Deloitte.

Gobierno inteligente frente al riesgo en la era de las amenazas cibernéticas

Lo que usted no conozca puede hacerle daño

Risk Intelligence Series

Issue No. 23

Contenidos

Prefacio

Esta publicación es el 23º. documento de la serie de Deloitte sobre inteligencia frente al riesgo. Los conceptos y puntos de vista que presentan se elaboran a partir de los contenidos en el primer documento de la serie, *The Risk Intelligent Enterprise™: ERM Done Right* [La empresa inteligente frente al riesgo®: ERM hecho correcto], así como también los títulos subsiguientes. La serie incluye publicaciones que se centran en los roles (El CFO inteligente frente al riesgo, La junta inteligente frente al riesgo, etc.); las industrias (La compañía de tecnología inteligente frente al riesgo, La compañía de energía inteligente frente al riesgo, etc.); y los problemas (Un punto de vista inteligente frente al riesgo sobre la reputación, Inteligencia frente al riesgo en una recesión, etc.). Usted puede tener acceso a todos los documentos de la serie, sin costo, en www.deloitte.com/us/RiskIntelligence.

La comunicación sin barreras es una característica clave de La empresa inteligente frente al riesgo.® Nosotros fomentamos que usted comparta este documento con sus colegas – ejecutivos, miembros de junta, y administradores clave de su compañía. Los problemas que se describen en este documento servirán como el punto de partida para el diálogo crucial para elevar la inteligencia frente al riesgo de su compañía.

Introducción:
¿Podría ello ocurrirnos?

Alarmadas por un aumento en los ataques cibernéticos en negocios de alto perfil, muchas juntas de directores les están haciendo a sus equipos ejecutivos esa pregunta. Desafortunadamente, en la mayoría de las compañías, la respuesta corta puede muy bien ser que *ello ya está ocurriendo*. Considere:

- Cincuenta negocios que participaron en un estudio realizado en el 2011 sobre el crimen cibernético experimentaron un promedio de más de un ataque cibernético exitoso por compañía por semana – un incremento del 44 por ciento en relación con la tasa del 2010.[1]
- Una encuesta realizada en 2010 de brechas de datos en 28 países encontró que más de 721.9 millones de registros de datos fueron comprometidos durante los cinco años que terminaron en diciembre 31, 2009. Esto se refiere a la exposición inadvertida de 395,362 registros cada día.[2]
- En noviembre 2011, una compañía líder de seguridad cibernética reportó que detectó cuatro veces más ataques "dirigidos" que los que detectó sólo 11 meses antes, en enero 2011. Definidos como los ataques dirigidos a una persona u organización específica más que a víctimas al azar, los ataques cibernéticos dirigidos se consideran especialmente peligrosos porque a menudo son la punta de lanza de amenazas persistentes avanzadas (ATP = advanced persistent threats) – "campañas" electrónicas maliciosas de largo plazo que pueden ser extremadamente difíciles de descubrir y abordar.[3]

A la luz de estadísticas como esas, pensamos que es razonable asumir que la mayoría de las compañías ya sea han estado o están en riesgo de ser comprometidas por el crimen cibernético.

"Dado que las amenazas cibernéticas son tanto una fuente de riesgo relativamente nueva como constantemente en evolución, muchas organizaciones pueden no ser tan efectivas en la administración del riesgo de amenaza cibernética como están administrando el riesgo en otras áreas."

Si bien la mayoría de los ataques cibernéticos no se convierten en titulares de las noticias nacionales, pueden dañar un negocio en cualquier número de formas, desde simplemente destrozar su sitio web hasta cerrar las redes, perpetrar fraude y robar propiedad intelectual. El impacto financiero puede ser importante: un estudio de 2011 reportó un costo medio anualizado de $5.9 millones relacionado con el crimen cibernético entre los negocios participantes, un incremento del 56 por ciento sobre el año anterior.[4] Los ataques cibernéticos también pueden asestar un duro golpe a la marca y a la reputación de la compañía, con consecuencias potencialmente importantes. Las preocupaciones acerca de la seguridad de los datos pueden inducir que los clientes actuales y prospectivos lleven sus negocios a otras partes, y las reacciones negativas entre los inversionistas pueden aún orientar pérdidas en el valor de mercado.[5]

Es más, dado que las amenazas cibernéticas son tanto una fuente de riesgo relativamente nueva como constantemente en evolución, muchas organizaciones pueden no ser tan efectivas en la administración del riesgo de amenaza cibernética como están administrando el riesgo en otras áreas. Una estadística reveladora en este sentido es que el 86 por ciento de las violaciones de datos examinadas en un estudio de 2011 fueron descubiertas, no por la misma organización victimizada, sino por partes externas tales como programas de cumplimiento forzoso de la ley o de detección del fraude realizados por terceros. Tal y como lo señalan los investigadores, "Si una organización… debe ser informada acerca [de la violación] por un tercero, es probable que no sea tan conocedora como debe serlo en relación con sus propias redes y sistemas."[6]

La reciente actividad de la U.S. Securities and Exchange Commission (SEC) respalda la opinión de que el riesgo de amenaza cibernética merece consideración a nivel de la junta, al menos desde el punto de vista de revelación. Tomando nota de que "los riesgos… asociados con la seguridad cibernética se han incrementado [recientemente]," la SEC publicó orientación en octubre de 2011 con la intención de "ayudarles a las entidades registradas a valorar qué revelaciones, si las hay, deben proporcionar acerca de la seguridad cibernética."[7] Esta orientación, si bien no es un requerimiento actual de presentación de reporte, ilustra la extensión en la cual las preocupaciones acerca del impacto que en los negocios tiene el crimen cibernético han influido en la conciencia del público.

Haga una pregunta útil, consiga una respuesta útil

Con probabilidad, el impacto, y la vulnerabilidad acerca del riesgo de amenaza cibernética son potencialmente altos – y con la SEC, en efecto, ahora urgiendo a que las compañías consideren rebelar los incidentes cibernéticos – las juntas de directores tienen una buena razón para hacer sus preguntas más allá de "¿Podría ocurrirnos a nosotros?" hasta "¿Qué tan probable es que nos ocurra, y qué estamos haciendo al respecto?" De manera más formal, los problemas centrales para que las juntas los consideren son *exposición* y *efectividad*: "¿Cuál es el nivel de exposición de nuestra compañía ante el riesgo de amenaza cibernética? Y, ¿qué tan efectivo es para mantener esa exposición dentro de los límites que son aceptables?"

El desafío frecuente, sin embargo, es que reposar las preguntas en esos términos de alto nivel no siempre permitir que se obtengan respuestas útiles. Ello porque, a menos que la compañía sea bastante sofisticada en sus prácticas de administración del riesgo de amenaza cibernética, puede no tener en funcionamiento la infraestructura de administración del riesgo y/o los elementos de gobierno para respaldar una conversación significativa. Por ejemplo, los líderes pueden no haber acordado acerca de las definiciones del riesgo, tolerancias del riesgo, o métricas específicas para el riesgo de amenaza cibernética. O la compañía puede carecer de las herramientas de tecnología para recaudar y reportar de manera efectiva la información relacionada con las amenazas cibernéticas.

Afortunadamente, las juntas no necesitan estar completamente en la oscuridad aún en las compañías que todavía estén aumentando sus capacidades de administración del riesgo de amenaza cibernética. Si su organización todavía no está en posición para discutir la exposición y la efectividad como tal, nosotros recomendamos, como un primer paso, hacerle a su equipo ejecutivo cuatro preguntas acerca de las prácticas específicas de seguridad de la información que nosotros consideramos son esenciales para la administración efectiva del riesgo de amenaza cibernética.

Esas preguntas son:

- *¿Cómo rastreamos qué información digital está saliendo de nuestra organización y a dónde se va esa información?*
- *¿Cómo sabemos quién realmente está teniendo acceso a nuestra red, y desde dónde?*
- *¿Cómo controlamos el software que se ejecuta en nuestros dispositivos?*
- *¿Cómo limitamos la información que voluntariamente hacemos disponible para un adversario cibernético?*

Esas medidas no son todo lo que hay que hacer en la lucha contra las amenazas cibernéticas, pero representan los elementos centrales de una defensa cibernética efectiva. Esto, a su vez, hace que las prácticas de su organización en esas áreas sean una aproximación razonable para la efectividad de sus prácticas de administración del riesgo de amenaza cibernética en general. Mediante la aplicación de una perspectiva de maduración de la administración del riesgo (que se discute adelante) a cómo se abordan esos problemas, usted puede obtener luces valiosas sobre las fortalezas y debilidades de la administración del riesgo cibernético en su organización – así como también cómo puede ser capaz de mejorarlas.

Un punto de vista inteligente frente al riesgo de la madurez de la administración del riesgo de amenaza cibernética

Puede ser justo preguntarse, especialmente si usted no tiene los antecedentes de un profesional en TI, si pedirles a los ejecutivos información acerca de las medidas de seguridad puede conducir a que lo llenen de respuestas plagadas de jergas que lo dejen peor que antes. Sin embargo, una conciencia básica de los elementos clave a mirar puede ayudarle a usted a entender las implicaciones que una respuesta tiene para la administración del riesgo aún si usted no está familiarizado con alguna terminología técnica. Para hacer ello, le sugerimos que vea las prácticas de seguridad de la información de su compañía a través de los lentes de la *maduración* de la administración del riesgo: esto es, la extensión en la cual ha progresado hacia la inteligencia frente al riesgo en su enfoque para cada una de las cuatro áreas que se mencionaron arriba.

La Tabla 1 que se presenta en la siguiente página describe cada nivel organizacional al cual se puede acercar la empresa inteligente frente al riesgo para la administración del riesgo de amenaza cibernética en etapas sucesivas de maduración. (El recuadro que aparece en la página 6, *"El perfil de la maduración en la empresa inteligente frente al riesgo*[MR]," ofrece una discusión más completa). Incluso dibujando en esos grandes rasgos, podemos pensar que esta descripción de la evolución de la madurez de la administración del riesgo de amenaza cibernética puede llevarle un camino largo para determinar la posición de su propia organización en este sentido. Dicho esto – en caso de que las pinceladas amplias no sean suficientes – aquí hay una mirada más de cerca a cada una de las prácticas de seguridad de la información que pueden ayudar a arrojar más luz sobre los detalles.

No se trata sólo de quién lo consigue, sino de qué consigue

La pregunta para la administración: ¿Cómo rastreamos qué información digital está saliendo de nuestra organización y a dónde se está dirigiendo esa información?

En muchas compañías, las prácticas de la seguridad cibernética se inclinan fuertemente hacia medidas, tales como los cortafuegos y las contraseñas, que buscan limitar el acceso a la red de la compañía. Pero si bien esas precauciones son esenciales, no son suficientes. Los criminales cibernéticos de manera creciente se están volviendo adeptos a infiltrar las redes corporativas sin desencadenar una alerta de intrusión. Una vez que están adentro, de manera desapercibida fácilmente pueden desviar la información fuera de la red a menos que usted de manera activa mire las señales de actividad sospechosa.

Para ayudar a derrotar a los criminales cibernéticos que llegan más allá de los controles de acceso, una capacidad madura de administración del riesgo de amenaza cibernética incluirá salvaguardas contra *distribución* no autorizada de información, así como también el *acceso* no autorizado a información. El desempeño efectivo en este sentido hace uso de tecnologías y procesos que monitorean el tráfico de la salida de información tanto por contenido -¿la información es apropiada para compartirla? – como por destino - ¿a dónde se está enviando?. El destino, en particular, puede ser una bandera roja; si la información está siendo enviada a un país donde su compañía no tiene presencia operacional, probablemente es sabio mirar a quién se le está enviando y por qué. Una capacidad madura también será capaz de restringir la transmisión de comunicaciones sospechosas hasta tanto se verifique su legitimidad – por ejemplo, con tecnologías que electrónicamente "ponen en cuarentera" la comunicación mientras se realizan las verificaciones apropiadas.

Cuando Jane de Kanzas se conecta desde Uzbekistan, preocupa

La pregunta para la administración: ¿Cómo sabemos quién realmente está conectándose a nuestra red, y de dónde?

Dado que los criminales cibernéticos cada vez son más capaces en suplantar al personal corporativo de buena fe, la compañía no debe asumir que todo quien se conecta con las credenciales legítimas es actualmente un usuario legítimo. Una capacidad madura de administración del riesgo de amenaza cibernética usará al menos dos métodos – posiblemente más, dependiendo del valor de los activos que se estén protegiendo – para verificar la identidad de una persona en la vida real antes de aceptarla como auténtica. Las técnicas disponibles incluyen datos biométricos (e.g., lectores portátiles de huellas digitales), dispositivos de código token (dispositivos de tamaño miniatura, llevados físicamente por los usuarios legítimos, que cada vez que se conectan generan un diferente código aleatorio de autenticación) y programas de "huellas de la máquina" que rastrean el comportamiento posterior al conectarse contra los patrones históricos para determinar la probabilidad de que un usuario sea genuino. También existen otros enfoques más esotéricos, que su equipo de seguridad de TI debe ser capaz de describir.

Aquí, también, la información acerca de la localización – en este caso, los países donde se supone los usuarios están teniendo acceso a nuestra red – puede ser central para identificar las amenazas potenciales. Los inicios de sesión en países donde su compañía carece de operaciones deben ser identificados e investigados para determinar si los usuarios en cuestión son genuinos o fraudulentos. Sí, es posible que Jane de Kansas realmente esté conectándose desde Uzbekistan – pero no hace daño comprobar.

Tabla 1: Etapas de la maduración del riesgo de amenaza cibernética

		Etapa 1: Inicial	Etapa 2: Fragmentada	Etapa 3: Desde arriba-hacia-abajo	Etapa 4: Integrada	Etapa 5: Inteligente frente al riesgo
Gobierno del riesgo (junta de directores)		Reactiva, comunicación orientada-a-incidentes con la administración; métricas ausentes o inconsistentemente definidas/medidas	Comunicación ocasional y/o informal con la administración; métricas de alguna manera estandarizadas, pero carecen de vínculo claro con el valor del negocio	Comunicación formalizada pero inconsistente con la administración; métricas en su mayoría estandarizadas y disponibles a partir de solicitud	Comunicación regular (e.g., trimestral) con la administración; métricas estandarizadas construidas para elaborar KPI que de manera clara vinculen el valor del negocio	Diálogo continuo con la administración; métricas críticas e indicadores claves de desempeño (KPI) acordados y monitoreados en tiempo real
Infraestructura del riesgo (administración ejecutiva)	**Personas**	El equipo ejecutivo es consciente del riesgo de amenaza cibernética y tiene el conocimiento básico de las políticas, procesos, herramientas y tecnologías de seguridad que son deseables; los roles y las responsabilidades para la administración del riesgo de amenaza cibernética no están claramente diferidos; el equipo de seguridad de TI carece del conocimiento especializado acerca del riesgo de amenaza cibernética	El equipo ejecutivo reconoce el riesgo de amenaza cibernética como un área de riesgo potencialmente importante; los roles y responsabilidades pueden estar definidos en las unidades y funciones de negocio, pero no están coordinados centralmente; el equipo de seguridad de TI tiene algún conocimiento especializado acerca del riesgo de amenaza cibernética	El equipo ha establecido roles y responsabilidades para toda la empresa para la administración del riesgo de amenaza cibernética; el personal clave está entrenado en los procedimientos de respuesta incidentales; el equipo de seguridad de TI percibe al conocimiento del riesgo de amenaza cibernética como una competencia requerida	El equipo ejecutivo despliega recursos para obtener inteligencia de la amenaza proveniente de fuentes comerciales y alerta a las unidades y funciones de negocio (incluyendo TI) ante cualquier necesidad para desarrollar controles adicionales; el equipo de seguridad de TI posee conocimiento específico de la industria – y de negocios – para enriquecer la inteligencia de la amenaza y tomar la acción apropiada	El equipo ejecutivo tiene el conocimiento de fondo e información actualizada para integrar de manera activa al riesgo de amenaza cibernética en las decisiones más amplias de ERM; la empresa usa la inteligencia de la amenaza cibernética para ayudar a administrar el riesgo en todas las clases (no solamente el riesgo de amenaza cibernética) dentro de niveles de tolerancia definidos
	Procesos	Procesos ad hoc, desorganizados y/o fragmentados, principalmente manuales o basados en hojas de cálculo; ejecución inconsistente; poca o ninguna documentación	Existen procesos en islas; el diseño y la ejecución pueden variar de isla a isla; alguna documentación	Procesos definidos que se alinean con la estructura de administración del riesgo de toda la empresa; los procesos son ejecutados de manera consistente y están claramente documentados	La organización formalmente mide y monitorea la efectividad del proceso; la automatización se busca como meta; la administración del riesgo de amenaza cibernética puede estar organizada como su propio "programa"	Procesos dirigidos por esfuerzos de mejoramiento continuo, incluyendo automatización y otras medidas de facilitación cuando sea apropiado; programa estructurado de administración del riesgo de amenaza cibernética, integrado con la administración amplia del riesgo de TI y los programas de administración del riesgo de la empresa
	Tecnología	Tecnología instalada/ actualizada sobre una base fragmentaria; implementados controles basados-en-firmas tales como anti-virus y software de detección de intrusión; el acceso es permitido, pero no está centralizado	Acceso centralizado y se han establecido las correlaciones básicas para monitorear las amenazas; se utilizan herramientas forenses para responder a los incidentes	Los RSS de monitoreo de amenazas, comercialmente disponibles, se integran con el acceso centralizado y la capacidad de monitoreo para generar alertas automatizadas	Implementadas herramientas para realizar correlaciones avanzadas en la información de amenazas y para convertir la inteligencia enriquecida en alertas accionables	La tecnología es usada para automatizar no solo el monitoreo de las amenazas y de las alertas, sino también otros procesos de seguridad tales como malware, análisis forense, y valoración de la amenaza
Propiedad del riesgo (funciones y unidades de negocio)		Políticas, entrenamiento y/o comunicaciones existen en los bolsillos a través de la organización con poca o ninguna coordinación a nivel de la empresa	Políticas, entrenamiento y comunicaciones existen a través de la mayoría de la organización, pero no están coordinadas a nivel de la empresa; los empleados en roles "sensibles" pueden tener responsabilidades específicas de rol	Existen políticas, entrenamiento y comunicaciones estándar de la empresa; el cumplimiento puede no ser monitoreado o forzado de manera consistente; los empleados en roles "sensibles" tienen responsabilidades definidas específicas de rol	Políticas, entrenamiento, y comunicaciones estándar de la empresa son difundidas de manera efectiva y son monitoreadas y forzadas de manera consistente; la mayoría o todos los empleados (no solamente los que están en roles "sensibles") tienen responsabilidades claramente definidas para la administración del riesgo cibernético, apropiadas para su rol	Además de lo precedente, han sido diseñados de manera específica incentivos para recompensar al personal clave con base en su desempeño de la administración del riesgo de amenaza cibernética

El perfil de la maduración en la empresa inteligente frente al riesgo[MR]

De acuerdo con nuestro punto de vista, la madurez de la administración del riesgo puede ser valorada en tres niveles organizacionales distintos, que se ilustran en la Figura 1 como parte de la estructura de la Risk Intelligent Enterprise [Empresa inteligente frente al riesgo]. En una empresa inteligente frente al riesgo, cada nivel organizacional asume responsabilidades específicas de administración del riesgo, con las actividades en todos los tres niveles integradas en un programa sistemático de administración del riesgo de la empresa (ERM = Enterprise Risk Management). La efectividad de cada nivel en la ejecución de sus responsabilidades en cualquier área de riesgo dada señala su madurez en esa área; los niveles más altos de madurez típicamente están asociados con mayor efectividad de la administración del riesgo y más baja exposición ante el riesgo.

Vale la pena observar aquí que usted no necesita apuntar al nivel "más alto" de maduración en la administración de *cada* área de riesgo que sea concebible. Mucho del arte de la inteligencia frente al riesgo radica en entender cómo la madurez de su organización necesita estar en áreas específicas con el fin de mantener dentro de límites aceptables la exposición total de la organización frente al riesgo.

Entonces, ¿qué significa "madurez" en relación con la administración del riesgo de amenaza cibernética? A nivel de *gobierno del riesgo* dos indicadores fuertes de madurez son la extensión del compromiso entre la junta y la administración ejecutiva en el riesgo de amenaza cibernética, y la sofisticación del enfoque de la administración ante las métricas del riesgo de amenaza cibernética.

Una junta altamente comprometida tendrá un enfoque formal, disciplinado, para monitorear el riesgo de amenaza cibernética. Puede, por ejemplo, requerir que el director de información jefe o el director de seguridad de información jefe presente actualizaciones regulares del riesgo de amenaza cibernética, y el tablero de reporte de la junta puede incluir métricas o indicadores clave de desempeño (KPI = key performance indicators) relacionados con el riesgo de amenaza cibernética. Las métricas y los KPI mismos típicamente serán definidos en términos cuantitativos y estandarizados a través de la empresa, y su relevancia para el valor de negocios habrá sido reconocida tanto por la junta como por la administración ejecutiva. La junta y la administración también habrán acordado sobre un conjunto central de métricas, o KPI derivados de ellas, para ser monitoreados continuamente por banderas rojas que disparen cualesquiera planes de contingencia.

El nivel de *infraestructura del riesgo*, propiedad de la administración ejecutiva, es responsable por implementar y mantener las personas, los procesos y los elementos de tecnología que se necesitan para hacer que la administración del riesgo "funcione." Con relación a las personas, el equipo ejecutivo puede dedicar recursos para recopilar la inteligencia de la amenaza cibernética con el fin de alertar a las unidades y funciones de negocio (incluyendo el equipo de seguridad de TI) para cualquier necesidad de controles adicionales. El equipo de seguridad de TI, por su parte, verá al conocimiento especializado acerca del riesgo de amenaza cibernética como una competencia central. Dado que cada industria tiene un perfil distintivo de riesgo de amenaza cibernética orientado por la naturaleza de la información que la industria maneja y los tipos de criminales cibernéticos que busca, los especialistas en amenaza cibernética de la compañía deben entender no solo la naturaleza de las amenazas mismas, sino también el panorama de las amenazas que aplica a la industria y al negocio específicos de la organización. Además, un enfoque maduro colocará la responsabilidad por la administración del riesgo de TI, incluyendo la administración del riesgo de amenaza cibernética, en ángulo recto al nivel principal de la sala directiva. En lugar de ser tres o cuatro pasos removidos del CEO, por ejemplo, el director de seguridad de información o equivalente puede reportar directamente al CEO.

Figura 1. Estructura de la empresa inteligente frente al riesgo[MR], de Deloitte

Los procesos altamente maduros de administración del riesgo cibernético son repetibles, claramente definidos, bien documentados, y alineados con la estructura más amplia de administración del riesgo de TI (ITRM*) y de ERM de la organización. La organización puede medir y monitorear la efectividad y la eficiencia del proceso, así como también aplicar técnicas de mejoramiento continuo para fortalecer el desempeño.

La madurez tecnológica alrededor de la administración del riesgo de amenaza tecnológica cae en dos categorías. La primera es la extensión en la cual la tecnología apoya el proceso de ejecución. En particular, la automatización puede hacer más efectivos y eficientes los procesos mediante incrementar la velocidad, mejorar la confiabilidad, y reducir la necesidad del esfuerzo humano. La segunda dimensión de la madurez tecnológica es la manera como la tecnología es usada para disuadir, detectar, y defender contra las amenazas cibernéticas mismas. Esas tecnologías abarcan todas las gamas desde aplicaciones simples de protección de contraseñas hasta tecnologías sofisticadas de monitoreo, minería y análisis automatizado de los datos.

El nivel de *propiedad del riesgo*, que consiste en las unidades de negocio y las funciones de apoyo de la compañía, es donde ocurre la mayoría de las actividades actuales de administración del riesgo y monitoreo de la compañía. Aquí, madurez alta significa que los empleados tienen responsabilidades bien definidas, apropiadas para su rol, para la administración del riesgo de amenaza cibernética; que la organización ha implementado políticas para guiar la manera como los empleados reciben entrenamiento apropiado para el rol sobre cómo cumplir con las políticas y llevar a cabo sus responsabilidades. La organización promueve de manera activa entre sus empleados la administración del riesgo de amenaza cibernética, haciéndolo mediante comunicaciones, revisiones del desempeño, e incluyo incentivos que respaldan el comportamiento deseado.

"Mi teléfono inteligente se está comportando de manera extraña"

La pregunta para la administración: ¿Cómo controlamos el software que se está ejecutando en nuestros dispositivos?

Desde virus y gusanos hasta rootnets, troyanos, bots, y más, el malware – la abreviatura para el "software malicioso" – se ha convertido en el arma de los criminales cibernéticos para subvertir los dispositivos digitales. Ningún dispositivo es inmune: el malware puede infectar cualquier cosa que acepte información electrónica, incluyendo objetivos no-convencionales tales como registradoras de efectivo, cámaras, e incluso carros.[8] Los dispositivos móviles, especialmente, han visto un auge en las infecciones de malware en la medida en que ha crecido su popularidad.[9] Este incremento puede representar una vulnerabilidad importante en entornos donde los empleados usan teléfonos inteligentes, tabletas, computadores portátiles, y otros dispositivos móviles para propósitos tanto personales como de negocios.

Una organización capacidades altamente maduras anti-malware abordará el problema desde los lados tanto del usuario como de la tecnología. En el frente del usuario, la compañía debe desarrollar, comunicar y hacer forzosas políticas que limiten el uso de dispositivos de propiedad personal para los propósitos de negocio y viceversa. Esto puede ayudar a prevenir que los usuarios infecten los dispositivos corporativos con malware prevalente en sitios visitados principalmente por razones personales, así como también reducir el riesgo de que un dispositivo personal infectado contendrá información corporativa sensible. Los usuarios también deben ser educados en la necesidad de reportar el comportamiento sospechoso del dispositivo (tal como accidentes repetidos) a TI para investigación.

En el frente de la tecnología, las compañías deben emplear software tanto para ayudar a mantener el malware fuera de sus dispositivos en primer lugar, como para ayudar a identificar y remover cualquier malware que se deslice a través de – idealmente, antes que ocurra un daño importante. Sea consciente de que los programas anti-virus estándar usualmente no son efectivos contra el malware, el cual a menudo requiere técnicas más especializadas. A causa de esto, usted puede querer solicitarle a su equipo ejecutivo de manera específica acerca de qué tecnologías centradas en malware tiene en funcionamiento su organización.

* ITRM = Information Technology Risk Management = Administración del riesgo de tecnología de la información (N del t).

En boca cerrada no entran moscas

La pregunta para la administración: ¿Cómo limitamos la información que voluntariamente hacemos disponible para los adversarios cibernéticos?

Nadie cuestiona la necesidad de proteger la información que su organización de manera explícita designa como confidencial. Lo que muchas personas no se dan cuenta, sin embargo, es que los criminales cibernéticos también se pueden beneficiar de la información que usted y otros comparten *intencionalmente*. Recursos Humanos, sin saberlo, puede colocar detalles en una descripción de trabajo – digamos, para una posición de seguridad de TI – que revela de manera exacta qué versión de plataforma de planeación de recursos de la empresa está operando su compañía y qué software de seguridad está usando usted para protegerlo. O el anuncio que un empleado haga en un medio de comunicación social puede mencionar que administra las contraseñas de su compañía – por consiguiente diciéndoles a los criminales cibernéticos exactamente a quién necesitan engañar, usando phishing y otras técnicas de ingeniería social, para tener acceso a la red de su compañía.

Una capacidad madura de administración del riesgo de amenaza cibernética reconocerá la necesidad de administrar los riesgos que puedan surgir del compartir información que, si bien no es estrictamente confidencial, puede darles a los criminales cibernéticos pistas valiosas acerca de cómo infiltrar su organización. Los elementos para mirar aquí incluyen políticas para toda la empresa y entrenamiento en problemas tales como la extensión en la cual los empleados pueden discutir su trabajo en foros de Internet o usar cuentas personales de correo electrónico para propósitos de negocio. Esos requerimientos de políticas y de entrenamiento deben ser personalizados para los diferentes roles organizacionales, y de manera especial deben ser exigentes para departamentos, tales como Recursos Humanos, que comúnmente liberan información que se sabe es útil para los criminales cibernéticos. Políticas similares deben ser escritas en los acuerdos de la organización con proveedores y contratistas.

La compañía también puede tomar ventaja de las tecnologías avanzadas de búsqueda y de filtros para monitorear Internet y otras fuentes de datos electrónicos por la aparición de información que pueda señalar un riesgo incrementado de amenaza cibernética. Cualquier esfuerzo de monitoreo debe considerar como un todo el universo de la información disponible más que cada pieza individual de información, dado que los criminales cibernéticos – usando el mismo tipo de tecnología – pueden hacer minería de una variedad de fuentes por bits de información que, si bien en si mismos cada uno puede ser inofensivos, colectivamente pueden revelar lo suficiente como para constituir una amenaza.

Administración madura del riesgo de amenaza cibernética: proactiva y preventiva

El enfoque que aquí esbozamos no tiene la intención de sustituir la valoración formal, rigurosa, de la seguridad de TI realizada por especialistas. Pero puede darle a usted un inicio razonable hacia el entendimiento de las capacidades de su organización para administrar y mitigar el riesgo siempre presente que hoy generan las amenazas cibernéticas. Las luces que usted puede obtener a través de estos pasos pueden ayudarle a realizar indagaciones adicionales que examinen el problema con mayor profundidad – lo cual puede incluir solicitar una valoración formal para determinar cómo su organización puede mover sus prácticas de administración del riesgo de amenaza cibernética hacia un enfoque más proactivo, preventivo y maduro.

En el cierre, consideramos que explorar con su equipo el riesgo de amenaza cibernética puede dar un valor más allá de ayudarle a usted a mejorar el gobierno sobre esta área de riesgo. También puede darle a usted la oportunidad para construir un diálogo más productivo con los ejecutivos acerca de la administración del riesgo de TI en general. Nosotros fomentamos que usted use esas discusiones con la administración tanto como una manera para fortalecer las prácticas de administración del riesgo de amenaza cibernética de su compañía, como una plataforma de lanzamiento hacia mayor compromiso con su equipo de administración en todos los aspectos del riesgo de TI.

Apéndice: 10 pasos hacia el gobierno más efectivo del riesgo de amenaza cibernética

1. Manténgase informado acerca de las amenazas cibernéticas y su impacto potencial en su organización.
2. Reconozca que la inteligencia frente al riesgo de amenaza cibernética es tan valiosa como la inteligencia tradicional de negocios.
3. Haga responsable a los ejecutivos del nivel directivo por la administración del riesgo de amenaza cibernética.
4. Proporcione recursos suficientes para los esfuerzos de la administración del riesgo de amenaza cibernética de la organización.
5. Requiera que la administración elabore reportes regulares (e.g., trimestralmente), sustantivos, sobre las prioridades principales de la administración del riesgo de amenaza cibernética de su organización.
6. Espere que los ejecutivos establezcan métodos de monitoreo continuo que puedan ayudarle a la organización a predecir y prevenir los problemas relacionados con la amenaza cibernética.
7. Requiera que auditoría interna evalúe la efectividad de la administración del riesgo de amenaza cibernética como parte de sus revisiones trimestrales.
8. Espere que los ejecutivos hagan seguimiento a y reporten sobre las métricas que cuantifican el impacto de negocios que tienen los esfuerzos de administración del riesgo de amenaza cibernética.
9. Monitoree la legislación y la regulación, actual y futura potencial, relacionada con la seguridad cibernética.
10. Reconozca que la administración efectiva del riesgo de amenaza cibernética puede darle a su compañía más confianza para asumir ciertos riesgos “recompensados” (e.g., adoptar la computación en la nube) para buscar valor nuevo.

Contactos

Donna Epps
U.S. Co-Leader
Governance and Risk Management
Deloitte Financial Advisory Services LLP
+1 214 840 7363
depps@deloitte.com

Henry Ristuccia
U.S. Co-Leader
Governance and Risk Management
Deloitte & Touche LLP
+1 212 436 4244
hristuccia@deloitte.com

Scott Baret
Partner
Deloitte & Touche LLP
+1 212 436 5456
sbaret@deloitte.com

Rita Benassi
Partner and U.S. Tax Leader
Governance and Risk Management
Deloitte Tax LLP
+1 813 470 8638
rbenassi@deloitte.com

Mark Carey
Partner
Deloitte & Touche LLP
+1 571 882 5392
mcarey@deloitte.com

Michael Fuchs
Principal
Deloitte Consulting LLP
+1 973 602 5231
mfuchs@deloitte.com

Sandy Pundmann
Partner
Deloitte & Touche LLP
+1 312 486 3790
spundmann@deloitte.com

Nicole Sandford
Partner
U.S. Center for Corporate Governance
Deloitte & Touche LLP
+1 203 708 4845
nsandford@deloitte.com

Rich Baich
Principal
Deloitte & Touche LLP
+1 704 887 1563
jbaich@deloitte.com

Michael Monday
Senior Manager
Deloitte & Touche LLP
+1 704 887 1544
mmonday@deloitte.com

Irfan Saif
Principal
Deloitte & Touche LLP
+1 408 704 4109
isaif@deloitte.com

Nueve principios fundamentales de un programa de inteligencia frente al riesgo

1. En la *empresa inteligente frente al riesgo*, una definición común de riesgo, que aborda tanto la preservación de valor como la creación de valor, es usada consistentemente a través de la organización.

2. En la *empresa inteligente frente al riesgo*, una estructura común del riesgo, apoyada por estándares apropiados, es usada a través de la organización para administrar los riesgos.

3. En la *empresa inteligente frente al riesgo*, los roles, responsabilidades y autoridades, que son clave en relación con la administración del riesgo, están claramente definidos y delineados dentro de la organización.

4. En la *empresa inteligente frente al riesgo*, se usa una infraestructura común de administración del riesgo para darle respaldo a las unidades de negocio y a las funciones en el desempeño de sus responsabilidades frente al riesgo.

5. En la *empresa inteligente frente al riesgo*, los cuerpos de gobierno (e.g. juntas, comités de auditoría, etc.), para cumplir sus responsabilidades tienen las adecuadas transparencia y visibilidad en las prácticas de administración del riesgo de la organización.

6. En la *empresa inteligente frente al riesgo,* la administración ejecutiva tiene a su cargo la responsabilidad primaria por diseñar, implementar y mantener un programa efectivo frente al riesgo.

7. En la *empresa inteligente frente al riesgo*, las unidades de negocio (departamentos, agencias, etc.) son responsables por el desempeño de sus negocios y por la administración de los riesgos que asumen dentro de la estructura del riesgo establecida por la administración ejecutiva.

8. En la *empresa inteligente frente al riesgo*, ciertas funciones (e.g., finanzas, legal, tecnología de la información, recursos humanos, etc.) tienen un impacto penetrante en el negocio y le proveen apoyo a las unidades de negocio en cuanto se relaciona con el programa de riesgo de la organización.

9. En la *empresa inteligente frente al riesgo*, ciertas funciones (e.g., auditoría interna, administración del riesgo, cumplimiento, etc.) proveen aseguramiento objetivo así como también monitorean y le reportan, a los cuerpos de gobierno y a la administración ejecutiva, respecto del programa de riesgo de la organización.

Notas finales

[1] "Second annual cost of cyber crime study: Benchmark study of U.S. companies," Ponemon Institute, August 2011, p. 1. Available online at http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf.

[2] Suzanne Wildup, "The leaking vault: Five years of data breaches," Digital Forensics Association. July 2010. Available online at http://www.digitalforensicsassociation.org/storage/The_Leaking_Vault-Five_Years_of_Data_Breaches.pdf.

[3] "Symantec Intelligence Report: November 2011," Symantec Corporation, 2011. Available online at http://www.symanteccloud.com/mlireport/SYMCINT_2011_11_November_FINAL-en.pdf.

[4] "Second annual cost of cyber crime study," 2011, p. 1.

[5] Ashish Garg, Jeffrey Curtis, and Hilary Halper, "The financial impact of IT security breaches: What do investors think?", Information Systems Security, March/April 2002, pp. 22-33. Available online at http://www.auerbach-publications.com/dynamic_data/2466_1358_cost.pdf.

[6] "2011 data breach investigations report: A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit," Verizon, 2011. Available online at http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

[7] "CF Disclosure Guidance: Topic No. 2 – Cybersecurity," U.S. Securities and Exchange Commission, October 13, 2011. Available online at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[8] "Caution: Malware ahead: An analysis of emerging risks in automotive system security," McAfee, Inc., 2011. Available online at http://www.mcafee.com/us/resources/reports/rp-caution-malware-ahead.pdf.

[9] Tony Bradley, "Mobile devices are new frontier for malware," PCWorld.com, February 8, 2011. Available online at http://www.pcworld.com/businesscenter/article/218983/mobile_devices_are_new_frontier_for_malware.html.

Esta es una traducción al español de la versión oficial en inglés de **Risk Intelligent governance in the age of cyber threats – What you don't know could hurt you,** publicado por Deloitte Development 2012**–** Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.