TANIUM

Lo que no sabe puede perjudicarle

Consejos de expertos sobre la medición de riesgos.

Los expertos de la industria ofrecen perspectivas y orientación para medir los riesgos en el mundo actual, altamente distribuido y en constante evolución.

TANIUM

Lo que no conoce puede perjudicarlo: asesoramiento experto sobre la medición del riesgo

Los expertos de la industria ofrecen perspectivas y orientación para medir los riesgos en el mundo actual, altamente distribuido y en constante evolución.

Contenido

Capítulo 1: Medir lo que importa: alinear la medición de riesgos con las metas y los objetivos corporativos

Capítulo 2: Medición del riesgo mediante la identificación de cadenas de suministro de valor

Capítulo 3: Modernización de las evaluaciones de riesgos para las empresas descentralizadas actuales

Capítulo 4: La importancia de hacer que la evaluación de riesgos sea un proceso continuo

Lista de verificación: Guía esencial para medir el riesgo

Consejos de expertos sobre la medición de riesgos

La gestión de riesgos comienza con la medición de riesgos.

Pero ¿cómo mide los riesgos de manera significativa? ¿Debe realizar el recuento de cada vulnerabilidad de software en la empresa? ¿Necesita hacer una lista de todos los dispositivos de punto final que requieren parches de software? ¿Debe reportar las estadísticas de tiempo de actividad para las aplicaciones más críticas de su empresa?

Cuando su trabajo es medir el riesgo, debe enfocarse en lo que es significativo para su audiencia. Y para las decisiones más importantes sobre el riesgo, su audiencia es el equipo ejecutivo de su empresa y la junta directiva.

En este libro electrónico, tres expertos de la industria de TI comparten su conocimiento sobre la práctica de medir el riesgo de la manera más práctica, integral y procesable.

Al final del libro electrónico, incluimos una lista de verificación que resume los consejos presentados por estos expertos. *Comencemos.*

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

Si le pregunta a la mayoría de los expertos en seguridad de TI, el riesgo está en todas partes. Está en puntos finales sin parches, nuevas variantes de malware, ataques de phishing, servicios de nube de TI oculta, computadoras portátiles que quedan en los bancos del parque: la lista continúa. Con tantos detalles técnicos que contribuyen al riesgo, su equipo de riesgo podría estar preguntándose cómo abordar el importante trabajo de medir el riesgo en su empresa.

Por supuesto, nadie mide el riesgo simplemente por medir el riesgo. Las evaluaciones de riesgos se realizan para brindar información a los responsables de la toma de decisiones. La verdadera pregunta es esta: ¿Cómo mide el riesgo de manera que ayude a los líderes de su organización (el equipo ejecutivo y la junta directiva) a comprender el riesgo para que puedan tomar las decisiones correctas para reducirlo?

Medir los riesgos que son importantes para el liderazgo de su empresa

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

Independientemente del negocio en el que se encuentre su empresa, esos objetivos de alto nivel casi con certeza incluyen los siguientes:

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

Consideremos cada uno de estos uno a la vez.

Medición del riesgo asociado con la continuidad del negocio

La continuidad del negocio significa mantenerse atento, mantener a los empleados productivos, mantener las operaciones de fabricación y envío activas y garantizar que cualquier otro tipo de operaciones, ya sea que se trate de bombear aceite o entregar un producto SaaS, pueda continuar funcionando, sin importar qué.

La recuperación ante desastres entra en esta categoría. También protege los servicios críticos para el negocio de las amenazas cibernéticas.

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

En todas las industrias, las personas reconocen la importancia de los datos, es el "nuevo petróleo" de la economía digital, así como la importancia de proteger los datos que son confidenciales.

Los desafíos para proteger esos datos han aumentado. Por un lado, se accede a los datos confidenciales desde más ubicaciones que nunca en un mundo donde el personal trabaja desde casa (work-from-home, WFH), un personal que cada vez depende más de la modalidad de "traiga su propio dispositivo" (BYOD), en lugar de computadoras portátiles y de escritorio probadas y aprovisionadas por el departamento de TI.

Sin embargo, independientemente de dónde o cómo los empleados accedan a los datos, las empresas deben garantizar la confidencialidad (confidentiality), integridad (integrity) y disponibilidad (availability) de los datos (o como se conoce en algunos círculos de TI, la "CIA de datos").

Medición del riesgo asociado con el cumplimiento normativo

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

Pero también existen otras regulaciones, que abarcan todo, desde los reportes financieros hasta la discriminación racial, que las empresas no pueden permitirse infringir. Las fallas regulatorias pueden dar lugar a multas financieras considerables, cancelación de contratos y mala publicidad que dura años.

Para medir el riesgo de manera efectiva, debe saber cuáles son las regulaciones que son importantes para el liderazgo de su empresa. Luego, realiza un seguimiento de los activos y procesos de TI que ayudan a determinar si su empresa cumple con estas regulaciones.

Enmarcar el riesgo con objetivos estratégicos

El trabajo del equipo ejecutivo y de la junta directiva es liderar a la empresa para que logre los objetivos centrales de continuidad del negocio, privacidad de los datos y cumplimiento normativo. Por supuesto, podrían llevar a la empresa a alcanzar otros objetivos, como uno sobre un determinado porcentaje de crecimiento anual o uno que tiene que ver con la cultura de la empresa.

Si desea llamar la atención de estos líderes, enmarque su análisis de las mediciones de riesgos en términos de los objetivos a nivel directivo de su empresa. En otras palabras, identifique y evalúe los diversos riesgos técnicos, reglamentarios y de otro tipo de su empresa, y muestre cómo se relacionan con las metas estratégicas de alto nivel de su empresa.

Verá que enmarcar sus mediciones de riesgo de esta manera ayuda a enfocar su trabajo. Y hace que su trabajo sea más propenso a ser comprendido y apreciado por los líderes empresariales que marcan el rumbo para el futuro de su empresa.

Medición del riesgo a través de la identificación de cadenas de suministro de valor

En este capítulo, profundizamos más en la medición de riesgos para los objetivos de la empresa al analizar la importancia de las escalas ponderadas para diversos riesgos e incluso para los objetivos mismos.

Identificar los riesgos asociados con las metas estratégicas

El trabajo de medir los riesgos comienza identificando las metas estratégicas de su empresa y luego explorando las personas, los procesos y la tecnología que respaldan la búsqueda de su empresa de esas metas.

Considérelo un análisis de la cadena de suministro. Está rastreando el flujo de datos, personas y operaciones desde una meta de alto nivel hasta sistemas y procesos de TI específicos que ayudan a la empresa a alcanzar esa meta. Esos sistemas y procesos funcionan como un tipo de cadena de suministro para las metas en sí.

Para medir el riesgo, identifique las dependencias en esta cadena de suministro y rastree las mismas en la medida en que tenga sentido para las metas y capacidades de su empresa. Para comparar los riesgos dentro de la cadena de suministro en sí, se debe asignar una calificación a todo dentro de la cadena de suministro.

Desarrollar una escala ponderada para los riesgos

Incluso las metas estratégicas en sí se deben comparar y evaluar. Es raro que una empresa trate a todas sus metas estratégicas por igual.

Una vez que haya identificado esas metas, asígneles calificaciones 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 los ingresos de al menos 10% de CAGR con una calificación de 10 y cumplimiento normativo con una calificación de 7.

Luego, identifique a las personas, los procesos y la tecnología involucrados en el apoyo de cada objetivo estratégico y clasifique la importancia de cada uno de esos factores de apoyo.

Para proporcionar más matices, puede estimar la probabilidad de que ocurra un tipo particular de falla. Por ejemplo, imagine que su empresa tiene un servidor web que admite una aplicación móvil crítica para el negocio. Las probabilidades de que ese servidor ofrezca un rendimiento inaceptablemente lento durante un período de uso máximo son probablemente mayores que las probabilidades de que ese mismo servidor sucumba a un corte de energía que bloquee los sistemas de energía principal y de respaldo.

Al multiplicar la calificación de la importancia estratégica del servidor (digamos, 7 de 10) por la probabilidad de un riesgo específico (digamos, 50% o 0,5), puede comenzar a clasificar los riesgos e identificar los riesgos que requieren una acción más inmediata.

Por ejemplo, el servidor que ofrece un rendimiento lento puede tener una probabilidad del 40% y el servidor que falla debido a un corte de energía catastrófico puede tener una probabilidad del 2%. Si la importancia del servidor es 7 de 10, entonces la calificación de riesgo para el escenario de rendimiento lento sería 7 veces 0,40 (lo que da 2,8). La calificación de riesgo para el escenario de corte de energía sería 7 veces 0,02 (lo que da 0,14). El escenario de rendimiento lento, que tiene la calificación de riesgo más alta, es obviamente el riesgo que necesita atención primero.

La importancia de la colaboración en la medición del riesgo

Realizar este tipo de evaluación de riesgos requiere recopilar información detallada sobre las personas, los procesos y la tecnología en toda la empresa. El departamento de TI tendrá que buscar ayuda.

¿Mi consejo? Pida ayuda a cada departamento cuyos procesos y tecnología esté evaluando. Por ejemplo, si realmente desea comprender los riesgos relacionados con las aplicaciones del departamento de RR. HH., hable con las personas del departamento de RR. HH. Podrían conocer aspectos sobre la importancia de una aplicación que el equipo de operaciones de TI ha pasado por alto.

Cuando hable con personas fuera del departamento de TI, minimice el uso del lenguaje técnico. Además, nunca le diga a alguien cómo hacer algo sin preguntarle primero cómo cree que debe hacerse. Si impone una solución a las personas, es posible que omita una alternativa creativa. También puede encontrar que las personas se resisten a seguir una nueva política que los afecta directamente sin tener sus ideas en cuenta.

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

Cuando las personas fuera del departamento de TI se den cuenta de que usted confía en ellas y que está genuinamente 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 implementan juntos.

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

Modernización de las evaluaciones de riesgos para la empresa distribuida actual

La medición del riesgo solía ser un evento especial realizado con los consultores. Con datos y automatización en tiempo real, las empresas ahora miden el riesgo de manera más precisa, continua y efectiva.

El cambio repentino del año pasado a un modelo de trabajo desde casa cambió muchas cosas en la TI empresarial, incluida la forma en que los equipos de TI llevaron a cabo las evaluaciones de riesgos.

En este capítulo, analizamos cómo las empresas tradicionalmente realizaban evaluaciones de riesgos. Luego, consideramos cuántas empresas las han estado llevando a cabo desde que comenzó la pandemia y ofrecemos algunas mejores prácticas para modernizar la evaluación de riesgos, a fin de servir mejor a la empresa altamente distribuida de la actualidad.

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 realizaron reportes detallados que intentaron resumir todos los riesgos de la organización en áreas como seguridad de TI, recuperación ante desastres y cumplimiento.

A fin de recopilar información para sus reportes, los equipos visitaron centros de datos y distribuyeron cuestionarios. Incluso si las visitas fueron minuciosas y los cuestionarios fueron exhaustivos, las evaluaciones invariablemente reflejaron el riesgo en un solo momento en el tiempo.

Si, cinco minutos después de que el equipo abandonara el centro de datos, una nueva actualización de software pusiera en peligro repentinamente la integridad de los reportes financieros de la empresa, el reporte de evaluación de riesgos no reflejaría ese mayor riesgo.

Para muchas organizaciones, la fragilidad de estas evaluaciones de riesgos aumentó durante la pandemia. Los cuestionarios enviados por correo electrónico reemplazaron a las inspecciones en persona. Las partes interesadas completaron debidamente los formularios, 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 manera de realizar evaluaciones de riesgos? He pasado mucho tiempo en mi carrera profesional enfocado en la práctica de las evaluaciones de riesgos, y creo que sí.

Llevar la evaluación de riesgos a la era de la computación en la nube y del trabajo desde casa

Lo primero que hay que cambiar sobre las evaluaciones de riesgos es su puntualidad. Si los reportes se basan en datos recopilados una vez al año, serán imprecisos la mayor parte del tiempo.

Todos sabemos que el ritmo de los negocios es más rápido que nunca. Datos, dispositivos, software, relaciones comerciales: todo esto está en constante cambio. Las evaluaciones de riesgos deben reflejar ese cambio.

Afortunadamente, los departamentos de TI tienen nuevas herramientas que pueden ayudar a mejorar la precisión de las evaluaciones de riesgos. El monitoreo de endpoints en tiempo real, por ejemplo, puede reportar sobre la ubicación, el estado de TI y la actividad de los endpoints en cualquier ubicación, incluso en las oficinas en las casas. Este monitoreo funciona a través de conexiones de Internet estándar sin necesidad de VPN.

Con estas herramientas modernas, las organizaciones de TI pueden recopilar datos de puntos finales más completos, actualizados y precisos de lo que podían cuando la mayoría de los puntos finales todavía estaban en redes internas y siendo monitoreados solo esporádicamente por las herramientas tradicionales de gestión de puntos finales.

Lo segundo que debe hacer es medir el riesgo con el tiempo. Los ejecutivos quieren saber si las medidas de mitigación de riesgos que se han implementado están funcionando. Los equipos de riesgo deben hacer un seguimiento de las métricas que indican si la empresa está logrando o no sus metas para gestionar el riesgo.

Lo tercero es tener conversaciones basadas en datos con el equipo ejecutivo sobre el riesgo. Aquí es donde los datos más oportunos e integrales dan sus frutos. Con una visibilidad mejorada de los puntos finales y otros activos de TI, puede tener un debate más significativo sobre cuáles son las inversiones que funcionan y cuáles no.

Cuatro elementos clave de la gestión de riesgos

Teniendo en cuenta las metas estratégicas de su organización, estos son cuatro pasos para gestionar el riesgo en una empresa moderna.

1. Recopilación de datos

Esto significa recopilar todos los datos necesarios para medir los riesgos relacionados con las metas estratégicas de su organización. Esto obviamente incluye datos de puntos finales, así como datos ambientales y del usuario.

2. Análisis

Una vez que haya recopilado los datos, analícelos, preferentemente utilizando la mayor cantidad de automatización posible. Es más probable que su análisis consuma mucho tiempo y sea propenso a errores si depende de varias hojas de cálculo e impresiones de Excel. Si ha creado planillas de calificaciones para evaluar riesgos, puede automatizar tabulaciones y hacer que el análisis sea un proceso continuo en lugar de una instantánea de una vez al año.

3. Reportes

Este paso implica sintetizar las métricas de riesgo y el análisis para los reportes de nivel ejecutivo. Estos reportes guiarán las discusiones de su organización sobre riesgos, prioridades, decisiones de inversión y más. En estos reportes, enmarque el análisis de riesgos en términos de las metas estratégicas en las que su equipo ejecutivo y la junta se centran continuamente.

4. Corrección

Existen dos tipos de corrección de riesgos. En primer lugar, el personal de seguridad de TI y operaciones de TI toma medidas a diario para responder a las amenazas, como infecciones de malware. Estas acciones no requieren aprobación ejecutiva. En segundo lugar, hay acciones tomadas por los líderes de TI y de negocios en respuesta a los reportes de nivel ejecutivo creados en los primeros tres pasos de este proceso. Las empresas deben emprender ambas formas de remediación de riesgos.

Durante el año pasado, muchas empresas se reinventaron como organizaciones más ágiles y distribuidas geográficamente. 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 fuerzas de trabajo remotas al mismo tiempo.

CAPÍTULO 4:

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

Medir el riesgo es un trabajo complicado. Afortunadamente, la nueva tecnología puede ayudar a que la evaluación de riesgos sea un proceso automatizado.

Todas las organizaciones se ven amenazadas por el riesgo, pero evaluar ese riesgo es más difícil que nunca. En este capítulo, explicamos 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 medir el riesgo se ha vuelto más difícil

¿Por qué medir el riesgo es tan difícil en estos días? Le presentamos cuatro razones.

Dificultad #1: Activos de TI desiguales y variados

Hace veinte años, las evaluaciones de riesgos de TI consistieron principalmente en contar las computadoras de los empleados y los servidores en los centros de datos, analizar las vulnerabilidades probables de varios modelos de hardware y producir un reporte.

En la actualidad, los activos de TI que se catalogarán y analizarán podrían distribuirse entre, por ejemplo, 50 oficinas, 500 centros de datos (la mayoría de los cuales 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 oculta”, 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 los enfoques tradicionales de medición de riesgos simplemente no funcionarán.

Dificultad #2: Complejidad de TI

Una segunda razón por la que la evaluación de riesgos es difícil es la complejidad de TI. No es solo que hay más dispositivos; la forma en que se construye y funciona el software ha cambiado.

La era de las aplicaciones monolíticas grandes ha terminado. La infraestructura de TI actual consta de 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. Esos componentes pueden variar desde el código de la UI hasta varias bases de datos de back-end. Los riesgos asociados con cada uno de esos componentes afectan los riesgos de la aplicación en general. Por eso es fundamental que las empresas tengan una **lista de materiales de software en tiempo real.**

Dificultad #3: Ataques de seguridad sofisticados

Tercero, las empresas están siendo atacadas por un creciente número de ciberdelincuentes, muchos de los cuales tienen acceso a tecnologías altamente sofisticadas.

Hace veinte años, los atacantes eran principalmente creadores de travesuras, programadores informáticos interesados en encontrar formas ingeniosas de causar problemas. Hoy en día, los atacantes incluyen a estados-nación, organizaciones delictivas y "script kiddies" (individuos no calificados que usan scripts ajenos) malintencionados dispuestos a gastar 50 dólares en la web oscura para comprar un malware o un script para completar credenciales y una lista de credenciales corruptas.

Dificultad #4: Responsabilidades compartidas

¿Una última dificultad? Una tendencia reciente en la gestión de riesgos exige compartir los riesgos de manera más amplia con las unidades de negocios. La organización de TI podría liderar el proyecto de evaluación de riesgos de una organización. Pero ahora, los equipos ejecutivos y las juntas directivas piden a los líderes de las unidades de negocios que se pongan a la altura y asuman la responsabilidad de los riesgos que afectan sus operaciones.

Para abordar estas dificultades, adopte un enfoque descendente para medir el riesgo, como lo describieron mis colegas en los capítulos anteriores de este libro electrónico. Identificar las "cadenas de suministro" que respaldan cada meta estratégica y recopilar tanta información en tiempo real sobre el estado de cada cadena de suministro como sea necesario.

La medición del riesgo es una actividad estratégica continua

Sabrá si cuenta con una práctica efectiva para medir el riesgo si brinda orientación continua para tomar decisiones comerciales. Para brindar esa orientación, su mejor práctica para medir el riesgo debe ser:

la continuidad

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

Priorizada

Su práctica de evaluación de riesgos debe facilitar la priorización de riesgos y mitigaciones de riesgos en términos de las metas estratégicas de su organización. Tiene una calificación de riesgo establecida para poder comparar, por ejemplo, el riesgo de mover un repositorio de datos de las instalaciones a un proveedor de nube de confianza para ahorrar dinero.

Accesible

Puede acceder fácilmente a las evaluaciones de riesgos cuando sea necesario. No es necesario que explore 43 hojas de cálculo de Excel para encontrar el análisis que está buscando. Tiene reportes de riesgos 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 de datos en tiempo real y la automatización, puede crear la práctica de medición de riesgos que necesita para guiar a su organización a través del crecimiento y la transformación en los próximos años.

Guía esencial para medir el riesgo

1. Reúnase con los líderes de su empresa para comprender sus objetivos estratégicos a largo plazo para la empresa.
2. Asigne calificaciones a estos objetivos para comprender la importancia relativa de cada uno.
3. Identifique a las personas, los procesos y las tecnologías que respaldan cada objetivo.
4. Explore 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, como datos sobre el estado operativo de los puntos finales.
6. Reúnase con las partes interesadas de varios departamentos para comprender sus inquietudes sobre los riesgos y colaborar en las recomendaciones para reducir esos riesgos.
7. Asigne a cada incertidumbre una calificación en términos de importancia y un porcentaje en términos de probabilidad. Multiplique las calificaciones por la probabilidad de derivar una calificación de riesgo para una persona o equipo, proceso o tecnología en particular en la cadena de suministro de un objetivo.
8. Realice un recuento de los resultados de sus mediciones y organícelos de una manera que relacione cada riesgo con un objetivo estratégico.
9. Vuelva a reunirse con el liderazgo de su empresa para realizar un análisis sobre el riesgo basado en datos. Ayúdelos a comprender los riesgos existentes y las decisiones que se pueden tomar para reducirlos.
10. Ahora que cuenta con un marco de medición de riesgos, continúe actualizándolo, utilizando la automatización siempre que sea posible para que los riesgos puedan evaluarse en detalle en cualquier momento.

El riesgo, según lo define la norma *ISO 31000,* significa incertidumbre acerca de los objetivos. En este libro electrónico, compartimos la conocimientos sobre cuáles son los objetivos importantes y cómo medir su incertidumbre para obtener el mejor resultado posible: reducir los riesgos que ponen en peligro el objetivo de una empresa.

Los dispositivos de punto final de la empresa desempeñan un rol importante en la gestión de riesgos. La plataforma Tanium Converged Endpoint Management (XEM) puede ayudar a dar a las organizaciones mayor visibilidad de sus métricas de seguridad para así identificar riesgos y corregirlos en tiempo real. Tanium Benchmark es la única solución que proporciona comparaciones de riesgos en tiempo real con pares de la industria.

Obtenga más información sobre **Tanium Benchmark.**