TANIUM

Lo que se ignora puede hacerte daño: consejos de expertos para medir el riesgo

Los expertos del sector ofrecen orientación y perspectivas para medir los riesgos en un mundo como el actual, en rápido movimiento y altamente distribuido.

TANIUM

Lo que se ignora puede hacerte daño: consejos de expertos para medir el riesgo

Los expertos del sector ofrecen orientación y perspectivas para medir los riesgos en un mundo como el actual, en rápido movimiento y altamente distribuido.

Contenido

Consejos de expertos sobre la medición de riesgos

La gestión de riesgos comienza por su medición.

Pero, ¿cómo se miden los riesgos de forma efectiva? ¿Debería contemplar todas las vulnerabilidades de software de la empresa? ¿Necesita hacer una lista de todos los dispositivos que requieren parches de software? ¿Debería informar sobre las estadísti cas de los tiempos de actividad para las aplicaciones más críticas de la empresa?

Cuando su trabajo mide el riesgo, debe centrarse en lo que es significativo para los destinatarios de su análisis. Y para las decisiones más importantes sobre riesgos, su destinatario es el Consejo Directivo y el equipo ejecutivo.

En este eBook, tres expertos del sector de TI comparten sus conocimientos sobre la práctica de medir el riesgo de la manera más exhaustiva y práctica.

Al final del eBook verá una lista de verificación que resume los consejos presentados por estos expertos. *Empecemos.*

Medir lo que importa: alinear la medición de riesgos con las metas y objetivos corporativos

Si pregunta a la mayoría de los expertos en seguridad de TI, el riesgo está en todas partes. Se encuentra en las terminales sin parches, las nuevas variantes de malware, los ataques de phishing, los servicios de nube de TI en la sombra, las computadoras portátiles en los bancos del parque... la lista sería interminable. Con tantos detalles técnicos que contribuyen al riesgo, es posible que su equipo de riesgo se pregunte cómo abordar el importante trabajo de medir dichos riesgos en su empresa.

Por supuesto, nadie mide el riesgo simplemente por el placer de medirlo. Las evaluaciones de riesgo se llevan a cabo para proporcionar información a los responsables de decisiones. La verdadera pregunta es esta: ¿Cómo medir el riesgo de manera que ayude a los responsables de su organización, el Consejo Directivo y el equipo ejecutivo, a entender el riesgo para que puedan tomar las decisiones correctas y reducirlo en consecuencia?

Medir los riesgos que son importantes para la dirección de la empresa

Para responder a esta pregunta, comencemos por arriba. El Consejo Directivo y el equipo ejecutivo son responsables de establecer la dirección estratégica de la empresa. Y parte de su trabajo es asegurar que las decisiones y las inversiones realizadas en toda la organización respalden los objetivos estratégicos de alto nivel de la empresa.

Independientemente del sector de negocio de su empresa, esos objetivos de alto nivel casi seguramente incluyen lo siguiente:

- Continuidad del negocio
- Confidencialidad, integridad y disponibilidad de los datos (CIA de datos)
- Cumplimiento normativo

Consideremos cada uno de estos aspectos.

Medición del riesgo asociado con la continuidad del negocio

Continuidad del negocio significa mantener las luces encendidas, a los empleados productivos, cualquier operación de fabricación y envío en marcha, y asegurar que cualquier otro tipo de operaciones, ya sea bombeando aceite o entregando un producto SaaS, puedan seguir funcionando, pase lo que pase.

La recuperación después de un desastre entra en esta categoría. También está la protección de los servicios críticos de la empresa frente a las ciberamenazas.

Medición del riesgo asociado a la confidencialidad, integridad y la disponibilidad de los datos

En todos los sectores se reconoce la importancia de los datos como el "nuevo petróleo" de la economía digital y de proteger los datos confidenciales.

El desafío de proteger esos datos ha aumentado. Por un lado se accede a los datos confidenciales desde más ubicaciones que nunca en un mundo en el que el teletrabajo (Work From Home, WFH) es la nueva norma: una fuerza laboral que depende cada vez más de "traiga su propio dispositivo" (Bring Your Own Device, BYOD), en lugar de recurrir a computadoras portátiles y computadoras de sobremesa probadas y suministradas por el departamento de TI.

Pero sin importar desde dónde o cómo acceden los empleados a los datos, las empresas deben garantizar la confidencialidad, la integridad y la disponibilidad de los datos (o como se conoce en algunos círculos de TI, "CIA de datos", Confidentiality, Integrity and Availability of data).

Medición del riesgo asociado con el cumplimiento normativo

Cuando pensamos en la privacidad de los datos, naturalmente pensamos en normativas como el RGPD y la HIPAA, que exigen la protección de los datos personales.

Pero también hay otras normativas que pueden abarcar ámbitos tan diversos como la información financiera o la discriminación racial, y que las empresas no pueden permitirse infringir. Los incumplimientos normativos pueden dar lugar a sanciones elevadas, cancelación de contratos y mala publicidad, con la consecuente mala reputación, que puede durar años. Para medir el riesgo de forma efectiva, debe saber qué normativas son importantes para la dirección de su empresa. Después será preciso hacer seguimiento de los activos y los procesos de TI, para ayudar a determinar si su empresa cumple con estas normativas.

Enmarcar el riesgo en los objetivos estratégicos

Es responsabilidad del Consejo Directivo y el equipo ejecutivo estar al frente de la empresa para lograr los objetivos principales de continuidad del negocio, privacidad de datos y cumplimiento normativo. Por supuesto, podrían llevar a la empresa a alcanzar otros objetivos, como un determinado porcentaje de crecimiento anual u otro relacionado con la cultura de la empresa.

Si desea llamar la atención de estos responsables empresariales, enmarque su debate en las mediciones de riesgo en términos de los objetivos a nivel del Consejo Directivo de la empresa. En otras palabras, identifique y sopese los diversos riesgos técnicos, normativos y de otro tipo de la empresa, y muestre su interrelación con los objetivos estratégicos de alto nivel de su empresa.

Descubrirá que enmarcar sus mediciones de riesgo de esta manera ayuda a centrar su trabajo. Y hace que sea más probable que los responsables de la empresa que marcan el rumbo del negocio para el futuro entiendan y aprecien su trabajo.

Medición del riesgo mediante la identificación de cadenas de suministro de valor

En este capítulo profundizaremos en la medición de los riesgos para los objetivos de la empresa. Se trata de analizar la importancia de las escalas ponderadas para diversos riesgos, e incluso para los propios objetivos.

Identificar los riesgos asociados con los objetivos estratégicos

La labor de medir los riesgos comienza identificando los objetivos estratégicos de la empresa y explorando a continuación las personas, los procesos y la tecnología que hay detrás los esfuerzos para lograr esos objetivos por parte de la empresa.

Piense en ello como un análisis de la cadena de suministro. Está rastreando el flujo de datos, personas y operaciones desde un objetivo de alto nivel hasta sistemas y procesos de TI específicos que ayudan a la empresa a alcanzar ese objetivo. Esos sistemas y procesos funcionan como una especie de cadena de suministro para los propios objetivos.

Para medir el riesgo, identifique las dependencias en esta cadena de suministro y rastréelas en la medida en que tenga sentido para los objetivos y capacidades de la empresa. Para comparar los riesgos dentro de la propia cadena de suministro, debe asignar una puntuación a todo dentro de la cadena de suministro.

Creación de una escala ponderada para los riesgos

Incluso los propios objetivos estratégicos deben compararse y ponderarse. Es raro que una empresa trate todos sus objetivos estratégicos por igual.

Una vez identificados dichos objetivos, asígneles puntuaciones en algún tipo de escala, como del 1 al 10. Por ejemplo, en función de las conversaciones con el equipo ejecutivo, podría asignar un crecimiento continuo de la facturación de al menos un 10 % de CAGR con una puntuación de 10 y una puntuación de cumplimiento normativo de 7.

Identifique a continuación las personas, los procesos y la tecnología implicados en el desarrollo de cada objetivo estratégico y clasifique la importancia de cada uno de esos factores de desarrollo.

Y para aportar más matices, puede estimar la probabilidad de que se produzca algún tipo particular de fallo. Por ejemplo, imagine que la empresa dispone de un servidor web vinculado a una aplicación móvil que es crítica para el negocio.

Las probabilidades de que ese servidor ofrezca un rendimiento inaceptablemente lento durante un período de uso intensivo son probablemente mayores que las probabilidades de que ese mismo servidor sucumba a un corte de suministro eléctrico que bloquee tanto los sistemas principales de suministro de energía como los de reserva.

Al multiplicar una puntuación asignada a la importancia estratégica del servidor (por ejemplo, 7 de 10) por la probabilidad de un riesgo específico (por ejemplo, 50 % o 0,5), puede empezar a clasificar los riesgos e identificar aquellos que requieren una actuación más inmediata.

La importancia de la colaboración en la medición del riesgo

Llevar a cabo este tipo de evaluación de riesgos requiere recopilar información detallada sobre personas, procesos y tecnología en toda la empresa. El departamento de TI tendrá que pedir ayuda.¿Mi consejo? Pida ayuda a todos los departamentos cuyos procesos y tecnología esté evaluando. Por ejemplo, si realmente desea comprender los riesgos que rodean a las aplicaciones del departamento de RR. HH., hable con las personas del departamento de RR. HH. Es posible que sepan cosas sobre la importancia de una aplicación que el equipo de operaciones de TI puede haber pasado por alto.

Cuando hable con personas ajenas al departamento de TI, minimice el uso de jerga técnica. Además, nunca le diga a alguien cómo hacer algo sin preguntarle primero cómo cree que debe hacerse. Si se impone una solución a las personas, podrían perderse alternativas creativas. También puede descubrir que la gente se resiste a seguir una nueva política que les afecta directamente si no se han tenido en cuenta sus ideas.

La gestión de riesgos es un problema de la empresa, no un problema del departamento de TI

Cuando personas ajenas al departamento de TI se dan cuenta de que confía en ellas y que está realmente interesado en lo que tienen que decir, se comunicarán con usted más libremente. También es más probable que asuman la responsabilidad de las soluciones de gestión de riesgos que vaya a poner en marcha.

Esta colaboración continua es uno de los beneficios de adoptar un enfoque de “cadena de suministro” para medir el riesgo. No solo detectará los detalles que necesita para medir los riesgos con mayor precisión. También formará a las partes interesadas de toda la organización sobre la importancia de la medición y mitigación de riesgos. Y tendrá la oportunidad de colaborar con estas partes interesadas en el desarrollo de soluciones para minimizar los riesgos que ambos han identificado.

CHAPTER 3:

Modernización de las evaluaciones de riesgos para el modelo actual de empresa distribuida

Medir el riesgo solía ser una actuación especial realizada con consultores. Con datos y automatización en tiempo real, las empresas miden ahora el riesgo de forma más precisa, continua y efectiva.

El cambio repentino del año pasado a un modelo de teletrabajo cambió muchas cosas en las TI empresariales, incluida la forma en que los equipos de TI realizaban las evaluaciones de riesgos.

En este capítulo analizaremos cómo las empresas llevaban a cabo tradicionalmente las evaluaciones de riesgos. Y consideraremos cuántas empresas las han estado realizando desde que comenzó la pandemia y ofreceremos algunas prácticas recomendadas para modernizar la evaluación de riesgos a fin de prestar un mejor servicio al modelo de empresa altamente distribuido de hoy en día.

Cómo cambiaron los riesgos y las evaluaciones de riesgos en la pandemia

Tradicionalmente, muchas organizaciones realizaban evaluaciones de riesgos solo una vez al año. Los equipos de evaluación de riesgos elaboraban informes detallados que intentaban resumir todos los riesgos de la organización en áreas como la seguridad de las TI, la recuperación ante desastres y el cumplimiento.

Para recopilar información para sus informes, los equipos visitaban centros de datos y distribuían cuestionarios. Incluso si las visitas eran escrupulosas y los cuestionarios exhaustivos, las evaluaciones siempre reflejaban el riesgo en un único momento.

Si cinco minutos después de que el equipo acabara la visita al centro de datos, una nueva actualización de software ponía en peligro de repente la integridad de los informes financieros de la empresa, el informe de evaluación de riesgos no reflejaba ese mayor riesgo.

Para muchas organizaciones, la fragilidad de estas evaluaciones de riesgo aumentó durante la pandemia. Los cuestionarios enviados por correo electrónico sustituyeron a las inspecciones presenciales. Las partes interesadas cumplimentaron los formularios de forma obligatoria, incluso si nadie podía decir con certeza qué dispositivos utilizaban los empleados de forma remota o qué software se ejecutaba en ellos.

¿Existe una mejor forma de realizar evaluaciones de riesgos? He pasado mucho tiempo en mi carrera centrándome en la práctica de las evaluaciones de riesgos, y creo que la respuesta es sí.

Trasladar la evaluación de riesgos a la era de la informática en la nube y el teletrabajo

Lo primero que hay que cambiar en las evaluaciones de riesgos es su idoneidad en el tiempo. Si los informes se basan en datos recopilados una vez al año, serán inexactos la mayor parte del tiempo.

Todos sabemos que el ritmo al que se ven sometidas las empresas es más rápido que nunca. Datos, dispositivos, software, relaciones comerciales... todo esto está en constante cambio. Las evaluaciones de riesgo deben reflejar ese flujo de cambio.

Afortunadamente, los departamentos de TI disponen de nuevas herramientas que permiten mejorar la precisión de las evaluaciones de riesgos. La supervisión de terminales en tiempo real, por ejemplo, puede informar sobre la ubicación, el estado de las TI y la actividad de terminales en cualquier ubicación, incluso en oficinas domésticas. Esta supervisión funciona sobre conexiones estándar de Internet sin necesidad de VPN.

Con estas modernas herramientas, las organizaciones de TI pueden recopilar datos de terminales cada vez más completos, actualizados y precisos respecto a lo que podía obtener cuando la mayoría de los terminales seguían en redes internas y se supervisaban solo esporádicamente con herramientas tradicionales de gestión.

Lo segundo que hay que hacer es medir el riesgo a lo largo del tiempo. Los ejecutivos quieren saber si las medidas de mitigación de riesgos que se han implementado están funcionando. Los equipos de riesgo deben realizar un seguimiento de las métricas que indican si la empresa está alcanzando o no sus objetivos de gestión de riesgos.

Lo tercero es celebrar reuniones sobre riesgos con el equipo ejecutivo basadas en datos. Aquí es donde vale la pena contar con datos más completos y obtenidos a su debido tiempo. Con una visibilidad mejorada de los terminales y otros activos de TI, puede tener una charla con más sentido sobre qué inversiones funcionan y cuáles no.

Cuatro elementos clave de la gestión de riesgos

Teniendo en cuenta los objetivos estratégicos de la organización, estos son cuatro pasos para gestionar el riesgo en una empresa moderna.

Recopilación de datos

Esto significa recopilar todos los datos necesarios para medir los riesgos relacionados con los objetivos estratégicos de la organización. Obviamente, eso incluye datos de los terminales, así como datos ambientales y de usuario.

Análisis

Una vez recopilados los datos, analícelos, preferiblemente utilizando la mayor automatización posible. Es más que probable que el análisis lleve mucho tiempo y sea propenso a errores si depende de varias hojas de cálculo e impresiones de Excel. Si ha creado tablas de puntuación para evaluar los riesgos, puede automatizar las tabulaciones y hacer que el análisis sea un proceso continuo en lugar de una foto fija anual.

Informes

Este paso implica sintetizar las métricas de riesgo y el análisis para los informes a nivel ejecutivo. Estos informes guiarán los debates de la organización sobre riesgos, prioridades, decisiones de inversión, etc. En estos informes, encuadre el análisis de riesgos en términos de los objetivos estratégicos en los que se centran continuamente el Consejo de dirección y el equipo ejecutivo.

Corrección

Hay dos tipos de corrección de riesgos. En primer lugar, el personal de seguridad y operaciones de TI toma medidas diariamente para responder a amenazas, como las infecciones por malware. Estas acciones no requieren aprobación ejecutiva. En segundo lugar, hay acciones adoptadas por los responsables de la empresa y de TI en respuesta a informes a nivel ejecutivo creados en los tres primeros pasos de este proceso. Las empresas deben adoptar ambas formas de corrección de riesgos.

A lo largo del último año, muchas empresas se reinventaron como organizaciones más ágiles y geográficamente distribuidas.

Ahora las empresas también tienen la oportunidad de reinventar sus procesos de evaluación de riesgos. Al aprovechar los datos y la automatización en tiempo real, las empresas pueden reducir los riesgos y mejorar la seguridad de sus trabajadores remotos al mismo tiempo.

CHAPTER 4:

La importancia de hacer que la evaluación de riesgos sea un proceso continuo

Medir el riesgo es un trabajo complicado. Afortunadamente, las nuevas tecnologías pueden ayudar a que la evaluación de riesgos sea un proceso automatizado.

Cada organización se ve amenazada por el riesgo, pero evaluar ese riesgo es más difícil que nunca. En este capítulo explicaremos qué hace que la evaluación de riesgos sea tan difícil y cómo adoptar un enfoque descendente para medir el riesgo puede agilizar este trabajo y ayudar a las organizaciones a tomar mejores decisiones.

Por qué es más difícil medir el riesgo

¿Por qué es tan difícil medir el riesgo hoy en día? He aquí cuatro razones.

Dificultad n.º 1: Activos de TI dispares y variados

Hace veinte años, las evaluaciones de riesgos de TI consistían principalmente en contar los PC y servidores de los empleados en los centros de datos, analizar las posibles vulnerabilidades de varios modelos de hardware y elaborar un informe.

Hoy en día, los activos de TI que se van a catalogar y analizar podrían distribuirse en, por ejemplo, 50 oficinas, 500 centros de datos (la mayoría pertenecen a otras empresas) y 10 000 redes domésticas. Y una parte significativa, probablemente al menos el 20 %, de esa arquitectura distribuida consiste en "TI en la sombra", es decir, productos y servicios que los empleados han adoptado sin aprobación formal y supervisión continua del departamento de TI.

En este entorno de TI altamente distribuido y difícil de catalogar, las herramientas y enfoques tradicionales de medición de riesgos simplemente no funcionarán.

Dificultad n.º 2: **Complejidad de las TI**

Una segunda razón por la que la evaluación de riesgos es difícil es la complejidad de las TI. No es solo que haya más dispositivos, es que la forma en que se crea y funciona el software ha cambiado.

La era de las aplicaciones monolíticas grandes ha terminado. Las actuales infraestructuras de TI abarcan muchos componentes pequeños y medianos que trabajan juntos para crear un todo mayor.

Por ejemplo, una aplicación de banca móvil puede depender de 75 componentes de TI diferentes para funcionar. Estos componentes pueden variar desde el código de interfaz de usuario hasta múltiples bases de datos de back-end. Los riesgos asociados a cada uno de esos componentes afectan a los riesgos de la aplicación en general.

Dificultad n.º 3: **Ataques de seguridad sofisticados**

En tercer lugar, las empresas se ven atacadas por un creciente número de ciberdelincuentes, muchos de los cuales tienen acceso a tecnologías altamente sofisticadas.

Hace veinte años, los atacantes eran principalmente "gente traviesa", programadores informáticos interesados en encontrar formas ingeniosas de causar problemas. Hoy en día, entre los atacantes se hallan estados, sindicatos criminales y los llamados "niños de guión" (Script Kiddies) malintencionados dispuestos a gastar 50 dólares en la Dark Web para comprar un malware o un guión de relleno de credenciales y una lista de credenciales corruptas.

Dificultad n.º 4: **Responsabilidades compartidas**

¿Una dificultad final? Una tendencia reciente en la gestión de riesgos exige compartir los riesgos más ampliamente con las unidades de negocio. La organización de TI podría dirigir el proyecto de evaluación de riesgos de una organización. Pero ahora, los Consejos de dirección y los equipos ejecutivos suelen pedir a los responsables de las unidades de negocio que den un paso adelante y asuman la responsabilidad de los riesgos que afectan a sus operaciones.

Para abordar estas dificultades, adopte un enfoque descendente para medir el riesgo, como mis colegas describieron en los capítulos anteriores de este eBook. Identifique las "cadenas de suministro" que respaldan cada objetivo estratégico y recopile tanta información en tiempo real como sea posible sobre el estado de cada cadena de suministro.

Medir el riesgo es una actividad estratégica continua

Sabrá si cuenta con una práctica eficaz para medir el riesgo si proporciona orientación continua para tomar las correspondientes decisiones empresariales. Para proporcionar esa orientación, la mejor práctica recomendada para medir el riesgo debe ser:

Continua

Las evaluaciones de riesgos de la organización deben actualizarse continuamente con información sobre el estado actual del entorno de TI. Cuando los datos de riesgo están actualizados, puede confiar en que está tomando decisiones sobre la tecnología y los proveedores con los que trabaja ahora, no un conjunto diferente con el que trabajó hace tres meses.

Priorizada

Su práctica de evaluación de riesgos debería facilitar la priorización y mitigación de riesgos en términos de los objetivos estratégicos de la organización. Dispone de puntuaciones de riesgo para poder comparar, por ejemplo, el riesgo de mover un repositorio de datos local a un proveedor de confianza en la nube para reducir costes.

Accesible

Puede acceder fácilmente a las evaluaciones de riesgos siempre que sea necesario. No tiene que buscar en 43 hojas de cálculo de Excel para encontrar el análisis que está buscando. Dispone de informes de riesgo a los que puede acceder rápidamente como parte de la toma de decisiones continua de la empresa.

El negocio se mueve más rápido que nunca. Los entornos de TI son amplios y complejos. Al adoptar un enfoque descendente para medir el riesgo y aprovechar la recopilación y automatización de datos en tiempo real, puede desarrollar la práctica de medición de riesgos que necesita para guiar a su organización por de crecimiento y transformación en los próximos años.

Guía esencial para medir el riesgo

1. Reúnase con los responsables de la empresa para comprender los objetivos estratégicos establecidos a largo plazo para la empresa.
2. Asigne una puntuación a estos objetivos para comprender la importancia relativa de cada uno.
3. Identifique a las personas, los procesos y las tecnologías que están detrás de cada objetivo.
4. Estudie incertidumbres sobre cada factor de apoyo en la "cadena de suministro" de un objetivo.
5. Siempre que sea posible, confíe en la automatización para recopilar datos, por ejemplo, los datos sobre el estado operativo de los terminales.
6. Asigne a cada incertidumbre una puntuación por su importancia y un porcentaje en términos de probabilidad. Multiplique las puntuaciones por la probabilidad de derivar una puntuación de riesgo para una persona o equipo en particular, proceso o tecnología en la cadena de suministro de un objetivo.
7. Cuente los resultados de las mediciones y organícelos de manera que relacionen cada riesgo con un objetivo estratégico.
8. Reúnase de nuevo con los responsables de la empresa para tener una charla sobre riesgos basada en datos. Ayúdeles a comprender los riesgos existentes y las decisiones que se pueden tomar para reducirlos.
9. Ahora que ya dispone de un marco de medición de riesgos, actualícelo recurriendo a la automatización, siempre que sea posible, para que los riesgos se puedan evaluar en detalle en cualquier momento.

El riesgo, según la definición de la norma ISO 31000, significa incertidumbre sobre los objetivos. En este eBook compartimos la sabiduría sobre qué objetivos importan y cómo medir la incertidumbre para obtener el mejor resultado posible: reducir los riesgos que ponen en peligro la misión de una empresa.

Los dispositivos terminales de la empresa desempeñan un papel importante en la gestión de riesgos. Para saber cómo la plataforma Tanium respalda a las organizaciones a administrar, supervisar y proteger sus terminales, visite **Tanium.com** o **solicite una demostración** hoy mismo.