisición, sino que además dudan de su capacidad para realizar dicha tarea. Así las cosas, se podría pensar que las empresas se inclinarían por invertir en una evaluación externa. Sin embargo, solo el 57 % de ITDM y BDM informaron de que sus empresas contrataban los servicios de alguna de las 4 grandes empresas auditoras (Big Four) para llevar a cabo una evaluación de ciberseguridad.

Teniendo en cuenta estas respuestas, no sorprende que el 80 % de los ITDM coincidan en afirmar que, durante la integración con las tecnologías de la empresa adquirida siempre aparecieron problemas relacionados con la ciberseguridad previamente desconocidos o no revelados.

Aunque esta encuesta no ofrece información específica sobre el volumen de dispositivos omitidos por categoría, más de la mitad (53 %) de los ITDM afirmó que encontraban dispositivos de los que se desconocía su existencia tras completar la integración de una nueva adquisición. Los dispositivos más encontrados era los de IT tradicional (portátiles, ordenadores de sobremesa, teléfonos móviles), seguidos de cerca de los dispositivos IoT y OT. Las respuestas sugieren que, antes de que se produzca una adquisición, se desconoce la existencia de una parte importante de los dispositivos conectados. Los dispositivos de IT tradicionales son a menudo los más fáciles de localizar y controlar. Los dispositivos IoT y OT también pueden ser omitidos, ya que estos suelen ser más pequeños (por ejemplo, los sensores son más pequeños y difíciles de detectar físicamente), además, hay otros dispositivos de OT que a veces ejecutan software heredado u obsoleto, lo que los hace difíciles de detectar y actualizar. Además, en muchas ocasiones las empresas carecen de las herramientas necesarias para identificar y controlar íntegramente todos y cada uno de los dispositivos conectados. Independientemente del volumen de dispositivos no contabilizados, cada vez que se pasa por alto un dispositivo, no sorprende si una empresa hereda ciberriesgos, ya que en realidad no saben lo que están heredando.

Oportunidad para el ataque

En términos de volumen de dispositivos, de media, el 43 % de los encuestados afirmó que sus empresas encontraban menos de 10 000 dispositivos conectados durante el inventario de una empresa compradora. Las empresas más grandes se enfrentan incluso a más dispositivos, y el 23 % de los encuestados afirmó que sus empresas encontraban más de 500 000. Eso significa que con la adquisición se incorporan a menudo miles de dispositivos, dispositivos que pueden estar completamente actualizados y seguros o bien no estar autorizados y plagados de malware. Y, si tenemos en cuenta que más de la mitad de los ITDM afirmó la existencia de otros dispositivos de los que se desconoce su paradero después de la integración, la oportunidad de ataque o de actividad maliciosa se hace evidente. Y solo hace falta un dispositivo para comprometer toda la red.

Los principales factores de riesgo

En nuestro estudio, preguntamos a los participantes qué factor fue en que más puso en riesgo sus empresas durante el proceso de información e integración tecnológica de la adquisición. Fueron tres las respuestas que destacaron: el error humano y una configuración deficiente (51 %), los dispositivos conectados (50 %), y los sistemas de administración y almacenamiento de datos (49 %).

El factor humano es un reto que se extiende más allá de los procesos M&A y se menciona con frecuencia como la fuente del peligro: una amenaza interna, una fuga de datos no intencionada, o una descarga de malware desapercibida a través de un mensaje de correo electrónico, son solo algunas maneras mediante las que los usuarios suelen comprometer las redes de las empresas. Los programas de formación, de incentivos o disciplinarios son métodos utilizados habitualmente para reducir el error humano.

RETRASOS Y PESARES

No hacer caso al riesgo de ciberseguridad puede hacer que las empresas se arrepientan de llevar a cabo una adquisición:

65 %

El sesenta y cinco por ciento afirmó que sus empresas lamentaron haber cerrado un acuerdo de M&A por cuestiones de ciberseguridad.

EE.UU.	RU	FR	ALE	AUS	SG	IN
65 %	65 %	67 %	61 %	61 %	65 %	70 %

Retrasos en el calendario de adquisiciones

El calendario, los recursos y las operaciones de una empresa pueden estar sujetos a cambios, sobre todo en el caso de las fusiones y adquisiciones. Menos de la mitad (49 %) de los encuestados afirman que experimentaron incidentes, problemas o riesgos de ciberseguridad desconocidos o no revelados al integrar la información y la tecnología de la empresa adquirida, que retrasaron el calendario de integración.

Estos contratiempos pueden provocar retrasos o pérdidas económicas, que en ambos casos pueden dañar la empresa y su estrategia de M&A. Se preguntó a los encuestados sobre los retrasos de menos y más de seis meses y las pérdidas de valor por debajo o por encima de 1 millón de dólares. Más de la mitad de los encuestados (54 %) reconoció un pequeño retraso (menos de seis meses) como consecuencia y la mitad (50 %), un gran retraso (más de seis meses) debido a un incidente de ciberseguridad. El 22 % de los encuestados reconoció una pérdida de valor de menos de 1 millón de dólares y solo el 5 % dijo que la pérdida había superado esa cifra.

Son muchos los factores que pueden contribuir a estos retrasos y costes, pero las empresas pueden reducir los riesgos mediante la implicación temprana de los responsables de la toma de decisiones de IT en el proceso y concediéndoles el tiempo y las herramientas necesarias para realizar bien su trabajo. Y, a menudo, estos responsables de la toma de decisiones verán la necesidad de una mayor implicación. De hecho, el 35 % de los responsables de la toma de decisiones de IT también piensa que necesitan implicarse más en el proceso de M&A de sus empresas.

Se preguntó a los encuestados sobre los retrasos de menos y más de seis meses y las pérdidas de valor por debajo o por encima de 1 millón de dólares.

54 %
pequeño retraso (menos de seis meses)

50 %
gran retraso (más de seis meses)

22 %
de pérdida de valor de menos de 1 millón de dólares

5 %
de pérdida de valor de más de 1 millón de dólares

Poco menos de la mitad (49 %) de los encuestados afirma que experimentaron incidentes, problemas o riesgos de ciberseguridad desconocidos o no revelados al integrar la información y la tecnología de la empresa adquirida, que retrasaron el calendario de integración.

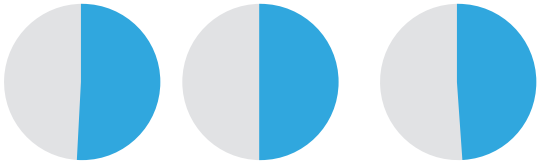
Problemas y pesares relacionados con las adquisiciones

Casi dos terceras partes de los encuestados (65 %) afirmaron que sus empresas lamentaron haber cerrado un acuerdo de fusión y adquisición por cuestiones de ciberseguridad.

El 22 % dijo que su empresa había experimentado un profundo pesar y el 44 % que su empresa había experimentado algún pesar, mientras que el 35 % de los encuestados dijo que su empresa jamás se había arrepentido de nada.

Cuando se les preguntó por la naturaleza de sus pesares, muchos encuestados señalaron incidentes o problemas relacionados con la ciberseguridad. El mayor número de referencias se produjeron entorno a la falta de diligencia debida o investigación, la pérdida de tiempo o de dinero, la brechas o ataques de ciberseguridad. A la pregunta de qué les gustaría que su empresa hubiera hecho de manera distinta, los encuestados a menudo afirmaron que les habría gustado que hubiera contratado un proveedor externo para verificar el nivel de ciberseguridad o que hubiera llevado a cabo una diligencia debida más exhaustiva. Muchos añadieron que deseaban que sus empresas hubieran empleado más tiempo y menos dinero en la compra o transacción actual.

Cuál fue el factor que más puso en riesgo las empresas durante el proceso de información e integración tecnológica de la adquisición.



51 %
error humano y configuración deficiente

50 %
dispositivos conectados

49 %
sistemas administración y almacenamiento de datos

Algunos ejemplos son

"Creo que mi empresa desearía haber sido más proactiva en lo relativo a los riesgos relacionados con la falta de ciberseguridad en la fundación de nuestra empresa y lamenta los incidentes que se produjeron debido a normativas laxas".

–Responsable de la toma de decisiones empresariales de EE. UU.

"Desearíamos haber sido más meticulosos en nuestra diligencia debida".
–Responsable de la toma de decisiones de IT del Reino Unido

"Si pudiera haber hecho las cosas de forma diferente, habría dado más tiempo a mi equipo de IT para que realizara una inspección completa".
–Responsable de la toma de decisiones de IT de Singapur

"A mi empresa le habría gustado haber tenido acuerdos legales más herméticos en relación con las cláusulas de limitación las compensaciones económicas".
–Responsable de la toma de decisiones empresariales de Australia

Comunicación de ciberriesgos

En general, las respuestas de ITDM y BDM estuvieron alineadas en muchos sentidos. Por ejemplo, hubo una coincidencia más estrecha cuando se preguntó a los ITDM y BDM que clasificaran su nivel de preocupación sobre ciberriesgos durante cada fase del ciclo de vida de M&A (creación de estrategia, selección del objetivo, diligencia y evaluación e integración). Los ITDM situaron en primer lugar la integración (7,52), tal y como hicieron los BDM (7,36).

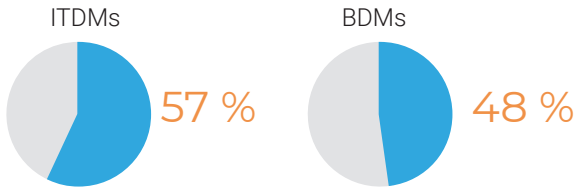
Sin embargo, hubo algunos casos que indicaron una diferencia, en opinión, implicación o enfoque a un asunto concreto.

Por ejemplo, cuando se les preguntó en qué fases habían participado, el 51 % de los ITDM dijo haber participado en la integración, por solo el 35 % de los BDM. Cabría esperar una mayor implicación de los ITDM específicamente en la integración de IT, pero no necesariamente en la integración en su conjunto. Para la fase inicial de creación de estrategia, el 73 % de los ITDM confirmó su participación, frente al 66 % de los BDM.

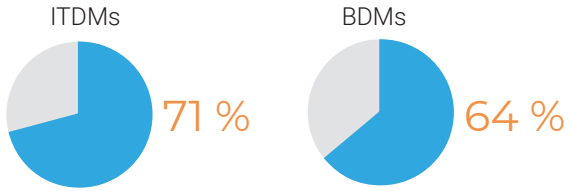
De hecho, para las cuatro fases, los ITDM afirmaron haberse implicado más de lo que lo hicieron los BDM. Estos resultados sugieren que las empresas podrían beneficiarse de una mayor implicación de los BDM.

A continuación incluimos un par de comparaciones más:

Los encuestados afirmaron que sus empresas habían experimentado un problema o incidente de ciberseguridad crítico que puso en peligro un acuerdo de M&A.



Consideraban muy importantes las evaluaciones de ciberseguridad.



Estas respuestas sugieren dos cosas:

En principio, aunque los ITDM y los BDM iban a menudo a la par, no fue siempre el caso. Incluyo cuando lo estaban, sus respuestas destacaban oportunidades de mejora en el área de la ciberseguridad y el ciberriesgo. Por ejemplo, tanto ITDM como BDM deberían estar más implicados a lo largo de cada fase del ciclo de vida del proceso de M&A.

En segundo lugar, los resultados sugieren que los ITDM y BDM previeron y priorizaron los riesgos de forma diferente. Por ejemplo, el 23 % de los ITDM afirmó que su empresa tuvo serios pesares después de un acuerdo de M&A debido a cuestiones relacionadas con la ciberseguridad, frente al 19 % de BDM. Estas diferencias, aunque ligeras, indican que los ITDM y BDM pueden cuantificar el riesgo de forma diferente. Desde el punto de vista de un ITDM, un serio pesar podría surgir del hecho de que una aplicación crítica se bloqueara durante la integración, dejando a empleados y clientes sin acceso durante horas. Desde el punto de vista de un BDM, sin embargo, podrían ver ese escenario desde la perspectiva de las pérdidas financieras.

Desde el primer día de una adquisición, resulta fundamental que los ITDM y los BDM alcancen un consenso sobre cómo van a comunicar, calcular, evaluar y mitigar los riesgos. Ellos no siempre son los responsables de las mismas personas, los mismos procesos, recursos y misiones organizativas, por lo que pueden abordar los riesgos de forma diferente, con umbrales de tolerancia distintos, así como con medios diferentes de comunicar las implicaciones de esos riesgos. Para garantizar que se es consciente de todos los riesgos, es importante que los ITDM y los BDM acuerden términos y condiciones comunes de evaluación y comunicación de los riesgos.

CONCLUSIÓN

El ciberriesgo es una preocupación cada vez mayor tanto para los responsables de la toma de decisiones empresariales como de IT durante el proceso de fusión y adquisición, y la integración. Mientras se produce la integración, las empresas son más vulnerables a ataques y tienen mayor exposición, ya que no pueden ver lo que puede ser más vulnerable o estar a punto de ser pirateado. La mitigación de ese riesgo se encuentra en el equilibrio entre dar tiempo a los equipos de IT para que lleven a cabo un trabajo adecuado de evaluación, diligencia e inventario con antelación, y disponer de más controles para supervisar el proceso.

Según los resultados de nuestra encuesta, existe una oportunidad para que las empresas aumenten su vigilancia su protección mediante la formación del personal de IT, permitiendo que los equipos de IT se impliquen más en el proceso de M&A, garantizando que se utiliza un programa de inventario de activos automatizado y dándoles el tiempo necesario para llevar a cabo la diligencia debida.

Los resultados de este informe indican claramente que cuantos más controles utilice una empresa, mejores serán los resultados a la hora de reducir el riesgo y proteger sus activos.

Para obtener más información sobre cómo minimizar sus riesgos de ciberseguridad, lea el **resumen de la solución sobre fusiones y adquisiciones (en inglés)**.

ACERCA DE FORESCOUT TECHNOLOGIES

Forescout Technologies es líder en visibilidad y control de dispositivos. Nuestra plataforma unificada de seguridad permite a las empresas y organismos oficiales obtener información completa sobre el estado de sus entornos empresariales ampliados y orquestar medidas destinadas a reducir el riesgo operativo y de ciberseguridad. Los productos de Forescout se despliegan rápidamente y ofrecen descubrimiento y clasificación en tiempo real y sin agentes de todos los dispositivos conectados mediante IP, así como una evaluación continua de estado. A fecha de 31 de diciembre de 2028, 3300 clientes de más de 80 países confían en la solución independiente de la infraestructura de Forescout para reducir el riesgo de interrupciones de la actividad empresarial por incidentes de seguridad o fugas, garantizar y demostrar el cumplimiento en materia de seguridad y aumentar la productividad de las operaciones de seguridad. Descubra cómo en www.forescout.com.

Los investigadores de Forescout limitaron el ámbito de aplicación y la muestra de datos por razones de coherencia y la conveniencia de generar un informe único. Hemos observado limitaciones debidas al tipo de estudio, al momento, ámbito, anonimización de los datos, métodos de captura de datos pasiva, y errores en la clasificación basada en inteligencia artificial de las funciones, sistemas operativos y proveedores de los dispositivos. La realidad de utilizar datos de nube de entornos de producción reales significa asumir imperfecciones en el suministro de datos. Dentro de estos límites, los investigadores de Forescout han hecho todo lo posible para garantizar la coherencia, fiabilidad e integridad del informe.

RECOMENDACIONES

Las adquisiciones pueden ser un ejercicio laborioso y que implique muchos recursos, y en ocasiones una adquisición puede verse frustrada por los resultados de la diligencia debida. Históricamente, la diligencia de fusiones y adquisiciones ha estado centrada, entre otros, en los departamentos Financiero, Legal, Comercial, Operaciones, Recursos Humanos y Tecnologías de la Información. Y, aunque la ciberseguridad se ha ignorado completamente como su propia área de evaluación, lo que parece claro es que, dados los riesgos, las organizaciones que consideren una adquisición podrían beneficiarse de una evaluación de la ciberseguridad mayor y más dedicada. A continuación incluimos algunas recomendaciones que deberían tener en cuenta las empresas mientras se preparan durante para próximo acuerdo comercial.

El dinero bien invertido con antelación será inestimable si le protege de sorpresas más adelante.

Dé prioridad a la administración e inventario de activos: si las empresas no consiguen contabilizar todos los dispositivos y activos de su red, no pueden conocer completamente los riesgos que podrían estar heredando como parte de una adquisición. Es primordial que las empresas den prioridad a la administración e inventario de archivos como mejor práctica fundamental para reducir los ciberriesgos durante los procesos de M&A. Y para ir un paso más allá, es necesario determinar la importancia relativa de cada activo, así como conseguir un conocimiento profundo de la red a la que está conectado cada activo. En otras palabras, si hay un activo vulnerable en la red, pero está segmentado, el activo y el riesgo asociado pueden gestionarse de forma eficaz.

Deje que los equipos internos lleven a cabo una auditoría rigurosa e incorpore a un tercero para obtener más ayuda (si su equipo interno no es capaz de llevar a cabo el nivel adecuado de diligencia debida necesario). Las empresas deben estar dispuestas a reconocer que no siempre pueden hacer esto ellas mismas y que se requiere una formación importante para dotar a los equipos internos de los conocimientos necesarios para llevar a cabo la diligencia debida.

Asigne presupuesto para una auditoría de ciberseguridad externa: esté preparado para dedicar el dinero necesario para asegurarse de que la empresa realiza un examen en profundidad antes de llegar a un acuerdo. El dinero bien invertido con antelación será inestimable si le protege de sorpresas más adelante.

Ofrezca formación a sus equipos de IT para que estén adecuadamente equipados para gestionar y prepararse para una adquisición: los equipos de IT necesitan más formación sobre lo que tienen que buscar y cómo abordar los problemas relacionados con las M&A. Los protocolos y sistemas pueden ayudarles a informar a los mediadores del acuerdo sobre cualquier problema de ciberseguridad que encuentren, pero necesitan estar informados sobre las últimas amenazas.

Utilice más controles para proteger su organización: las empresas con controles de ciberseguridad más avanzados identifican, comprender, gestionan y mitigan mejor los riesgos de ciberseguridad.

Incluya cláusulas de contingencias y de limitación: aunque el 89 % de los encuestados piensa que su empresa debería incluir cláusulas de limitación, solo el 69 % lo hace en la actualidad. Incluir una cláusula de limitación es una forma habitual de mitigar riesgos en el caso de que se descubran riesgos o pérdidas de valor imprevistos. El 73 % de los encuestados también utiliza contingencias y permite a la empresa compradora rescindir un contrato después de firmarlo si averigua que las representaciones o garantías no son ciertas.

Forescout Technologies, Inc.
190 W Tasman Dr.
San José, CA 95134 EE. UU.

C. e.: info-espana@forescout.com
Tel. (internacional) +1-408-213-3191
Soporte técnico +1-708-237-6591