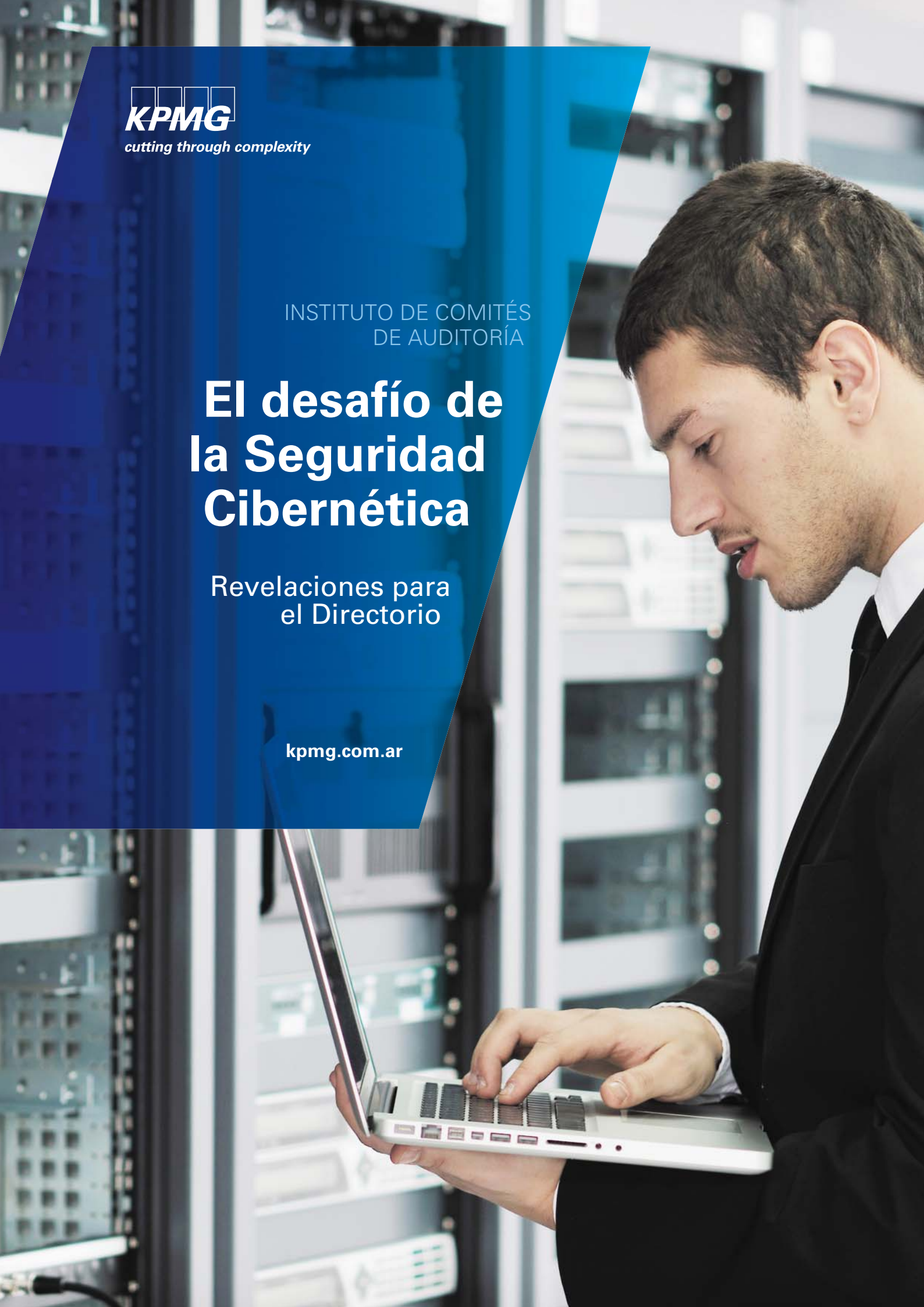
KPMG
cutting through complexity

INSTITUTO DE COMITÉS
DE AUDITORÍA

El desafío de la Seguridad Cibernética

Revelaciones para el Directorio

kpmg.com.ar



Índice

Prólogo

> Como muchas compañías y organizaciones están reconociendo - y experimentando de primera mano - los ataques cibernéticos ya no son una cuestión de si ocurrirán, sino de cuándo.

Los recientes ataques cibernéticos a grandes corporaciones ponen de relieve la creciente sofisticación, el sigilo, y la persistencia de estos ataques que las organizaciones se enfrentan hoy en día, provengan del mismo Estado, del crimen organizado y de hacktivistas, así como las amenazas de dentro de la organización (que a menudo plantean el mayor riesgo).

El reto fundamental de la protección de los sistemas y otros activos informáticos – como la información financiera, los datos de clientes, la propiedad intelectual - y las implicancias para la reputación y el cumplimiento regulatorio por no hacerlo hacen subir las apuestas sobre la seguridad cibernética y la gobernabilidad. Los inversores y los reguladores están cada vez más desafiantes hacia el Directorio para que intensifique su supervisión de la seguridad cibernética y piden una mayor transparencia en torno a los principales incidentes cibernéticos y su impacto en el negocio.

Como era de esperar, el riesgo cibernético está subiendo rápidamente en la agenda del Comité de Auditoría. De acuerdo con la Encuesta Global 2014 del Comité de Auditoría de KPMG casi el 40 por ciento de los comités de auditoría tienen la responsabilidad de supervisión primaria de los riesgos de seguridad cibernética y el 45 por ciento cree que el Comité de Auditoría (o el Directorio) no dedican tiempo suficiente a la seguridad cibernética.

En esta edición del "Global Boardroom Insights " de KPMG, se plantea una inmersión profunda en este tema, la exploración de los elementos clave de la supervisión eficaz del riesgo cibernético y la gobernanza - desde la comprensión de las vulnerabilidades clave hasta la integración de la seguridad cibernética en el programa general de gestión de riesgos de la organización, para asegurar una comunicación efectiva y la presentación de informes del CIO (o función equivalente) y tener implementado un robusto plan de respuesta a incidentes cibernéticos.

Nuestro sincero agradecimiento a aquellos que compartieron su tiempo y conocimientos con nosotros - Sir Jonathan Evans, Jeffrey Keisling, Brian Stevenson, Richard Doern, Sridar Iyengar y Jan Zegering Hadders.

Timothy Copnell
Audit Committee Institute
KPMG in the U.K.

Dennis T. Whalen
Audit Committee Institute
KPMG in the U.S.

Wim Vandecruys
Audit Committee Institute
KPMG in Belgium

Sidney Ito
Audit Committee Institute
KPMG in Brazil

Mritunjay Kapur
Audit Committee Institute
KPMG in India

SIR JONATHAN EVANS

HSBC AND NATIONAL CRIME AGENCY
(REINO UNIDO)

Sir Jonathan Evans es un director independiente no ejecutivo de HSBC Holdings Plc, donde es miembro del Comité para Vulnerabilidades del Sistema Financiero. Él es también un director no ejecutivo de la Agencia Nacional para la Delincuencia. Sir Jonathan pasó 33 años en el Servicio de Seguridad del Reino Unido, seis como Director General. Su experiencia incluye el contraespionaje, protección de la información clasificada y la seguridad de la infraestructura nacional crítica. Su principal objetivo era la lucha contra el terrorismo, tanto internacional como nacional, incluyendo iniciativas contra las amenazas cibernéticas. Como Director General era un asesor del gobierno del Reino Unido sobre la política de seguridad nacional y asistió al Consejo de Seguridad Nacional.

> “Una buena seguridad cibernética no se trata sólo de tener un muro muy fuerte en el exterior, sino también acerca de tener dentro algún tipo de sistema inmune.”

ENTREVISTA

ACI: ¿Qué tan importante es la seguridad informática para los negocios hoy en día?

Sir Jonathan Evans: Creo que es un tema muy importante, no menor, porque abarca toda una gama de diferentes riesgos - riesgos para las empresas y los riesgos para los gobiernos - y hay una amplia gama de amenazas en juego. Estos van desde algo de bajo nivel/mucho volumen hasta el crimen de delincuencia más sofisticada, con "actores" establecidos, algunos de los cuales están atacando tanto a empresas comerciales como a los gobiernos. Y luego están los que no quieren robar información en absoluto, sino potencialmente deshabilitar las capacidades de las empresas o los gobiernos. Hoy en día casi todos los negocios dependen críticamente de sus capacidades de TI y son potencialmente vulnerables a los ataques, ya sea porque la gente quiere controlar la información o porque quieren corromper la información o porque quieren destruir la capacidad de la empresa para acceder a la información.

ACI: ¿Qué tan alto, es lo que piensa, está este tema en la agenda de negocios?

Sir Jonathan Evans: Creo que ha habido un cambio significativo en los últimos tres o cuatro años. Antes era visto como un problema del CIO o la "gente de TI", pero ahora hay un creciente reconocimiento de que esto es algo que tiene implicancias en toda la empresa.

El actual gobierno ha dado prioridad a las cuestiones de seguridad cibernética y que era algo que en mi trabajo anterior, yo estuve involucrado en ayudar a ponerlo en práctica. Creo que los casos de alto perfil que han afectado a algunas empresas - vinculadas con este creciente enfoque del gobierno- ha aumentado considerablemente la conciencia de muchas empresas, pero sigue siendo desigual. Hablando con colegas y gente de la industria, todavía hay una sensación de que está más alto en el orden del día en los Estados Unidos que en el Reino Unido; pero igualmente es probable que esté más alto en el orden del día en el Reino Unido que en algunas otras partes de Europa o de otras partes del mundo. Así que creo que hay un margen pero los niveles generales de interés están subiendo.

ACI: ¿Quién tiene la responsabilidad de la seguridad cibernética dentro de una organización?

Sir Jonathan Evans: Creo que hay que considerar esto como un riesgo para todo el negocio y desde ese punto de vista tiene que ser un tema de la agenda del Directorio. Eso no quiere decir que el Directorio se encuentre en una posición de tomar decisiones técnicas sobre cómo proteger el negocio, pero que el Directorio debe estar seguro de que conoce cuales son sus activos de información críticos y que entiende cuales son los riesgos para estos activos y el potencial impacto en el negocio. A continuación, hay que considerar el apetito de riesgo – esto es en gran medida un tema de Directorio - y asegurarse de que en el nivel ejecutivo se han implementados planes de gestión de riesgos y que esos planes están operando eficazmente. Comprender el riesgo para el negocio es muy importante y no se debe simplemente delegar en el CIO o en la gente de TI - o para el caso, al comité de auditoría.

ACI: Sin perjuicio de los conocimientos técnicos dentro de, por ejemplo, la función de TI, ¿cree que los Directorios tienen suficiente conocimiento en esta área?

Sir Jonathan Evans: Creo que esto depende de la empresa. Hay empresas en las que la seguridad cibernética es un tema tan central que es prudente tener a alguien con experiencia real en el Directorio; en otras empresas, el Directorio podría ser satisfecho con saber que existe apropiada experiencia disponible dentro de la empresa. No necesariamente tiene que ser un miembro del Directorio en todos los casos, pero el Directorio tiene el deber de garantizar que el riesgo está adecuadamente identificado y tener acceso a las personas que pueden garantizar el nivel de protección adecuado. Algo de eso puede haber en casa, o se puede contratar, pero una vez más creo que eso depende de la escala y la naturaleza de la empresa. Habrá pequeñas empresas donde no es razonable asignar una persona a tiempo completo en la seguridad cibernética, pero en las empresas donde es un gran riesgo podría haber un número significativo de personal involucrado. La responsabilidad del Directorio es asegurarse de que el riesgo ha sido adecuadamente evaluado y que se está gestionando adecuadamente.

ACI: ¿Crees que hay algunos retos específicos para los Directorios y comités de auditoría en hacer eso?

Sir Jonathan Evans: Hay una serie de desafíos en esta área. La primera es que los "actores" que generan el riesgo están, evidentemente, encubiertos y tratan de cubrir sus huellas. Eso significa que la comprensión de la naturaleza exacta de los riesgos puede ser compleja y una inteligencia confiable puede ser difícil de obtener. La segunda es que los aspectos técnicos de la misma pueden ser muy complejo y cuando más grande y más interconectado es su sistema informático, hay más probabilidades de que existan más vulnerabilidades en él. Entender esas vulnerabilidades puede ser bastante difícil.

Además, está claro que el mercado de la experiencia en seguridad cibernética es bastante estrecho en este momento. Hay más demanda que personas que realmente saben lo que están haciendo y, por lo tanto, asegurarse de que se tiene la calidad y el número adecuado de personal puede ser difícil. Hay una serie de iniciativas en curso para tratar de aumentar la oferta, pero sin embargo, actualmente, la demanda está superando a la oferta.

Otra cuestión es que esto no es sólo algo que puede ser abordado en el aspecto técnico. Tiene implicancias para el comportamiento del personal en toda la organización, ya que sigue siendo el caso de que muchos de los ataques cibernéticos exitosos contra los negocios, como contra el gobierno, son como consecuencia de la "pesca por ingeniería social" - ataques adaptados específicamente contra las personas que se han diseñado para atraer socialmente a la víctima. Todo el personal necesita un cierto grado de formación y comprensión acerca de cómo combatir estos riesgos. Esto es difícil y cuanto más grande es la organización más difícil se vuelve.

ACI: Los atacantes presuntamente se centran en el eslabón más débil - ¿Esto debe ser un gran problema para las grandes organizaciones multinacionales?

Sir Jonathan Evans: Hay dos cosas a considerar. La primera es que las empresas que aún sienten que sus propios sistemas están bien protegidos están expuestos cuando enlazan sus sistemas a otra empresa - tal vez como resultado de una adquisición o fusión. Hay que pensar bien en cómo se puede mantener el nivel de seguridad deseado. Además, los atacantes cibernéticos están siempre en busca de la vulnerabilidad. Así como mejora la conciencia y las defensas cibernéticas, lo mismo ocurre con la sofisticación de los ataques. Eso tiene que ser entendido - el riesgo nunca se detiene.

Creo que hay una cuestión más amplia aquí en torno a la filosofía de protección dentro de una organización. El modelo tradicional de la seguridad cibernética ha sido un poco como un castillo - si usted tiene un conjunto bastante grande de murallas y fosos alrededor, se puede evitar que los chicos malos se suban. Pero, yo creo que hay que asumir que en algún momento los chicos malos van a entrar y, por tanto, hay que pensar en dos cosas - ¿cómo identificar la actividad dentro de sus redes y cómo se va a responder?. En caso de que usted sea una víctima de este tipo de ataques, entonces usted necesita planes de contingencia. Al igual que con otras áreas de seguridad, hay una variedad de elementos a considerar. Usted tiene el elemento de protección; usted tiene que tener la inteligencia de lo que las otras personas están tratando de hacerle; y tiene que ser capaz de gestionar la respuesta cuando se convierte en una víctima. Si todos estos elementos trabajan juntos, entonces usted puede tener mucha más confianza de ser capaz de resistir un ataque. Por lo tanto, una buena seguridad cibernética no se trata sólo de tener un muro muy fuerte en el exterior, sino de también de tener dentro un sistema inmune y, además, tener la capacidad de recuperarse rápidamente.

ACI: Eso nos lleva al costo real en los negocios de los delitos cibernéticos. ¿O sea no sólo se trata del dinero robado, sino también hay daño a la reputación y la intervención reguladora?

Sir Jonathan Evans: Hay tipos de ataques cibernéticos que tienen simplemente razones dinerarias y creo que la gente está razonablemente familiarizada con ellos. La cantidad de dinero que se pierde en la banca en línea, por ejemplo, es significativa pero es sostenible - y hay un proceso continuo de intensificación por parte de los delincuentes y por parte de aquellos que se protegen contra la criminalidad. La dificultad mayor es el daño a la reputación asociada con la pérdida de datos de clientes en un ataque - que puede ser tan importante como la pérdida financiera y el debilitamiento de la confianza. La gente comprensiblemente espera que las grandes empresas sean capaces de satisfacer sus necesidades 24/7 y si sus sistemas son tomados a causa de un ataque, entonces se puede afectar a la credibilidad que tienen sus clientes. También puede afectar al precio de la acción y el valor de la empresa, por lo que es un problema importante más allá de las pérdidas financieras directas derivadas del fraude criminal.

ACI: Los bancos a menudo compensan a los clientes por las pérdidas de la delincuencia cibernética - ¿significa esto que la delincuencia cibernética no se percibe como un gran problema por los clientes y el público en general?

Sir Jonathan Evans: Bueno, creo que la gente es consciente de ello y conozco a personas que dicen que no van a hacer uso de la banca en línea. Por otro lado, el enfoque general adoptado por el sector bancario minorista del Reino Unido es que las pérdidas no lleguen al cliente. Es interesante que no es el caso en todas las jurisdicciones. Hay lugares que están más propensos a que las pérdidas sean afrontadas por el cliente y que por eso pueden tener un impacto en el comportamiento del cliente. No obstante, en el Reino Unido, no lo afrontan los individuos y por lo tanto pueden estar razonablemente seguros en el uso de los sistemas, que es donde se concentra gran parte de la protección de la seguridad cibernética. Creo que los grandes temas de reputación derivan de las pérdidas de datos importantes y del potencial sabotaje de los sistemas a una gran escala. Estos son mucho menos frecuentes, pero potencialmente más catastrófico si se producen y que, por supuesto, no es algo que está, en ningún sentido, restringido a la industria de servicios financieros.

ACI: ¿Hasta qué punto la tecnología es un problema? En un mundo donde los ciberdelincuentes tienen lo último en equipos y, a veces más poder de cómputo que las organizaciones que están atacando, ¿Crea la nueva tecnología una ventaja comercial?

Sir Jonathan Evans: Pues claro que hay ventajas en la construcción de sus sistemas teniendo en mente a la actual seguridad cibernética. La mejora de la seguridad es más que un reto, pero creo que no se trata de un tema específico de la banca. Es inevitable que si usted tiene una serie de sistemas heredados, estos no habrán sido construidos considerando a la seguridad como un tema clave. Pero, también depende de los atacantes. Existe la impresión de que los criminales cibernéticos son altamente sofisticados, con grandes cantidades de recursos a su disposición y, si bien esto es cierto para algunos de ellos, pero para muchos de ellos no lo es. Hay ciertos sitios web por ahí que ofrecen la capacidad cibernética de un ataque de una sola vez o durante un período más largo - es un mercado bastante sofisticado y no todas las personas que están detrás de los ataques son necesariamente muy técnicos ellos mismos. Es un modelo poco común por lo que es importante disponer, en la medida que se pueda, una comprensión de la naturaleza de esta amenaza. Si usted está preocupado acerca de un ataque importante sofisticado hacia su infraestructura, entonces, evidentemente, debería tener un alto nivel de atención, pero si usted está preocupado acerca de la pequeña escala de fraude de gran volumen, entonces eso es diferente. La mayoría de las empresas pequeñas no están propensas a ser víctimas de un ataque sofisticado, pero habrá empresas que sí; y es por eso que tener su evaluación de riesgos adecuada es tan importante. Usted necesidad poner los recursos que tiene disponibles en los lugares adecuados para las circunstancias particulares - y hacer que eso suceda es parte de la responsabilidad del Directorio.

ACI: Y en estos días que también tienes los así llamados disruptores, que no están robando información o cualquier otra cosa, sino que, por sus pasiones personales, se ocupan de denegar el servicio a una organización. ¿Este debe ser un riesgo difícil de gestionar?

Sir Jonathan Evans: La amenaza de activistas cibernéticos debe tenerse en cuenta. Puede ser algo con intención puramente publicitaria si se puede hackear su sitio web público y poner sus consignas a través de él - que es una muy buena forma de llamar la atención hacia sus asuntos particulares. O puede ser que sean los hackers más malignos que quieran montar un ataque de denegación de servicio con el fin de defender su postura; una vez más, esto dependerá de la industria que se encuentre, pero es sin duda uno de los diversos aspectos de la seguridad cibernética que necesitan ser considerados.

ACI: ¿En qué medida las organizaciones comerciales comparten información acerca de los ataques que están teniendo? ¿Los gobiernos comparten este tipo de información con el mundo empresarial?

Sir Jonathan Evans: Bueno, eso fue sin duda uno de los objetivos clave de la estrategia de seguridad cibernética del gobierno, que se esbozó hace dos o tres años. Desde mi punto de vista, la seguridad cibernética no debería ser un problema de competencia entre las empresas y la existencia de mecanismos bien establecidos para el intercambio de información sobre una variedad de temas de seguridad, sobre todo para aquellas empresas que forman parte de la infraestructura nacional crítica.

El otro aspecto es el grado de que el gobierno sea capaz de compartir. Hay una serie de modelos que se están desarrollando y creo que se están moviendo en la dirección correcta. No es sencillo porque parte de la información que el gobierno gestiona es muy sensible y no puede ser ampliamente compartida sin perder su valor. Creo que habrá un período de experimentación para encontrar la mejor manera de hacer esto y luego, por supuesto, las medidas de fomento de la confianza se vuelven importantes; pero creo que hay una clara determinación por parte del gobierno para compartir todo lo que puedan, porque la seguridad nacional no abarca solo al gobierno.

Con esto quiero decir que la seguridad de un país depende no sólo de que su gobierno sea seguro, sino también los servicios públicos, los servicios financieros y otros, muchos de los cuales se entregan a través del sector privado. Así que hay un interés de seguridad nacional del gobierno para compartir y, por tanto, el gobierno está centrado en el equilibrio de los ideales de la protección respecto del compartir información.

ACI: ¿Tiene algún consejo o consejos para los comités de auditoría o los directores? - ¿Cuáles son las dos primeras cosas en que pensar?

Sir Jonathan Evans: Creo que lo primero, y en cierto modo lo más difícil, es el de identificar los activos de información críticos. Las empresas no siempre son buenos para pensar acerca de su información como un activo y, por tanto, reconocer cuál es su valor. Todo el mundo entiende el valor de su dinero, y se preocupan por eso; por lo que la información tiene un valor y debe ser pensada de una manera similar.

La segunda es que, para la mayoría de las empresas, la seguridad cibernética abarca la defensa en profundidad y una variedad de enfoques diferentes. No hay balas de plata.

JEFFREY E. KEISLING
PFIZER (EE.UU.)

Jeff Keisling es Vicepresidente Senior y Director de Información de Pfizer, con la responsabilidad de la estrategia de tecnología de la información de la compañía, incluyendo los sistemas de negocio de la empresa y los servicios compartidos globales de TI. Antes de unirse a Pfizer en 2009, fue Vicepresidente de Servicios de Información Corporativos y Jefe de Información de Wyeth Pharmaceuticals (que fue adquirida por Pfizer). El Sr. Keisling también ha servido como el CIO de Advanta Financial Services y Rhône-Poulenc Rorer Pharmaceuticals, y ha dirigido a los equipos de desarrollo de los sistemas de negocio de Knoll International. Es miembro de la junta directiva de la Asociación Farmacéutica de Servicios de Información, el Consejo de Investigación de la Junta Asesora de IBM, CIO Strategy Exchange, y el Consejo Asesor Microsoft.

> “El Comité de Auditoría quiere que demostremos que estamos patinando hacia donde va la pelota, en lugar de donde está ahora.”

ENTREVISTA

ACI: ¿Cuáles son los desafíos de la seguridad cibernética en Pfizer, y considerando las recientes series de incidentes cibernéticos publicados en los titulares, se ha elevado el tema en la empresa y en el Directorio?

Jeff Keisling: La seguridad cibernética ha estado en el ADN de nuestro programa de gestión de riesgo empresarial (ERM) desde hace algún tiempo. No es visto como un único programa o proceso, sino como un riesgo permanente que está integrado con nuestro programa de ERM. Como los incidentes y ataques se han vuelto más sofisticados, las amenazas cibernéticas sin duda han subido en nuestra estratificación de riesgos de la empresa.

Creo que lo que hemos hecho particularmente de manera efectiva es la inclusión de la seguridad cibernética en nuestras principales actividades de gobierno corporativo - en la alta dirección y en el Directorio – e integrado en el marco ERM de manera multidisciplinaria.

ACI: ¿Puede explicarnos este aspecto multidisciplinario? ¿Quiénes están en la mesa con usted para tratar las cuestiones de seguridad cibernética?

Jeff Keisling: Se trata de un proceso impulsado por los negocios. Recibimos aportes de nuestros socios de negocios en las distintas áreas: comercial, I + D, abastecimientos, médicos y finanzas, que identifican y estratifican el riesgo. Hace años que formamos un consejo de seguridad de la información para ayudar a abordar estos riesgos definidos, que reúne diferentes perspectivas sobre la seguridad global, incluyendo representantes de nuestros equipos de legales y de cumplimiento, recursos humanos, auditoría interna, comunicaciones y tecnología. El consejo es donde el ciclo de gobernanza en torno a la seguridad cibernética comienza – las políticas, los programas educativos, la concientización, la vigilancia constante y recordatorios. A partir de ahí, se expande hacia el marco amplio de gobernabilidad de la empresa.

ACI: ¿Qué papel desempeña la auditoría interna?

Jeff Keisling: La auditoría interna es nuestro socio. Trabajamos en estrecha colaboración con el equipo de auditoría en todas las facetas de TI, ya sea la seguridad cibernética o la forma en que se rigen los programas en general.

El equipo de auditoría ofrece su experiencia en políticas. Por ejemplo, cuando hacemos una actualización de nuestra política de respuesta a incidentes cibernéticos, la auditoría interna está en la mesa cuando afinamos la estrategia y la política, y la incorporamos en el programa de ERM.

La auditoría también ha agudizado su enfoque en el riesgo cibernético ya que ha crecido en la escala de riesgo, y ayuda a desarrollar la agenda de gobierno de TI en toda la empresa y con nuestro comité de auditoría. También trabajan con nosotros de una manera muy directa y de colaboración cuando estamos investigando los incidentes o problemas cibernéticos específicos. La auditoría es un socio de gran valor ya que aportan una perspectiva independiente y equilibrada a la mesa.

ACI: ¿Cómo ayudan al Directorio a sentirse cómodo acerca de que la empresa tiene bajo control al riesgo cibernético? ¿Cómo está comunicandose con los directores acerca de los riesgos y la seguridad cibernética, y que información es la que encuentran más útil?

Jeff Keisling: El Directorio quiere comprender la estructura de gobernanza y nuestro sistema de gestión de riesgos de seguridad, y cómo se integra en el programa de ERM general de la compañía. La comprensión de la estrategia de riesgo cibernético es clave.

El Directorio también quiere entender cuáles son las mayores amenazas y riesgos para los activos de mayor valor de la compañía. Ellos quieren ver cómo el capital humano y el capital financiero están alineados para manejar las mayores amenazas que enfrentamos.

Nuestro comité de auditoría está especialmente dedicado a la revisión del desempeño de nuestros procesos y protecciones. Un tablero de control de la seguridad cibernética se revisa de manera rutinaria durante nuestras reuniones, que abordan nuestras principales áreas de riesgo, incidentes, tendencias, y una visión de lo que está sucediendo en el entorno externo.

Por último, quieren que demostremos que estamos patinando hacia donde va la pelota, en lugar de donde está ahora. Es bien sabido que nuestros esfuerzos de seguridad cibernética es ir mejorando continuamente para añadir capacidades que protegen a nuestra empresa de los cambios en las amenazas y los riesgos.

Hemos encontrado que aquellos elementos - discutidos de manera abierta y franca - ayudan a crear un alto nivel de transparencia y confianza, y el diálogo que obtenemos a cambio es extremadamente valioso.

ACI: ¿Puede hablar un poco más acerca del tablero de control que utilizan?

Jeff Keisling: Revisamos con el comité de auditoría el tablero de control que contiene cuatro grandes áreas de riesgos y tendencias clave. Esto incluye el volumen de incidentes y la materialidad de cualquier evento durante el período más reciente y cómo se administran esos eventos. También proporcionamos información y actualizaciones sobre lo que está pasando fuera de la empresa, en el sector privado y público, así como lo que está sucediendo en el frente legislativo.

En general, creo que la madurez de la información de riesgo cibernético y la calidad de nuestro diálogo en la sala de juntas mejora con cada conversación. Los directores traen sus propios puntos de vista de otras compañías - incluyendo de aquellas que tienen perfiles de mayor riesgo, como el sector de servicios financieros. Ha sido un proceso de aprendizaje colectivo con el Directorio, y juntos hemos conseguido el lenguaje, las herramientas y la información afinada hasta obtener un buen diálogo.

ACI: ¿Cómo es su enfoque de la seguridad cibernética - interna y externamente - hacia las tecnologías móviles y el uso de las redes sociales?

Jeff Keisling: con aproximadamente seis mil millones de dispositivos en el mundo actual, las tecnologías móviles y las redes sociales han creado nuevos canales de riesgo y los mayores volúmenes de ataques. En muchos casos, estamos viendo los mismos tipos de amenazas que hemos visto antes, sólo repite y vuelve a intentar con un volumen más alto. Para darle un orden de magnitud, hemos visto un aumento del 400 por ciento aproximadamente en un período de un año.

Aunque todavía vemos técnicas de "phishing" y "spam" clásicos, los ataques crecen en sofisticación de alta gama y posible fraude. Pero tenemos que mantener nuestros ojos en la pelota si se trata de actividades más sofisticadas, patrocinados por el estado o de gama baja. Las redes sociales y las tecnologías móviles, lamentablemente significan más tiros al arco para el equipo contrario - y eso es una gran parte de nuestra conversación cuando se habla de la forma en que estamos usando estas capacidades para avanzar en nuestro negocio y la ciencia.

Los móviles y las redes sociales también aumentan las apuestas sobre el riesgo reputacional. Uno de nuestros cuatro principales imperativos estratégicos es "ganar mayor respeto por parte de la sociedad". Como compañía en el espacio de ciencias de la vida, centrándose en la innovación terapéutica, nada es más importante para nosotros que nuestros clientes y pacientes. Así que nuestra reputación y respeto por parte de la sociedad son las principales prioridades. Tenemos un programa de monitoreo interactivo social muy activo para entender lo que está sucediendo en el mercado en relación con nuestros pacientes y nuestros clientes. Se suma a la cantidad de trabajo y el reto de mantener un ojo en las redes sociales y en el mercado en general, pero es un imperativo para nosotros.

ACI: Estamos viendo más empresas y Directorios que adoptan una actitud de "no si, sino cuándo" se produce un incidente cibernético. ¿Qué cree usted que son los elementos críticos de un buen plan de respuesta a incidentes cibernéticos?

Jeff Keisling: Es un reto el definir un proceso preciso o un conjunto de medidas concretas para la gestión de un incidente cibernético ya que no todos tienen los mismos atributos y consecuencias para la empresa o nuestros clientes. Dicho esto, la gestión de incidentes es un componente crítico de un programa global de riesgo cibernético - y creo que un par de cosas determina qué tan efectivo será esa respuesta.

En primer lugar, la participación temprana, especialmente durante el proceso de planificación, y la participación de los actores clave, con un enfoque multidisciplinario, es crítica. Incluimos nuestros equipos de comunicaciones y de políticas, que están activamente involucrados con la planificación de escenarios. En segundo lugar, es importante establecer una responsabilidad clara - si tenemos una brecha, quien es responsable de hacer qué. A pesar de que no sabemos qué es exactamente el juego que vamos a jugar, en función de los hechos, sabemos quién va a estar en el juego y ellos saben cuál será su papel.

La tercera pieza crítica es la toma de decisiones; sobre todo, si un incidente tiene implicancias externas. Internamente, se trata con la educación de nuestros colegas y ese proceso no cambiará mucho. Pero en los casos en que tengan que ser notificados terceros o clientes, es importante contar con un marco para la toma de esas decisiones - a veces muy rápidamente.

ACI: Un gran porcentaje de los incidentes cibernéticos se atribuyen a las "personas de riesgo" internas – aquellos empleados que no siguen los procedimientos o controles internos – más que a ataques externos de hackers. ¿Cómo deben las empresas y los Directorios estar pensando en el riesgo interno?

Jeff Keisling: Los medios de comunicación tienden a centrarse en los ataques más sensacionales de fuentes externas. Pero seguimos asesorando a la dirección y a los directores que los riesgos internos y riesgos externos son igualmente importantes.

El riesgo interno se presenta en diferentes formas. Una de las cosas que estamos viendo es más intentos de ingeniería social, que son mayormente ataques de baja sofisticación, pero presentan un riesgo, no obstante. En estos casos, un colega se convierte en objetivo por medio de la "huella digital" de su vida privada. El atacante utiliza esta información para crear un nivel de confianza con esa persona, con el objetivo de obtener, por vía social, un acceso a los sistemas o procesos de la empresa.

Además, si tenemos en cuenta que la mayoría de las grandes empresas tienen muchas terceros que realicen un volumen alto o servicios de transacciones altamente controladas - contratistas, proveedores, socios - la pendiente de la curva de complejidad aumenta. Ya sea que se trate de operaciones financieras o el intercambio de información confidencial o de propiedad intelectual, es una buena idea aumentar al doble los recursos dedicados a la protección de los activos de los riesgos de terceros.

ACI: ¿Diría que por ser una compañía global tienen diferentes tipos o niveles altos de riesgo cibernético?

Jeff Keisling: Yo respondo con un sí ensordecedor. Tenemos una presencia física en aproximadamente 175 mercados de todo el mundo, desde los lugares de fabricación y de I + D a una amplia gama de locaciones comerciales. Al combinar nuestra presencia física con la cantidad que gastamos para financiar la I + D cada año, las colaboraciones con las instituciones académicas y los contribuyentes del sistema de salud y otros, y nuestra visibilidad global, usted puede imaginar tenemos una gran cantidad de atención por parte de las personas que buscan penetrar en nuestros sistemas. Viene con el territorio, y me remonto a mi punto anterior acerca de patinar hacia donde va el disco para estar tratando de estar siempre un paso por delante.

Una gran parte de lo que se está comunicando y reforzando continuamente son las políticas de seguridad cibernética de la compañía, los protocolos y las expectativas de nuestra gente alrededor del mundo. Es acerca de herramientas y recordatorios de entrenamiento, es acerca de herramientas de cumplimiento y de gobernanza. Cada empleado recibe capacitación, es probado y vuelto a probar periódicamente sobre el cumplimiento, y se requiere una puntuación del 100 por ciento.

Nuestros colegas son muy conscientes de nuestros estándares y expectativas respecto de la seguridad cibernética; está grabado a fuego en la cultura de la empresa. Es una gran tarea, y en realidad nunca termina. Todo lo que hacemos en seguridad cibernética se incrusta profundamente en el ADN de la compañía y nuestros esfuerzos de gestión de riesgos en toda la empresa.

BRIAN STEVENSON
AGRICULTURAL BANK OF CHINA (REINO UNIDO)

Después de una larga carrera en la banca con Barclays Plc, Deutsche Bank AG y el Royal Bank of Scotland Group Plc, Brian Stevenson es ahora un director no ejecutivo del Banco Agrícola de China (UK) Ltd, donde preside el comité de riesgo y es un miembro del comité de auditoría; y asesor de WorldPay (UK) Ltd, donde es miembro de la comisión de riesgos. Él es también un miembro del Directorio de New Model Identity Ltd y miembro del consejo asesor de Lisis Financial Ltd.

> “Asegurarse de que las defensas cibernéticas están tan actualizadas como los atacantes constituye un gran desafío.”

ENTREVISTA

ACI: ¿Tiene usted alguna experiencia de los ataques cibernéticos?

Brian Stevenson: Tengo una experiencia muy específica de un ataque cibernético - un ataque del crimen organizado en la cual el atacante tenía más potencia informática a su disposición que la empresa atacada. Una de las razones por las que he tomado un interés en la seguridad en línea es porque cuando miré alrededor de la empresa para encontrar a otras personas con la experiencia necesaria, había muy pocos. Eso me llevó a convertirse en el presidente de la comisión de auditoría interna de una división de la sociedad - que tenía experiencia tanto en la ejecución de un medio de pagos (que en cierto modo son los más vulnerables a los ataques del crimen organizado porque es allí donde fluye mayor cantidad de dinero), sino también porque pasé por la experiencia de tener que lidiar con los reguladores, pagar multas y todos esos costos ocultos de la delincuencia cibernética. El hecho de que hubo dinero robado fue casi incidental, debido a que el costo de la remediación fue casi ocho veces a la cantidad robada. El daño a la reputación y la pérdida de dinero es una cosa, pero en una industria regulada, las multas a pagar por no proteger los datos de sus clientes pueden costar mucho dinero.

ACI ¿Qué tan alto en su agenda del Directorio/comité de auditoría está el riesgo cibernético y qué tan alto debe estar?

Brian Stevenson: Qué tan alto debe esta, depende de la empresa en que se encuentra y la vulnerabilidad percibida de su organización a un ataque cibernético. Un modelo de negocio inmune es difícil de imaginar porque la mayoría de las organizaciones dependen de alguna forma de las comunicaciones web y tan pronto como su sistema informático interno está conectado a un sistema informático externo son vulnerables a los ataques. Usted tiene que tomar un enfoque basado en el riesgo. Si usted tiene un montón de dinero para ser robado o know-how o datos de clientes importantes, entonces el riesgo siempre será mayor. Si usted tiene un negocio en el que tiene niveles bajos de datos de los clientes, o bajos niveles de flujos de pago, o no hay secretos comerciales y ese tipo de cosas, entonces el riesgo podría ser relativamente bajo.

Hay cinco tipos diferentes de atacantes según los análisis en los que he participado: los gobiernos, los competidores (espionaje industrial), delincuentes organizados, delincuentes de poca monta y disruptores o ' hactivistas ' . Un buen comité de auditoría pasará a través de estas cinco categorías y evaluará el riesgo en cada caso. Si usted piensa que es vulnerable a las cinco formas de ataque, entonces será una prioridad en su agenda. Se requiere un análisis riguroso dentro de la empresa y el conocimiento suficiente y la educación que aquellos que se sientan alrededor de la mesa en el Comité de auditoría y del Directorio para entender la naturaleza de estos riesgos.

ACI: ¿Cree usted que hay suficiente conocimiento en torno a las mesas del Directorio?

Brian Stevenson: Me gustaría ir un paso atrás y preguntar quién es el responsable de la seguridad cibernética en la organización. ¿Qué miembro del Directorio tiene una preocupación diaria sobre la seguridad cibernética en su plato? Muy pocas organizaciones tienen un director de TI sentado en la mesa del Directorio, a pesar de que la mayoría de las organizaciones dependen críticamente de su infraestructura de TI. Muy a menudo es el director de finanzas, pero los directores de finanzas tienen un montón de otras cosas de qué preocuparse. Puede estar delegada por el director de finanzas en una persona que no se sienta en la mesa del Directorio - ¿Pero esa persona tendrá el apoyo y la representación correcta dentro de la estructura de gobierno? Esta es una especie de análisis crítico que creo las organizaciones tienen que hacer.

ACI: ¿Debería la supervisión de los riesgos de seguridad cibernética ser asignada al comité de auditoría o al comité de riesgos?

Brian Stevenson: El enfoque preferido dentro de la banca es monitorear riesgos a través del comité de riesgos, pero no ignorar el tema a nivel del comité de auditoría. Por lo tanto, el seguimiento detallado se realiza en el comité de riesgos, que incluye conversaciones con la gente de TI. El comité de riesgos tiene que estar convencido de que tenemos respuestas, tenemos políticas en su lugar, tenemos las defensas adecuadas, las defensas están al día, que los ataques conocidos son reportados y cómo se los defendió - incluyendo si nuevas tecnologías nos han atacado.

Los comités de riesgo son relativamente raros fuera del sector financiero, por lo que estos temas caen a menudo en la agenda del comité de auditoría.

ACI: ¿Cuáles son los otros retos más allá de establecer las funciones y responsabilidades adecuadas dentro de la organización?

Brian Stevenson: Hay una pieza educativa para tratar de asegurarse de que las empresas de primera línea entiendan las consecuencias de sus acciones frente a las amenazas informáticas. Por ejemplo, ¿existe un método estandarizado para el desarrollo de sitios web? En un negocio complejo, usted no quiere un vale todo, donde cualquiera puede ir y desarrollar un sitio web público, sin apego con las disposiciones de gobernanza centrales, porque una página web es la puerta de entrada para un criminal a su organización - particularmente si la página web que tiene es un motor de procesamiento de pagos, ya que es exactamente lo que están buscando. Por desgracia, no debe haber libertad en una organización para que cualquiera pueda desarrollar una página web que sea una ruta de acceso interno sin cumplir con todos los estándares más altos posibles de seguridad web. Hoy en día, ¿cuántas organizaciones reportan estadísticas sobre este tipo de eventos a la auditoría o el comité de riesgos y cuántos determinan las vulnerabilidades que tienen en su infraestructura web? Este es el tipo de rigor que se necesita.

En el viejo mundo, nadie esperaba que un banco dejara la caja fuerte abierta, pero básicamente eso es lo que significa tener una seguridad web ineficaz; pero las personas no siempre piensan así.

La auditoría interna debe estar mirando a la política de desarrollo de sitios web - asegurándose de que no sólo no hay una política vigente, sino que la política está en realidad operando eficazmente. Para un banco, que es donde tengo la mayor parte de mi experiencia, tan pronto como usted permite que sus clientes se conecten en línea para hacer un pago se permite a un atacante potencial pasar de la primera línea de defensa a la ingeniería de procesamiento de su organización y eso es lo que les gusta.

ACI: ¿Los equipos de auditoría interna tienen las habilidades para hacer esto?

Brian Stevenson: Generalmente no, pero aquí es donde aplican los acuerdos de tercerización. La mayoría de las grandes firmas de servicios profesionales tienen ahora un conjunto considerable de conocimientos especializados en cuestiones cibernéticas, incluyendo en algunos casos, a los ex-delincuentes reconvertidos que tratan de entrar en los sistemas de los clientes para ver lo vulnerable que son.

ACI: ¿Cuál es la siguiente pista de los retos tecnológicos?

Brian Stevenson: Ciertamente hay retos técnicos - entre otras cosas porque los atacantes cibernéticos pueden estar por delante de la curva en términos de conocimientos técnicos y la capacidad de procesamiento. Una vez dentro del sistema, buscan alrededor el punto más vulnerable a los ataques - y que puede ser una subsidiaria que no se ajusta a los mismos estándares mundiales como el resto del grupo. Por lo tanto, asegurarse de que su departamento de TI interno y sus defensas cibernéticas están tan actualizadas como los atacantes conforman un gran reto.

Creo que una de las áreas que podrían ser mejoradas es la cooperación entre la industria. Por ejemplo, ¿Comparten las empresas información acerca de los ataques que han tenido y la tecnología que utilizan con otros que podrían ser vulnerables? ¿Lo compartirían con sus competidores o los bancos? Luego está la cuestión más grande y más irritante de gobernanza de compartir con el Gobierno - pero podemos guardar este tema para otro día.

ACI: ¿Cree usted que los comités de auditoría en la actualidad tienen las habilidades y conocimientos necesarios que se requieren con el fin de proporcionar una supervisión eficaz? O los comités de riesgo para el caso?

Brian Stevenson: Es muy difícil generalizar, pero como se está verificando un incumplimiento importante, tengo una clara impresión de que los organismos policiales y los reguladores no sienten que el sector bancario en su conjunto tiene esta cuestión en la cima de sus prioridades. La ciberdelincuencia es un fenómeno relativamente nuevo y la mayoría de las personas que se sientan en los comités de auditoría o incluso en los Directorios no han crecido con él. Han crecido con las normas contables y han crecido con las preocupaciones reguladoras y todas esas clases de cosas, pero no han crecido con el conocimiento preciso de cómo los ciberdelincuentes podían atacar o no atacar a su organización. Por lo que su conocimiento no es algo que está en el alma, es algo que han tenido que adquirir. Por el contrario, los ciberdelincuentes han crecido a menudo desde una edad temprana con la intención de ganar dinero, o interrumpir algo o hacer una actividad política por medio de atacar a las tecnologías. La sensación intuitiva es que el sujeto no está en los Directorios y comités de auditoría. Por supuesto, las personas que se sientan en los Directorios y comités de auditoría son perfectamente capaces de aprenderlo - aunque dada lo ocupado de su posición, es poco probable que puedan permanecer en el borde de la curva.

ACI: Esto es interesante, porque una de las grandes ventajas de los directores no ejecutivos es que traen la sabiduría y la experiencia adicional al Directorio- ¿pero tal vez no en este caso?

Brian Stevenson: A menos que tengan una persona canosa como yo que ha pasado por un ataque cibernético, necesitas personas mucho más jóvenes que probablemente han crecido en la industria de TI. Es posible que tengan poco conocimiento de la banca, por ejemplo, pero tendrían grandes preguntas que hacer como miembro del comité de auditoría sobre el nivel de conciencia cibernética dentro de las defensas de seguridad empresarial, seguridad informática, defensas cibernéticas y todas esas cosas. Para las empresas, donde el uso de la tecnología está muy alto en el registro de riesgos, los miembros del Directorio tradicionales podrían ser apoyados por nuevos funcionarios con conocimientos especializados. Hay algunos muy buenos ejemplos de esto en la banca.

ACI: ¿Está la cuestión cibernética como prioridad en la agenda como debe ser?

Brian Stevenson: Creo que no es tan importante en la agenda de la gente, como podría ser debido a que los consumidores no se preocupan demasiado por ello. Hay varias encuestas realizadas que muestran que, incluso en cosas como el robo de identidad, la mayoría de las personas no se preocupan por él tanto como deberían. Creo que parte del problema es que si usted sufre algún tipo de pérdida de datos o robo de identidad, la organización que ha sido vulnerable a ese ataque (es decir, cuando su información ha sido robada a) la banca se hace cargo. Como individuo, muy rara vez sufre una pérdida financiera y por lo tanto la actitud del público en general, parece ser uno de "no es mi problema". Podría causar alterar un poco mi vida, pero no me va a costar dinero.

Otro factor que contribuye es la cuestión de transparencia. No se informa bien lo mucho que el crimen cibernético le cuesta a los negocios. El gobierno ha estimado una cifra de, creo, 27 mil millones - pero no tengo ni idea cómo llegaron a ese número. Las pérdidas cibernéticas no son sólo la pérdida real de dinero, sino también el costo de la pérdida de datos, las multas y la reputación que afecta las oportunidades futuras. Y no siempre es claro si una organización ha sufrido una pérdida - por lo menos no inmediatamente claro. Por ejemplo, la propiedad intelectual podría ser robada y la empresa recién toma nota del robo cuando un producto rival de repente aparece en el mercado.

Esto me regresa al tema del diseño de los sistemas de TI. Es que, con los sistemas antiguos, los delincuentes pueden entrar en el sistema, robar información y se van otra vez, y no hay forma de saber que han estado allí y se han ido. Con las nuevas tecnologías no ocurre - ya que como parte de su defensa cibernética es fundamental mantener su tecnología al día y que sea capaz de recoger pistas de los ataques. Si los riesgos fueron correctamente evaluados, entonces usted necesita tener la información correcta y eso significa que necesita sistemas de TI que sean adecuados a sus objetivos.

En el ataque cibernético que viví, entraron en los sistemas y se fueron, y no sabíamos que habían estado y se habían ido. Sólo nos enteramos cuando la contabilidad tradicional mostró una falta de correlación entre el dinero que los clientes habían retirado y el dinero real que se había retirado. Estuvo muy bien organizado - extrajeron dinero de los cajeros automáticos en muchos países de todo el mundo al mismo tiempo.

ACI: Es de suponer que el diseño de los sistemas informáticos es, en gran medida, reactiva. ¿Es fácil de mantenerse en la cresta de la ola de los riesgos emergentes?

Brian Stevenson: La única manera de que realmente se puede mantener en la cresta de los riesgos emergentes es monitorear lo que los criminales están escribiendo. Hay un montón de "sitios oscuros" en el Internet donde los criminales intercambian información. Usted necesita saber lo que está pasando y, hasta cierto punto usted es dependiente de que los organismos encargados de hacer cumplir la ley comparten información sobre las amenazas emergentes con la comunidad empresarial. Esto puede que no se discuta en un comité de auditoría o de riesgo, pero usted puede tener un sub-comité en el que sólo las personas clave puedan compartir información que han recibido de la policía, o de los gobiernos y así sucesivamente.

ACI: Así que es importante el flujo de información desde las agencias estatales a las empresas; pero ¿qué hay acerca de que las empresas divulguen información sobre el delito cibernético con los inversores?

Brian Stevenson: Es cuestión de equilibrio. Como banco, usted que tiene que decirle el regulador inmediatamente que usted ha descubierto algo. Siempre hay un flujo de información al regulador y luego se entra en un período de cooperación con el regulador para ayudar a resolver el problema. Esperamos así que el regulador no lo multe por ello - pero a menudo lo hacen.

Las multas son normalmente mayores, cuando los datos del cliente han sido revelados a terceros y está circulando en la web. Los costos de remediación pueden a menudo mucho mayores que las mismas multas, ya que hay que remediar a cada cliente. Esto no es sólo un problema de la banca. Usted es vulnerable si es (por ejemplo) una empresa de servicios públicos y tiene los detalles de la tarjeta de crédito de los pagadores de sus facturas.

El patrón actual parece ser revelar que usted ha sido atacado pero comunicarlo de tres a seis meses después de sucedido. Esto no es irrazonable, ya que lleva a un buen montón de tiempo trabajar en la gravedad de la crisis, y evaluar la magnitud de los daños y las pérdidas contingentes relacionados con ella.

Si se declara demasiado pronto, los inversores le harán un montón de preguntas que usted no será capaz de responder y luego ellos llegarán a la conclusión de que usted no sabe lo que está haciendo. Tiene que haber un período de tiempo para recopilar toda la información, para comprender sus vulnerabilidades y de manera crucial para rectificar sus debilidades. Si usted divulga antes de haber arreglado sus vulnerabilidades en efecto estás abriendo la puerta a todo el mundo de la delincuencia. Es un equilibrio delicado, pero creo que una de las maneras de lidiar con este tema es el aplazamiento en el tiempo.

ACI: ¿Alguna otra idea para los comités de auditoría?

Brian Stevenson: Yo creo que ha habido algunos avances en los últimos años y los riesgos asociados a la tecnología se están arrastrando en la agenda. Sin embargo, hay un largo camino por recorrer. El beneficio de contar con una organización orientada a la web se vendió a los Directorios hace mucho tiempo; pero sin duda el riesgo a la baja no se conocía en ese momento. No fue hasta que los atacantes consiguieron organizarse mejor y comenzaron explotando el hecho de que ahora tienen una ventana electrónica hacia su back office qué los Directorios se han despertado y ven el riesgo. Y yo todavía no creo que lo ven con claridad suficiente. En un mundo tan competitivo hay una gran tentación de aprovechar las oportunidades que ofrecen las tecnologías basadas en la web y sin prestar la debida atención a las amenazas. La amenaza tiene que ser manejada; tiene que ser gestionada a través de su infraestructura.

ACI: Así que, de nuevo se reduce a la comprensión de los riesgos involucrados y si los sistemas para la gestión de esos riesgos son adecuados a los objetivos y operan según lo previsto.

Brian Stevenson: En el pasado, he pasado una semana sentado en las mesas de la unidad de delitos cibernéticos de la función de TI para ver lo que estaban haciendo. Si tiene mi edad puede no tener la menor idea acerca de la actividad en la web oscura, y no tiene ni idea de cuál es la capacidad de la tecnología y no tiene ni idea acerca de cómo las personas pueden explotar las deficiencias y lagunas en la tecnología. Es que, no es un mundo en el que he crecido. Por lo tanto, es como aprender otro idioma; hay que sumergirse en el tema para ser bueno en ello. E incluso, así y todo, usted todavía necesita la ayuda de los especialistas.

ACI: Ese es un punto muy bueno. A menudo hablamos de los comités de auditoría patean los neumáticos de la empresa, pero creo que pocos de nosotros realmente lo ha hecho en materia de tecnología.

Brian Stevenson: Esto nos lleva al punto de partida. La tecnología forma una gran parte del mundo de los negocios modernos. Si usted es un banco, una cadena minorista o una distribuidora eléctrica, tiene el riesgo de sufrir alguno de los cinco diferentes tipos de agresiones cibernéticas. Para algunos, el perfil de riesgo será mayor que el de los demás; pero es difícil pensar en cualquier organización que no sería vulnerable a por lo menos algún tipo de ataque.

RICHARD DOERN
GRUPO STEFANI (BRASIL)

Richard Doern tiene más de 25 años de experiencia en liderar procesos de transformación organizacional en más de 75 empresas, de todos los tamaños y segmentos de mercado, tanto en Brasil como en el extranjero. Como director certificado por IBGC, el Sr. Doern ha servido como presidente y coordinador de comités de auditoría, de estrategia y de gobernanza. Actualmente, es miembro del Directorio y coordinador del Comité de Auditoría de Grupo Stefani (transporte y logística), miembro del Directorio y coordinador del Comité de Estrategia de Grupo Tiradentes (grupo de las universidades de lucro) y miembro del Directorio en Kinoplex (cadena de salas de cine). Se especializa en la recuperación empresarial (gestión de respuesta), siendo uno de los precursores en el país para actuar como CEO interino durante las fases críticas de la reestructuración.

> “La educación continua para todos los miembros del Directorio es esencial para mantenerse al día sobre la seguridad cibernética.”

ENTREVISTA

ACI: ¿Cuál es la mentalidad que los Directorios deben tener hoy sobre el entorno de riesgo cibernético?

Richard Doern: El aumento del acceso a la tecnología por parte de los empleados resulta en una mayor vulnerabilidad para las empresas y el uso inadecuado de las aplicaciones, plataformas y dispositivos móviles puede poner la información clasificada e importante en riesgo. Yo creo que los directores deben ser más conscientes de la importancia de incluir este tema en la agenda del Directorio. Este tema aún no es considerado como estratégico o relevante por la mayoría de los directores. La inmensa mayoría de los temas a tratar, la escasa cantidad de tiempo para las reuniones y, en especial, la falta de conocimiento profundo sobre este tema por los directores da como resultado que los problemas cibernéticos sean restringidos al área de IT y sus profesionales.

Otra cuestión importante que los directores deben ponderar es la alta rotación de los empleados. Además de la dificultad de mantener los procedimientos operativos, este factor aumenta el riesgo debido a la información clasificada se puede mover de una compañía a otra.

ACI : ¿Cuáles son los 3 o 4 mensajes clave que los CIOs deben comunicar regularmente al Directorio?

Richard Doern: Una consideración muy importante es que el perfil deseado de los CIO está cambiando. Hace años, el papel del departamento de TI estaba más restringido al back-office, infraestructura y apoyo, pero debido a la actual etapa de un amplio acceso a la tecnología y la relevancia de este tema para los negocios, TI tiene que desempeñar un papel más estratégico y de gestión de riesgos. Los profesionales de TI de hoy en día necesitan obtener el conocimiento sobre los procesos de negocio y la innovación para ser capaz de prever situaciones y proponer soluciones avanzadas, en lugar de actuar sólo de manera reactiva.

En este sentido, el principal mensaje que los CIO deben comunicar tiene que estar relacionado con la innovación, las nuevas aplicaciones y tecnologías que proporcionan productividad, habiendo ya evaluado y mitigado los respectivos riesgos. Teniendo en cuenta que los miembros del Directorio y del comité de auditoría a menudo no tienen un conocimiento profundo de la materia, la participación de los profesionales de TI en el mapeo de los riesgos y en la definición de medidas de mitigación se convierte en esencial.

ACI: ¿Cómo deben los CIOs estar comunicándose con el comité de auditoría / Directorio sobre la seguridad informática?

Richard Doern: Además de los informes periódicos simples y breves - que podrían tener frecuencia mensual o bimestral – hay que informar sobre el estado de la vigilancia y la mitigación de los riesgos identificados; el CIO debe estar presente en, al menos, una reunión del Directorio cada año, también para ayudar a incluir este tema en la agenda estratégica y mostrar su relevancia. También es importante que los directores conozcan al profesional que ocupa el cargo de director de TI y tengan acceso a él / ella cuando sea necesario.

ACI: ¿Cómo afectan las tecnologías móviles y de "redes sociales" a la forma de ver / administrar el riesgo cibernético?

Richard Doern: Anteriormente, era más centralizado y estandarizado, y tenía menos flexibilidad. Por lo tanto, su supervisión y control eran mucho más simples. Hoy en día es cada vez más descentralizada. Cada área de la empresa, con el objetivo de aumentar su eficiencia de los procesos, necesita dispositivos y software a la medida de sus necesidades. Esta situación da lugar a una gran cantidad de aplicaciones, plataformas y dispositivos contratados por una empresa, por lo que es más difícil de monitorear y controlar los procesos relacionados.

Otro punto importante es la amplia difusión de la computación en la nube. Las empresas incluyen más y más importantes documentos en las nubes y muchos empleados tienen acceso a esta información con una simple contraseña. Esto es seguido por - y también es un resultado de - el aumento del trabajo a distancia y, como consecuencia, la necesidad para el acceso remoto por los usuarios y el uso creciente de dispositivos móviles. Este conjunto de nuevas tecnologías, por un lado, promueve una mayor productividad en el trabajo, pero también aumenta la vulnerabilidad de las empresas en cuanto a seguridad de la información.

En los Directorios donde actúo, estamos siempre atentos a la implementación de políticas y procedimientos para el uso de las tecnologías móviles y las redes sociales para minimizar riesgos. La función del Directorio es esencial en el seguimiento de la eficacia de las políticas y procedimientos implementados.

ACI: Las estadísticas indican que "las personas de riesgo" son un factor de seguridad cibernética enorme. ¿Hay cuestiones de tono y de cultura que las empresas deben comunicar y el Directorio monitorear?

Richard Doern: Sí, yo creo que las medidas en este sentido en verdad ayudan. Es muy importante hacer que la gente se sienta parte de la empresa, especialmente hoy en día, cuando el compromiso con la empresa que existía en el pasado es casi inexistente. La rotación, particularmente en el nivel de gerencia media, aporta una considerable vulnerabilidad a la seguridad de la información que está cada vez más socializada. Además, los resultados de alta rotación traen dificultades para mantener la continuidad de los procesos y las tecnologías utilizadas por la empresa. En muchos casos, un nuevo profesional tratará de adaptar los procesos a sus propios hábitos de trabajos anteriores o tratará de implementar nuevas tecnologías, diferentes de los utilizados por la empresa, con los que están más familiarizados.

Con frecuencia, el resultado es la falta de continuidad de los procesos y la falta de información histórica. Un ejemplo sería un nuevo profesional de inteligencia de negocios que, solía trabajar con un determinado software de un trabajo anterior, sugiere que cambiar el software utilizado en la actualidad. Un cambio como éste parece simple al principio, pero requiere grandes esfuerzos para adaptar la red de la empresa, las normas de seguridad y generar una nueva política para los usuarios, etc. Multiplicando esto por todos los posibles cambios de la tecnología, puede resultar en trabajo sin fin y mayor inversión, además de poner en peligro la seguridad y fiabilidad de la información.

ACI: ¿Qué tan preocupado debería estar los Directorios sobre los riesgos cibernéticos que plantean los socios para negocios / vendedores de la compañía a lo largo de la cadena de suministro extendida?

Richard Doern: Este debe ser un punto de preocupación, especialmente para las empresas cuya política es la de subcontratar todas las actividades que no son del núcleo del negocio. Una vez más, las políticas, los procesos y los procedimientos deben ser implementados y monitoreados exhaustivamente. Aquí es donde los controles internos pueden contribuir considerablemente.

ACI: ¿Usted ve un papel de la auditoría interna para ayudar a identificar las vulnerabilidades de seguridad cibernética y mejoras?

Richard Doern: Por supuesto. La auditoría interna debe ser la estructura responsable de supervisar el cumplimiento de los procesos y políticas de toda la compañía, incluyendo las relacionadas con el uso de tecnología y seguridad de la información. Además, recomiendo que la auditoría interna se subordina directamente al comité de auditoría y tenga la autoridad necesaria para informar sobre posibles cambios en los riesgos identificados.

ACI: ¿Cuáles son los elementos críticos de un buen plan de contingencia en caso de un incidente cibernético importante?

Richard Doern: En primer lugar, creo que un plan de contingencia debe definirse durante el proceso de gestión de riesgos. Teniendo un buen conocimiento de la empresa, la industria y los riesgos críticos, el Directorio debe definir un plan de contingencia que satisfaga las necesidades del mercado. El plan debe ser mantenido por la alta dirección y ponerse en práctica en caso de situaciones extremas, y no depender de las reuniones del Directorio para resolver los problemas urgentes de última hora. Yo creo que el elemento más importante en situaciones extremas es actuar rápido. No es posible llamar a una reunión del Directorio para decidir qué se debe hacer en estas situaciones. El CEO tiene que tener autonomía suficiente y previa autorización de actuar en estos casos - por supuesto siguiendo el plan aprobado existente.

ACI: ¿Ve que los comités de auditoría tengan un papel particular que desempeñar (en comparación con el Directorio) en la supervisión de los esfuerzos de seguridad cibernética de la empresa?

Richard Doern: Si. Creo que el comité de auditoría debe incluir este tema en su proceso normal de gestión de riesgos, así como la gestión de otros riesgos. Es importante destacar que los miembros del comité de auditoría por lo general no tienen suficiente conocimiento en tecnología de la información y de seguridad para meterse de lleno en este tema específico y recomiendo el trabajo de consultores externos para ayudar.

ACI: La experiencia y el conocimiento de los riesgos de TI en el comité de auditoría / Directorio parecen ser un desafío permanente. ¿Cuáles son sus pensamientos sobre tener experiencia en TI en el comité de auditoría / Directorio, y la educación continua para los directores?

Richard Doern: En mi opinión, la presencia de un experto en TI en el comité de auditoría o en el Directorio puede ser muy útil. Sin embargo, tengo algunas dudas acerca de la contribución general de este profesional a los muchos otros temas estratégicos contemplados en el Directorio o en el comité de auditoría. Un experto de TI casi no tiene suficientes conocimientos en otras áreas para contribuir de forma relevante a las distintas decisiones tomadas por estos cuerpos.

A modo de ejemplo, un miembro del comité de auditoría que es un experto contable puede contribuir extraordinariamente a este tema y al comité de auditoría en general. Sin embargo, en una reunión del Directorio, este tema representa alrededor del 25 por ciento de los temas tratados. La contribución de un experto contable en el otro 75 por ciento es generalmente limitada, ya que él no tiene suficiente conocimiento en temas muy importantes como la estrategia, recursos humanos, etc. En la mayoría de los Directorios, los sujetos de TI aún representan una pequeña parte (incluso más pequeño que los contables) del Directorio y en la agenda del comité de auditoría y creo que no habrá ningún cambio relevante en el futuro cercano.

Sin duda, es fundamental para algunas industrias y tendrán una mayor necesidad de un experto en la materia, pero creo que para los demás, con obtener ayuda de la consultoría profesional o externa parece la medida más adecuada. Además, sin duda es necesario contar con un programa para la actualización constante de los directores. Como la mayoría de ellos no están familiarizados con la tecnología, es esencial que se actualizan sobre las nuevas tecnologías y en este sentido los CIOs pueden ayudar haciendo presentaciones y proporcionar materiales para las reuniones.

ACI: ¿Otras ideas para ser tenidas en cuenta por los miembros del comité de auditoría / directores respecto del riesgo cibernético?

Richard Doern: Un par de ideas, que se relacionan con algunos puntos que he tocado. Está claro que la seguridad cibernética debe recibir más atención y tiempo en el Directorio - y no debería estar completamente delegada en el comité de auditoría. Es importante llevarlo al Directorio periódicamente, haciendo hincapié en su importancia para la organización.

Estar atentos a los cambios en el perfil del CIO, que debe ser más estratégico, e invitar a los CIO a participar en al menos una vez al año en la reunión del Directorio. Es importante que los directores conozcan al CIO y tengan fácil acceso a él, y también que el CIO se sienta cómodo para ponerse en contacto con miembros del Directorio para informar sobre las nuevas tecnologías y los riesgos implicados, cuando sea necesario.

La educación continua para todos los miembros del Directorio es esencial para estar al día sobre este tema. Una medida útil es la creación de un glosario con los términos técnicos y expresiones, y que se ponga a mano de los directores literatura sencilla.

Asegúrese de que la empresa está monitoreando los medios de comunicación social; esto ayuda a tener empleados centrados en el trabajo.

Sea claro acerca de las funciones del Directorio, los comités, y el CEO, el CFO, el CIO cuando se requiera respuesta a una eventual crisis relacionada con la seguridad cibernética.

Por último, las inversiones para mitigar los riesgos de TI son enormes. Estas inversiones no generan ningún ingreso y consisten en tecnologías que estarán obsoletas en poco tiempo. Por lo tanto, se requieren grandes esfuerzos para convencer a los Directores y ejecutivos que tienen menos conocimientos en la materia para aprobar este tipo de gastos.

SRIDAR IYENGAR - DR. REDDY LABORATORIES E INFOSYS (INDIA)

Sridar Iyengar es presidente del comité de auditoría de DR.REDDY laboratorios. También es miembro de la junta directiva de ICICI Ventures, Rediff.com, Murugappa Group, Mahindra Holidays, Cleartrip, iYogi y otras empresas en los EE.UU. y la India. Anteriormente se desempeñó en los Directorios de Infosys y ICICI Bank, donde fue presidente del comité de auditoría. También es co-fundador de The Sounding Board, una red de líderes de negocios y empresarios que asesoran a las empresas de crecimiento rápido en la India.

> “El riesgo cibernético debe abordarse en el nivel estratégico más alto debido a su impacto potencial.”

ENTREVISTA

ACI: ¿Conoce un caso particular o ejemplo de un incidente de seguridad cibernética que haya sido una verdadera "revelación" para usted en términos de su potencial impacto?

Sridar Iyengar: tengo conocimiento de una serie de incidentes de alto perfil en los titulares, pero yo me enfrenté a un incidente personal, que me hizo conocer la cruda realidad de los ataques cibernéticos.

El ataque fue simple y al mismo tiempo sofisticado. Fue un ataque planeado y dirigido. Alguien había hackeado deliberadamente mi cuenta de correo electrónico y estudiado mis contactos de correo electrónico y - para no hacer el cuento largo - persuadió a mi banco para transferir dinero a la cuenta de una empresa ficticia de la que fue retirado de inmediato en efectivo. Todo ocurrió en un período de 24/36 horas. El hacker se enteró desde mis mensajes de correo electrónico que yo estaba en una zona horaria diferente, sabía cuales eran mis contactos en el banco, la ubicación de las empresas con las que yo podía estar lógicamente haciendo una operación personal, etc. Con esta información y con sólo interceptar, desviar y responder a los correos electrónicos que me enviaba el personal del banco que buscaba ponerse en contacto conmigo, el hacker tuvo éxito en la extracción de dinero de mi cuenta bancaria. Sólo una coincidencia me alertó sobre la piratería, mientras que sucedió. Demasiado tarde para detener la operación, pero a tiempo para detener el encubrimiento que habría eliminado todos los rastros.

Este incidente personal tiene algunas similitudes con algunos de los incidentes de alto perfil aparecidos recientemente en los titulares. El malware fue igualmente capaz de infectar a las interfaces de usuario (mi cuenta de correo electrónico) y extraer información de la tarjeta de crédito (mis contactos, datos bancarios). Además, el ataque salió a la luz sólo después que las operaciones fraudulentas se hicieron, utilizando la información que se extrajo. Pero no todos los ataques se originaron en las transacciones en línea, o a través de Internet. Esto demuestra que el mundo virtual y el mundo real se mezclan y los riesgos se están cruzando. Por lo tanto, ¿Cómo y cuándo sabemos que hemos sido comprometidos es una pregunta clave que uno se tiene que preguntar. A medida que haya más información personal y mayores transacciones financieras en línea, vamos a ver más y más ataques en el futuro.

ACI: ¿Qué tan alto está el riesgo cibernético en el mapa de riesgos de su empresa y en la agenda de las reuniones del Directorio / comité de auditoría?

Sridar Iyengar: La seguridad de la información es muy importante en nuestra agenda. El riesgo cibernético debe abordarse en el más alto nivel estratégico por el potencial impacto en la reputación, en las cotizaciones bursátiles, etc.

Nos centramos en la educación y en los niveles de conocimiento de los empleados, su cultura de cumplimiento de las políticas y procedimientos y la adhesión a los valores y la higiene de las buenas prácticas de seguridad informática. En todos los Directorios en los que participo, se requiere actualizaciones periódicas de información sobre nuestras defensas, estado de preparación, los tiempos de respuesta y la capacidad de contrarrestar y detener los ataques. También alentamos el uso de los hackers éticos para hacer regularmente pruebas de penetración.

ACI: ¿Cuáles son los tres principales desafíos que enfrenta cuando se trata de riesgos de seguridad cibernética?

Sridar Iyengar: Mis tres primeros serían: ser capaz de mantenerse a la vanguardia de la creciente sofisticación de los ataques cibernéticos; el ritmo al que aparecen nuevos riesgos y nuestra capacidad para hacer frente a tales riesgos; y la conciencia integral sobre las amenazas entre los empleados, clientes y ciudadanos en general.

ACI: ¿A quién se debe asignar las responsabilidades de supervisión sobre el riesgo de la seguridad cibernética - es decir, al comité de auditoría, al Directorio, u a otros comités del Directorio?

Sridar Iyengar: La supervisión de los riesgos de seguridad no debe ser sólo la responsabilidad de una auditoría o de un comité de riesgos. Es un asunto de negocios y todo el Directorio debe pasar tiempo dedicado a tomar conciencia de la percepción del riesgo, las amenazas y la preparación de la empresa para hacer frente a ellos. El comité de auditoría, a menos que exista un comité específico de seguridad de la información, sin embargo, podría tener delegada la responsabilidad de asegurar que estén implementados los programas adecuados, los procesos internos, la educación, las pruebas y de recibir los correspondientes informes.

ACI: En su opinión, ¿Cuáles son los factores críticos de éxito en la gobernanza del riesgo cibernético?

Sridar Iyengar: El éxito en esta área no puede ser definido como la ausencia de ataques o de la defensa exitosa contra uno. Se trata de un ámbito en constante evolución. Por lo tanto, la seguridad cibernética debe ser administrada a todos los niveles para tener un gobierno eficaz. Como se mencionó anteriormente, el Directorio y el comité de auditoría proactivamente deben participar en la supervisión del riesgo de seguridad cibernética. Los líderes empresariales deben ser responsables de los problemas de seguridad cibernética. El gobierno del ente debe centrarse en garantizar que tanto las personas y los sistemas que los apoyan están listos en todo momento para hacer frente a las amenazas. Por lo tanto, el refuerzo periódico de los valores corporativos, la educación y la mejora de las competencias, la sensibilización, la mejora de los sistemas, las pruebas y repetición de pruebas de las defensas son los factores críticos. El Directorio debe asegurar que los programas y procesos están en su lugar para cada una de estas áreas y están en funcionamiento en todo momento.

ACI: ¿Qué espera que haga la Gerencia en términos de políticas y procedimientos y, más concretamente, en cuanto a la información proporcionada?

Sridar Iyengar: La Gerencia tiene la responsabilidad de proteger la información que pertenece a la empresa. Por lo que necesitan articular los riesgos, cómo se está educando a los empleados acerca de ellos y cuáles son las disposiciones que se han implementado para contar con un marco global de seguridad cibernética para prevenir, detectar y solucionar cualquier incidencia de incumplimiento.

En el caso de un incumplimiento real, la Gerencia no sólo debe informar de la incidencia y su disposición sino que además tienen que demostrar que han hecho un análisis de la causa raíz y modificar las políticas o prácticas necesarias para prevenir nuevos casos, no sólo en el ámbito de la incidencia, sino en todas partes de la red corporativa. Es responsabilidad de la Gerencia darle al Directorio y/o al comité de auditoría la garantía necesaria de que la seguridad informática es una prioridad para toda la empresa en todo momento.

ACI: ¿Ves algún cambio o evolución en la interacción y compromiso de la comisión de auditoría / Directorio con el CIO - y en caso afirmativo, cuáles?

Sridar Iyengar: La seguridad informática es un tema de negocios y los líderes empresariales deben conocerla. La función del CIO es apoyar a los líderes de negocios mediante el aprovisionamiento del hardware más adecuado, el software y las personas necesarias para lograr una protección consistente en tener la menor fricción de las necesidades empresariales. La función del comité de auditoría es entender los riesgos involucrados, equilibrar las necesidades de la empresa con los imperativos de seguridad cibernética y apoyar el CIO y su equipo en la operación de un marco óptimo de seguridad cibernética. Por lo tanto, es imperativo que el CIO y el comité de auditoría colaboren y se comuniquen de manera proactiva y con frecuencia.

ACI: ¿Cómo se puede esperar de la auditoría interna y externa para cubrir los riesgos de seguridad cibernética?

Sridar Iyengar: Parte de la función de auditoría interna es determinar si todas las políticas y procedimientos de la organización se cumplan en la práctica. El marco de seguridad cibernética de la organización tendrá sus propias políticas y procedimientos. En virtud de su plan de auditoría aprobado por el comité de auditoría, la auditoría interna deberá comprobar regularmente que estas políticas y procedimientos y los controles necesarios que conllevan están funcionando como se han diseñado y debe notificar cualquier hallazgo significativo al comité de auditoría. Los comités de auditoría deben asegurarse de que la auditoría interna tiene las habilidades necesarias para hacer esto por sí o a través de otros expertos externos calificados.

Los expertos externos/auditores pueden proporcionar al Directorio y al comité de auditoría información y recomendaciones que reflejen los principales estándares de la industria y también compartir las experiencias adquiridas de su interacción con otras empresas.

ACI: ¿Sientes que los comités de auditoría en la actualidad tienen las habilidades necesarias de seguridad cibernética y los conocimientos necesarios para evaluar los planes e informes de auditoría sobre este asunto?

Sridar Iyengar: En mi experiencia, los comités de auditoría son conscientes tanto de la necesidad general de un marco de seguridad cibernética robusto y de las áreas específicas de información cuya fuga podría causar más daño a la organización. Pero es poco probable que conozcan o entiendan los detalles de las interdependencias de información, la robustez de la infraestructura de la tecnología o de la competencia requerida de las personas involucradas en el suministro de la capa de protección frente a cualquier incidente. Tener gente en el comité que tenga conocimiento en esta área ayuda claramente. Esta es una razón por la que los comités de auditoría exigen cada vez más especialistas en esta área.

ACI: Algunas organizaciones grandes, principalmente las instituciones financieras, están revelando cada vez más ataques cibernéticos en sus presentaciones regulatorias. ¿Cómo te sientes acerca de tales revelaciones?

Sridar Iyengar: Sí, muchos bancos divulgan este tipo de ataques en sus informes anuales, incluso en los casos en que los ataques no dan lugar a ningún daño material a la institución. Como alguien que cree que más divulgación es siempre mejor, es un paso en la dirección correcta. A medida que estos incidentes son cada vez más importante desde el punto de vista de los riesgos del negocio, es bueno que estén siendo revelados.

JAN ZEGERING HADDERS
AGEAS (BÉLGICA)

Jan Zegering Hadders es presidente del comité de auditoría de AGEAS y también sirve como miembro del comité de gobierno corporativo. También es miembro del consejo de supervisión de GE Artesia Bank y presidente del comité de auditoría de GE Artesia Bank, entre otros. También se desempeñó como presidente de la junta de supervisión de Grontmij NV y como presidente de la junta directiva de ING Netherlands.

> “La gente siempre va a seguir robando dinero, sólo el cambio de técnicas basadas en los sistemas que utilizamos.”

ENTREVISTA

ACI: ¿Tiene alguna experiencia con los ataques cibernéticos?

Jan Zegering Hadders: Estando activo en el sector financiero, por supuesto que me he encontrado tanto con delincuentes organizados como pequeños tratando de robar dinero del sistema.

El robo de dinero de los bancos o de los sistemas no es nuevo. Sucedió hace 600 años. Todo tipo de películas muestran cómo se ha hecho, desde el robo de un tren después de la voladura de una bóveda hasta la piratería en el sistema financiero. La gente siempre ha robado el dinero y siempre seguir robando dinero, sólo las técnicas cambian dependiendo del tipo de sistemas que utilizamos para almacenar y transferir dinero.

ACI: ¿Cuáles son los principales retos que los comités de auditoría se enfrentan cuando se trata de riesgos de seguridad cibernética?

Jan Zegering Hadders: Las empresas, sobre todo en el sector financiero, deben tomar muy en serio la seguridad cibernética y la defensa de sus sistemas de la forma más moderna o se encontrarán siendo burlados por los delincuentes cibernéticos.

Los sistemas de información y los sistemas de defensa contra ataques cibernéticos de las instituciones financieras suelen ser ya muy sofisticados, pero los delincuentes han demostrado ser muy inteligentes en la búsqueda de formas nuevas y más innovadoras para atacar. Si sus sistemas de defensas no tienen en cuenta las últimas innovaciones en materia de ataque cibernético, entonces son vulnerables a los ataques. Por lo tanto, un desafío importante para los comités de auditoría es tratar de asegurar que la gerencia tenga sus sistemas y controles actualizados y equipados para estar un paso adelante de los criminales cibernéticos.

ACI: ¿Tener la experiencia adecuada a bordo es de un reto importante?

Jan Zegering Hadders: Por ahora, prácticamente todas las instituciones bancarias y de seguros han acumulado conocimientos específicos sobre la prevención de los ataques cibernéticos y para minimizar la cantidad de dinero que es robado de sus sistemas. Ese conocimiento se ha adquirido principalmente de ataques ocurridos - de las lecciones aprendidas.

Por supuesto que el comité de auditoría no participa en la gestión del día a día de la empresa y, por tanto, no puede tener un conocimiento detallado de los aspectos específicos de TI y de los sistemas de seguridad cibernética. Pero, en general, yo personalmente no veo mucha gente con experiencia específica y detallada en el cibercrimen en el comité de auditoría o en el Directorio. Yo si veo comités de auditoría con cada vez más y más conocimientos sobre los conceptos básicos de riesgo cibernético. Además, los comités de auditoría solicitan más proactivamente información a la gerencias obre los riesgos y el nivel de madurez de los sistemas de defensa para poder evaluar adecuadamente si la empresa está a la velocidad adecuada en la prevención de, al menos, los ataques cibernéticos más significativos.

Con los miembros del comité de auditoría teniendo una buena noción básica de cómo funcionan los ataques cibernéticos y, junto con la experiencia específica y con información enfocada provista por la gerencia y expertos externos, el comité de auditoría debe ser capaz de hacer las preguntas correctas a la gerencia enfocándose en los riesgos clave.

Por supuesto, se podría decir que aún falta experiencia específica en el comité de auditoría, dependiendo de la compañía, pero le corresponde al comité de auditoría solicitar ayuda para conseguir esta experiencia extra del CIO o del CRO, o de expertos externos.

ACI: Dónde trazar la línea en la defensa contra los delincuentes cibernéticos podría ser un desafío por sí mismo.

Jan Zegering Hadders: Las empresas tienen que considerar si el costo de la defensa se encuentra todavía en equilibrio con la exposición al riesgo en su conjunto. Encontrar el equilibrio adecuado es de hecho un reto importante y difícil que el Directorio y/o el comité de auditoría tienen que considerar. Los sistemas de tarjetas de crédito, por ejemplo: los sistemas de defensa de tarjetas de crédito no pretenden estar equipados para evitar que el dinero sea robado. Desde una perspectiva general de gestión de riesgos, el riesgo de tener que reembolsar a los clientes por montos robados se refleja en el precio de la tarjeta de crédito.

ACI: ¿Qué tan alto debe estar el riesgo cibernético en el mapa de riesgos y en la agenda de la junta directiva y/o del comité de auditoría?

Jan Zegering Hadders: Normalmente el riesgo cibernético es una prioridad en la agenda del comité de auditoría y/o del Directorio cuando su empresa ha sido atacada o cuando los auditores internos u otros han informado de importantes vulnerabilidades en base a sus procedimientos.

Estoy muy a favor de un enfoque más proactivo de también ser conscientes de los riesgos emergentes, haciendo la pregunta correcta a tiempo, para también recibir la información por adelantado para presionar a la gerencia.

Por otro lado, muchos se preguntan por qué el riesgo cibernético no está más alto en la agenda de riesgos de lo que está hoy. En mi opinión, no hay razón lógica para esto. Los clientes son conscientes de que el crimen está allí cada día, cada hora, cada segundo y que lo han aceptado de esta manera. Y, por supuesto, todas las instituciones financieras son sensibles a la publicidad negativa y daños a la reputación, pero siempre y cuando las personas no se vean perjudicadas, ya que cualquier daño es reembolsado, el riesgo de reputación asociado al riesgo cibernético podría considerarse bastante bajo. Debido a la actitud relajada de los clientes hacia los ataques cibernéticos, el riesgo que una empresa está dispuesta a aceptar puede ser mayor del que uno podría esperar inicialmente.

ACI: Específicamente, ¿Qué es lo que se espera de la Gerencia en relación con la seguridad informática?

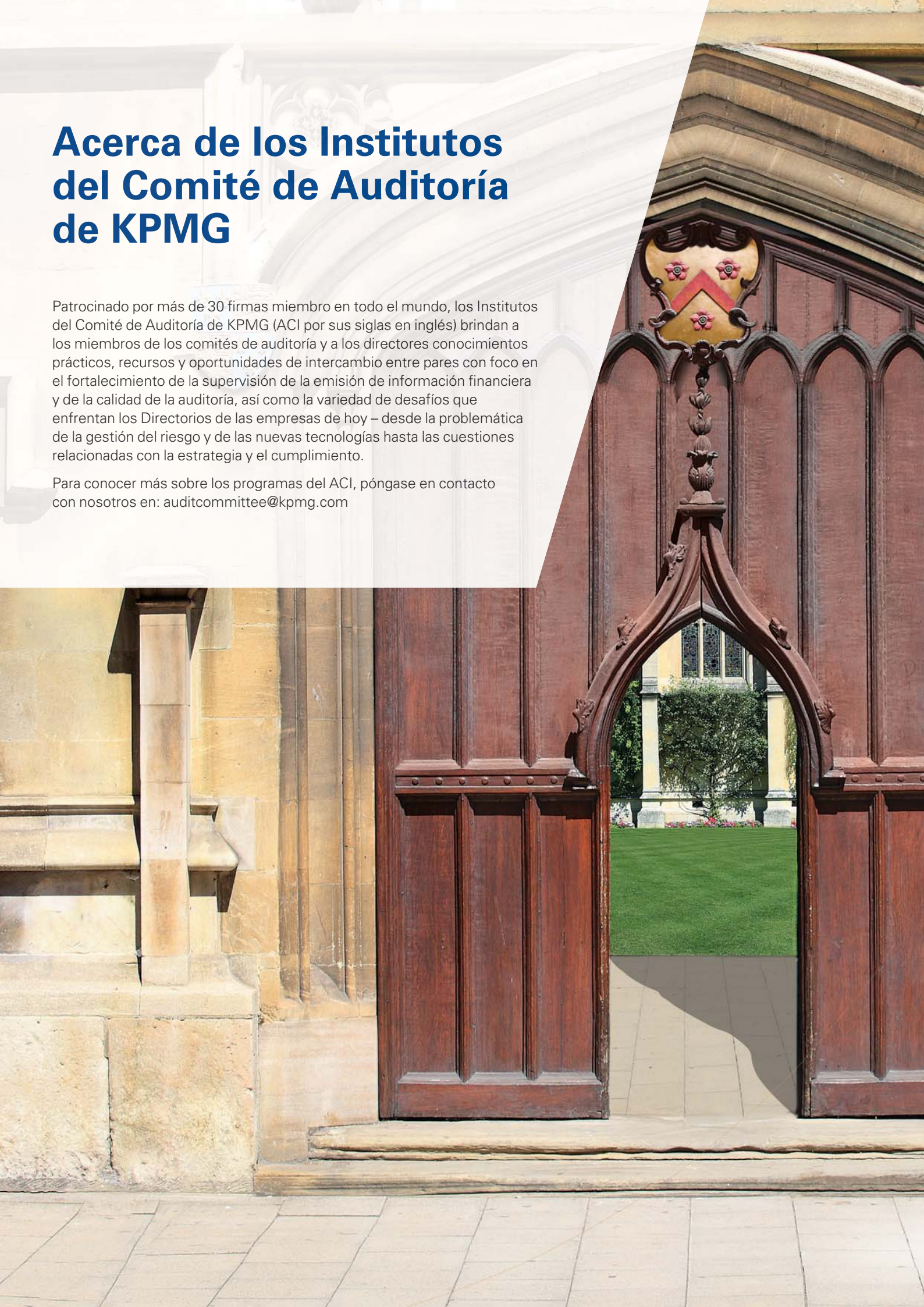
Jan Zegering Hadders: Por supuesto, es bueno escuchar a la gente en TI que se ocupa de la seguridad cibernética en el comité de auditoría y, por supuesto el riesgo cibernético debe tener un lugar en el mapa de riesgos y recibir la dedicación que necesita de parte de la Gerencia basada en su grado de riesgo relativo. Lo más importante es que la Gerencia y la empresa tengan el nivel adecuado de conocimientos para abordar con eficacia los riesgos cibernéticos.

Si el riesgo cibernético sube en la agenda del comité la auditoría y/o del comité de riesgos, debe sin duda estar también más alto en la pantalla de radar de los niveles C. Una de mis expectativas es que la seguridad cibernética se vea reflejada en un KPI formal para directores ejecutivos y no sólo para los mandos medios que trabajan en él en el día a día. Haciendo a los niveles C formalmente responsables de garantizar la seguridad cibernética para los clientes y la empresa es un aspecto importante desde una perspectiva más amplia del gobierno corporativo.

Acerca de los Institutos del Comité de Auditoría de KPMG

Patrocinado por más de 30 firmas miembro en todo el mundo, los Institutos del Comité de Auditoría de KPMG (ACI por sus siglas en inglés) brindan a los miembros de los comités de auditoría y a los directores conocimientos prácticos, recursos y oportunidades de intercambio entre pares con foco en el fortalecimiento de la supervisión de la emisión de información financiera y de la calidad de la auditoría, así como la variedad de desafíos que enfrentan los Directorios de las empresas de hoy – desde la problemática de la gestión del riesgo y de las nuevas tecnologías hasta las cuestiones relacionadas con la estrategia y el cumplimiento.

Para conocer más sobre los programas del ACI, póngase en contacto con nosotros en: auditcommittee@kpmg.com



kpmg.com.ar

Contactos:

Néstor García
Socio a cargo de Auditoría
+54 11 4316 5870
nrgarcia@kpmg.com.ar

Guillermo Calciati
Socio
+54 11 4316 5802
grcalciati@kpmg.com.ar

Viviana Picco
Socia
+54 11 4316 5802
vpicco@kpmg.com.ar

Diseñado por el equipo de Servicios Creativos - Marketing y Comunicaciones - Buenos Aires, Argentina.