KPMG

Los CEOs ante la encrucijada de la ciberseguridad

Mayo 2016

kpmg.es

Prólogo

En un mundo interconectado en el que la transformación digital, el Big Data o el Internet de las cosas están cambiando la forma de ver el futuro, la ciberseguridad no puede dejarse de lado. En paralelo a la fuerte apuesta por la innovación que están realizando los bancos, las empresas de telecomunicaciones o las de distribución, el cibercrimen también avanza en este sentido. Actualmente puede considerarse un sector perfectamente organizado y que mueve millones a diario, con sus clientes, proveedores, medios de pago (muchas veces en forma de bitcoins) y con su propia plataforma de e-commerce (la Darknet o red TOR).

Las empresas no pueden obviar estos riesgos y éstas, cada vez más, los discuten en los Comités de Dirección o en las reuniones del Consejo. Este estudio que presentamos en España y que se basa en la opinión de más de 1000 CEOs de 10 países indica que, actualmente, la ciberseguridad está al mismo nivel de preocupación que mantener o incrementar la lealtad de los clientes o mejorar la relevancia de los productos o servicios en los distintos mercados. Es, por tanto, el momento de reflexionar, y de concluir que la ciberseguridad ya no puede considerarse un tema técnico que se delegue en el Departamento de Sistemas, sino que ha de abordarse como un tema estratégico que alcanza a toda la organización.

Finalmente, y sin ánimo de que la ciberseguridad se convierta en un freno para abordar nuevas iniciativas, sino en un facilitador que aporta agilidad, reducción de riesgos y diferenciación, es clave considerar tres aspectos. El primero es que los grandes riesgos se pueden reducir en gran parte aplicando medidas de seguridad básicas. El segundo es que no se puede intentar proteger al mismo nivel todos los activos, por lo que hay que hacer un análisis de riesgos riguroso. Y el tercero, y más importante, es que hay que empezar a considerar las herramientas de ciberinteligencia como un aspecto clave de nuestra estrategia de defensa. Es necesario anticiparse a los cibercriminales y, para ello, es útil saber qué está ocurriendo en otras empresas, en nuestro sector y en el mercado en general.

Marc Martínez
Socio responsable
de Ciberseguridad
de KPMG en España

CEOs globales: la delgada línea entre el riesgo y la recompensa

Un email con una inofensiva fotografía de su hija en un partido de fútbol. El alto directivo de una empresa petrolera que lo abre no tiene ni idea (lo descubrirá años después) de que la imagen contiene un malware que, inmediatamente, permitirá a un ciberdelincuente registrar cada uno de sus movimientos en el ordenador, incluidos los correos. Tras este suceso, los ciberespías realizaron capturas de pantalla, consiguieron encender la cámara y el micrófono y, por consiguiente, pudieron obtener valiosa información sobre lo que estaba aconteciendo en la compañía. Mientras, la empresa había estado presentándose a diferentes concursos para adquirir ciertos derechos petroleros pero, "casualmente", siempre se quedaba algo por debajo de la propuesta ganadora.

En paralelo, un fabricante de monitores lanza al mercado una novedosa aplicación, cuya principal funcionalidad es el control remoto de la temperatura, las luces y los sistemas de seguridad domésticos a través del smartphone. El único problema es que la tecnología es tan fácil de utilizar que un grupo local de ciberdelincuentes hackea el sistema para planificar el robo en las casas. Un simple cambio en el sistema de seguridad y en la forma de iniciar sesión podría haberlo evitado.

Una empresa del sector retail se da cuenta de que una red de piratas informáticos ha estado desviando sigilosamente durante meses las ventas que se procesaban en sus establecimientos con tarjetas de crédito y débito. El equipo de alta dirección y el consejo de administración descubren el ataque gracias a las fuerzas de seguridad del Estado y la noticia sale a la luz sin que pudieran contener el ataque o si quiera prever las consecuencias.

Son tres casos ficticios pero que, en una sociedad tan interconectada como la actual, podrían tener lugar cada día en cualquier parte del mundo. Una mejor prevención podría haber ayudado en todos estos casos, pero no habría sido suficiente: la importancia de mejorar la seguridad en productos y procesos es indudable, pero, en igual medida, lo es conocer quién está atacando y contar con un plan para mitigar las amenazas cuando se detectan.

Asimismo, es necesario tener en cuenta que la innovación va, casi siempre, por delante de la seguridad. Hoy, la tecnología permite a las empresas conectar con sus clientes de formas que nunca antes hubiéramos imaginado, a través de dispositivos inteligentes, marketing y productos personalizados o servicios automatizados que facilitan la optimización de tareas administrativas y ofrecen servicios más inmediatos y personalizados.

El problema es que "los malos" también innovan. Es más, uno de los mercados considerados más avanzados es el de la red oscura (Darknet), que conecta al crimen organizado con los hackers de todo el mundo. En este entorno, todos los días se comparten y desarrollan nuevas herramientas, nuevos servicios de ataques y estrategias para captar efectivo. Todo se encuentra bajo un cambio constante: los puntos que se ven comprometidos, los riesgos y las consecuencias.

¿Qué le quita el sueño a los CEOs?

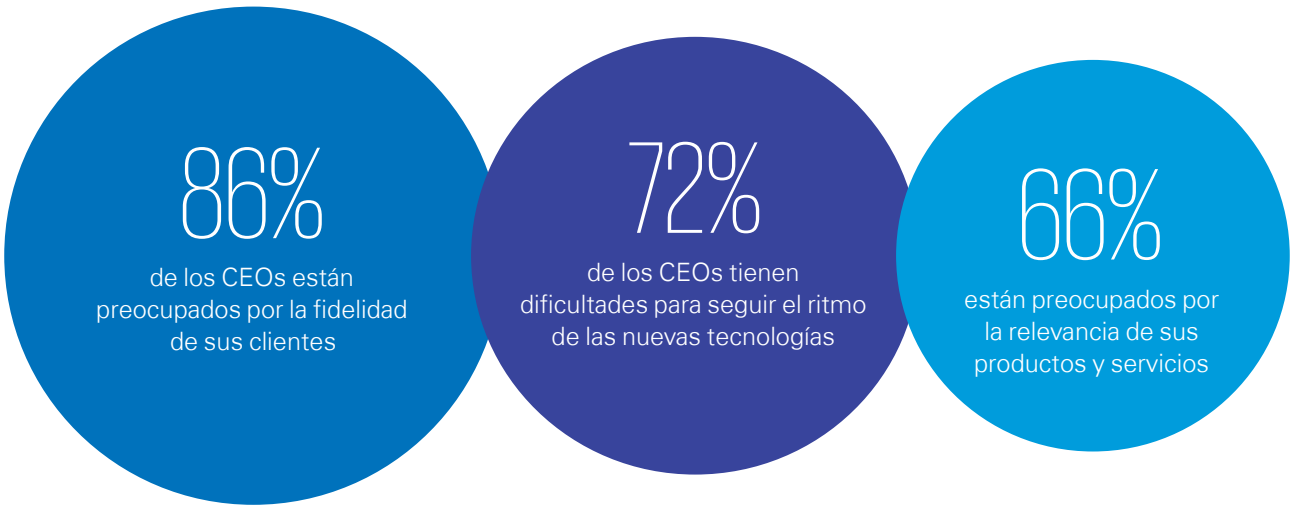
Preservar la seguridad de los datos (ya sean de clientes, relativos a la propiedad intelectual o internos de la propia empresa) ya no es una ocurrencia de última hora en la mayoría de las organizaciones. Sin embargo, aquellos temas que quitan el sueño a los CEOs de todo el mundo están relacionados con la relevancia de sus productos y servicios (les preocupa a dos tercios), con seguir el ritmo de las nuevas tecnologías (tres cuartas partes) y la fidelidad de sus clientes (que preocupa a casi todos). Así lo señala una encuesta de KPMG Internacional realizada a más de 1.200 altos directivos de algunas de las empresas más grandes y complejas del mundo[1].

Pero, sorprendentemente, España no se ajusta a esta tendencia. Aquí el grado de preocupación expresado por los CEOS en cuanto a los asuntos planteados es, en general, mucho más bajo. Los CEOs españoles sí que manifiestan preocupación por la relevancia de sus productos y servicios, pero el factor más mencionado es la llegada de nuevos competidores que cambien los modelos de negocio.

En este sentido, la relevancia de los productos y servicios está estrechamente ligada con la ciberseguridad, pues integrar este tipo de procesos podría convertirse en una ventaja competitiva. Según asegura Malcom Marshall, responsable global de Ciberseguridad de KPMG, "algunas organizaciones están convirtiendo la seguridad en un argumento de venta con la identificación mediante el contacto". Los bancos, por ejemplo, comienzan a sustituir complejos procesos de seguridad por este tipo de procedimientos, basados en la idea de que "si eres capaz de identificar a tu personal y a tus clientes con niveles muy elevados de certeza, puedes prestarles niveles de servicio mucho más personalizados", añade.

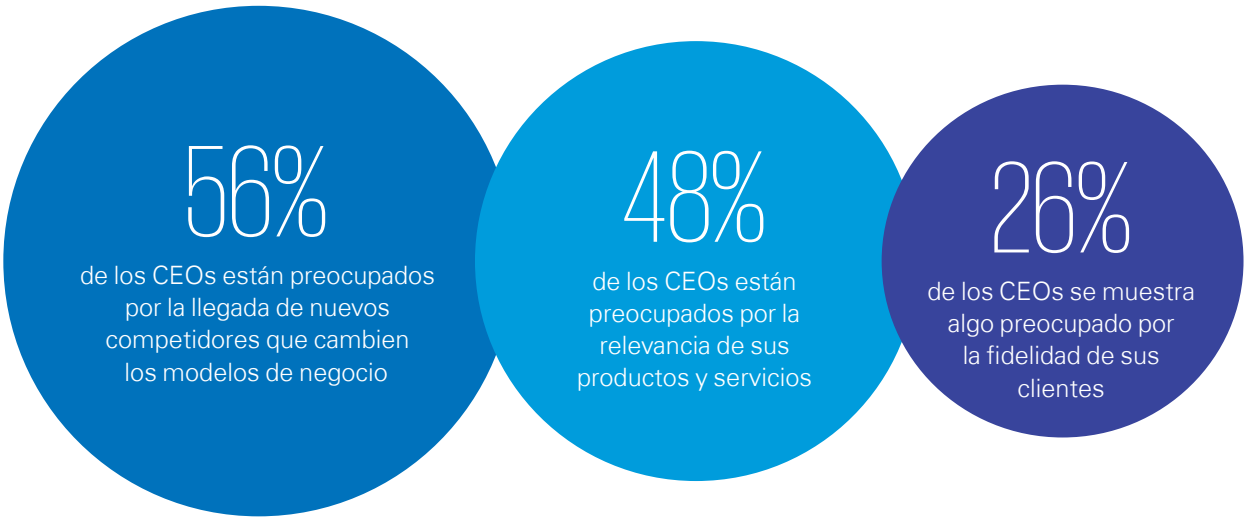
[1] Véase la metodología de la encuesta al final de este informe.

Global:



Fuente: 2015 KPMG CEO Outlook, mayo de 2015

España:



Fuente: 2015 KPMG CEO Outlook, mayo de 2015

Todas las compañías son ciberempresas

Uno de los mayores errores que puede cometer una organización es considerar la ciberseguridad una competencia exclusiva del CIO (máximo responsable del TI). "El CIO desempeña una función muy importante, pero, aunque aumenta el número de entidades que utilizan medios digitales para acercarse al cliente, no lo hacen en igual medida los expertos en ciberseguridad contratados o consultados por las compañías", indica Marshall. "Muchos altos directivos no son conscientes del nivel de tecnología que integran sus productos y tampoco suelen haber reflexionado sobre las artimañas que pueden emplear los ciberdelincuentes para sacarles provecho", añade Marshall. Queda mucho camino por recorrer para que los conocimientos sobre ciberdelincuencia se equiparen a aquellos de los que se dispone sobre la delincuencia convencional.

En definitiva, se trata de una cuestión de integridad y reputación del producto, un tema que preocupa al consejo de administración. Los inversores institucionales, por ejemplo, tienden a invertir menos en una empresa sobre la que los medios de comunicación han difundido que cuenta con fallos de ciberseguridad. Así, las consecuencias van más allá: incluso podría afectar al precio de las acciones y a la capacidad de obtener capital.

Conclusión:
Toda compañía es ahora una ciberempresa, y cada una de ellas debe permanecer vigilante.

> "Caminamos colectivamente como sonámbulos hacia la vulnerabilidad y fracasamos a la hora de aprender las lecciones de integrar la seguridad en los productos desde su origen"

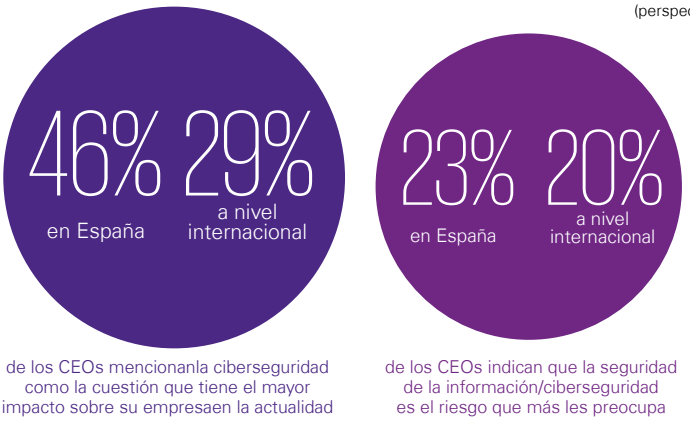
Malcolm Marshall
Responsable global de Ciberseguridad de KPMG

Ciberseguridad: un riesgo estratégico

La alta dirección y los consejeros de administración han considerado tradicionalmente la ciberseguridad como un problema táctico y no como una cuestión estratégica, pero, en los últimos diez años, han comprendido que estos riesgos podrían convertirse en un problema serio para la compañía.

Casi la mitad de los CEOs españoles mencionan la ciberseguridad como la cuestión que tiene el mayor impacto sobre su empresa en estos momentos, mientras que estas respuestas suponen un 29% en la encuesta global. Uno de cada cinco, tanto en España como a nivel global, indica que la seguridad de la información es el riesgo que más les preocupa. El riesgo operacional y el de cumplimiento normativo se mencionan como los riesgos principales internacionalmente, mientras que en España el primer riesgo mencionado es el estratégico.

Fuente: 2015 KPMG CEO Outlook (perspectivas de los CEO), mayo de 2015



Pero los ciberriesgos, si no se controlan, pueden derivar rápidamente en un problema operativo y regulatorio. "Cuando un fallo de seguridad sale a la luz, normalmente tengo que dejar de lado las operaciones para centrarme en el ciberevento", apunta Marc Martínez, socio responsable de Ciberseguridad de KPMG en España. "Tengo que interrumpir parte de mis operaciones para intentar corregir o subsanar el problema cibernético y, a continuación, gestionar una serie de procesos legales y las posibles consecuencias", añade.

El desarrollo de un marco para el ciberriesgo

Los riesgos reputacionales, regulatorios y legales preocupan a todas las compañías pero, en las organizaciones que gestionan infraestructuras físicas, estos se multiplican. Un ataque podría tener consecuencias en el manejo de los controles, provocar la destrucción de equipamientos o la paralización de operaciones, así como crear riesgos de liquidez. En este sentido, los ataques a empresas públicas de petróleo y gas que se han producido en los últimos años han dado la voz de alerta para otras organizaciones de los sectores energético e industrial. Sin las líneas de crédito y las garantías públicas del Estado, muchas de ellas habrían tenido que enfrentarse a problemas de liquidez en cuestión de días si hubieran sido objeto de este tipo de ataques.

"Muchas organizaciones disponen ya de un marco para evaluar el riesgo empresarial, pero el ciberriesgo sigue tratándose de un modo distinto", asegura Marshall, que cree un error actuar así.

Especialmente en el sector bancario, las organizaciones llevan años reflexionando sobre el riesgo de terceros. Para paliarlo, algunas entidades han optado por contar con múltiples proveedores, de modo que, si uno de ellos falla, siguen manteniéndose resilientes. Ahora bien, si se analiza la cuestión con más detenimiento, este tipo de riesgos se vuelve a consolidar en el siguiente nivel, porque todos estos proveedores diversificados dependen a su vez de un único proveedor. Este fenómeno se conoce como "riesgo de la cuarta parte". Este descubrimiento es habitual cuando se evalúa el riesgo de liquidez, pero el proceso puede ser igual ante ciberataques. Por ejemplo, ¿qué ocurre si todos los proveedores dependen del mismo proveedor que opera en la nube?

"Toda organización debería disponer de un marco de análisis de la ciberseguridad y lo ideal sería que estuviese integrado en el de riesgo empresarial de la organización", explica Marc Martínez. Son varios los marcos que pueden emplear las organizaciones: el Framework for Improving Critical Infrastructure Cybersecurity (el marco para mejorar la ciberseguridad en infraestructuras críticas), publicado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos; Cyber Essentials (aspectos esenciales de la ciberseguridad), emitido en Reino Unido; o la norma internacional ISO27001, que es el marco más común adoptado a escala global. No obstante, la elección de este marco es mucho menos importante que la forma de integrarlo e implantarlo. En opinión de Marc Martínez, "la clave reside en que se generalice dentro de la gestión de riesgos en la organización".

Conoce a tu enemigo

El primer paso para conocer al enemigo es averiguar qué persona o grupo podría llegar a planificar un ataque, qué parte de la empresa sería su objetivo y por qué (véase el apartado sobre inteligencia de seguridad en la página 13). Un marco también puede ayudar a las organizaciones a determinar qué activos necesitan proteger y en cuáles un ataque podría generar más daños. De esta forma, es más fácil dirigir la inversión allá donde sea necesario y proteger las áreas en las que el daño tendría más impacto.

La propiedad intelectual es una de las joyas de la corona para muchas empresas de tecnología, pero ¿qué ocurre cuando una organización internacional realiza el diseño del producto en un país, desarrolla el software en otro, partes del hardware en un tercero y, además, tiene proveedores situados en todo el mundo?

El consejo de administración de una empresa identificó la propiedad intelectual como uno de sus principales riesgos, pues llegó a la conclusión de que si alguien accedía a sus documentos podría descubrir sus planes para lanzar nuevos productos o incluso llegar a copiarlos. Su supervivencia, entonces, se pondría en peligro.

Gracias a los servicios de un hacker de sombrero blanco (white-hat hacker) contratado por la compañía, los directivos pudieron comprender que el punto débil estaba en una de sus instalaciones (precisamente en la que conseguían una fabricación más rentable y producir un mayor volumen de productos). El hacker fue capaz de acceder en unos 30 segundos a todos los sistemas del taller y de tomar el control total desde el punto de vista de la ciberseguridad, incluida la propiedad intelectual. Es más, aseguró que incluso un pirata informático sin un talento extraordinario podría hacerse con el control de los servidores, desde los programas de garantía de calidad hasta el proceso de fabricación. Al CIO este hallazgo no le sorprendió. Había intentado trabajar en la ciberseguridad con los equipos del área de fabricación, pero los proyectos se habían frenado ante el temor que le habían mostrado de que los controles de seguridad impidiesen el desarrollo de las operaciones.

Pero las vulnerabilidades detectadas no terminaban ahí. También se diagnosticó que el programa de garantía de calidad del producto más rentable de la empresa carecía de la integridad suficiente. A la hora de enfrentarse a una posible demanda colectiva, una empresa que ha perdido el control de la garantía de calidad tendría muchas dificultades para construir su defensa.

Otro riesgo que con frecuencia se pasa por alto es el que surge de las fusiones y adquisiciones. Algunas organizaciones están aprendiendo, para su desgracia, que comprar una empresa cuyos productos no son seguros puede salir caro. Por ejemplo, en una reciente operación, el coste de subsanar las debilidades en ciberseguridad de la empresa adquirida fue el equivalente al 25% del precio de compra. La due diligence realizada por la entidad adquirente no reveló estas debilidades, porque no se tuvo en cuenta lo crítica que puede ser la ciberseguridad en algunos productos y, en concreto, en uno diseñado para ser utilizado en vehículos.

¿Estás preparado?

La mitad de los CEOs encuestados a nivel internacional declaran estar totalmente preparados para un ciberataque futuro, pero, en Europa, la situación difiere: un 31% asegura estar completamente preparado, frente al 66% que se identifica como algo preparado. Malcom Marshall asegura que muchas empresas europeas aún se encuentran al comienzo o a medio camino del viaje de la ciberseguridad. "Aún están buscando soluciones de ciberseguridad eficaces y rentables que les permitan gestionar adecuadamente los incidentes. Incluso aunque hayan invertido en ciberseguridad, los CEOs europeos son más cautos y se muestran menos proclives a declararse completamente preparados en materia de ciberseguridad", puntualiza.

Asimismo, plantea que las revelaciones del caso Snowden han podido tener impacto en los CEOs europeos, de modo que están replanteándose sus estrategias de seguridad y ciberseguridad: "En los últimos años estamos viendo cómo muchas compañías europeas están cambiando sus proveedores de ciberseguridad, pasando de confiar en empresas radicadas en Estados Unidos a otras domésticas. Otras se están planteando hacerlo próximamente", asegura el experto.

En España, la situación se asemeja del resto de Europa. La mayoría de los primeros directivos españoles (56%) se siente algo preparado ante un ciberataque y solo un 28% se declara totalmente preparado.

Paradójicamente, las empresas españolas parecen haber

tomado más medidas para evitar y hacer frente a posibles fallos en ciberseguridad. Un 86% de los CEOs españoles aseguran que ya han creado un equipo de ciberseguridad o ha nombrado a un directivo en el área, mientras que a nivel mundial este porcentaje desciende al 50%.

Destaca también el porcentaje de CEOs que aseguran haber tenido múltiples reuniones del consejo de administración sobre ciberseguridad (58% en España frente al 46% a nivel internacional) o la implementación que ya realizan de las nuevas tecnologías (56%, frente al 40% en todo el mundo). Un 60% ha cambiado sus procesos internos, un porcentaje 15 puntos superior a la cifra internacional y un 52% los internos, frente a un 34%.

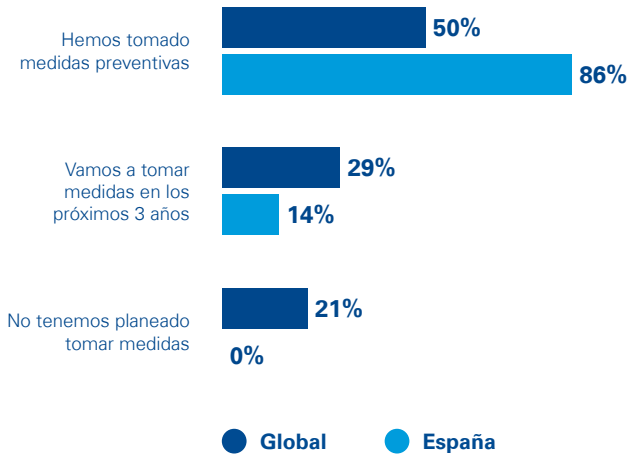
Así, el dato más sorprendente si se analizan estos resultados que lo ha hecho a nivel global es que solo un tercio de las organizaciones declara haber realizado cambios en los procesos externos, como el intercambio de datos o el procesamiento de transacciones. Actualmente, los ciberdelincuentes son capaces de burlar los controles de seguridad más estrictos, incluso en las organizaciones de mayor tamaño, infiltrando programas maliciosos (malware) en sus proveedores de productos y servicios, que habitualmente tienen menor tamaño.

Algunos de los fallos en seguridad más espectaculares que se han conocido en los últimos años fueron causados por proveedores externos. La creciente complejidad en la gestión de la cadena de suministro y la tendencia a establecer procesos más conectados hacen imprescindible ampliar los procesos de ciberseguridad hasta llegar al último proveedor.

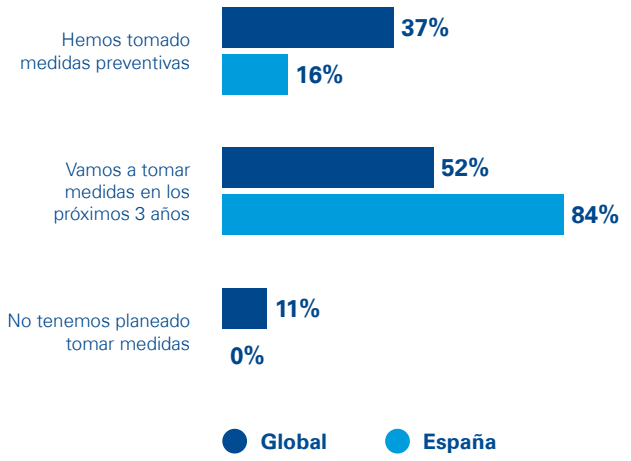
Así, la ciberseguridad puede convertirse en una ventaja competitiva: un protocolo sólido y demostrable de seguridad puede constituir un fuerte argumento de venta para una empresa que ofrezca la posibilidad a sus clientes de conectarse a través de una red abierta.

¿Qué medidas tiene previsto tomar en los próximos tres años?

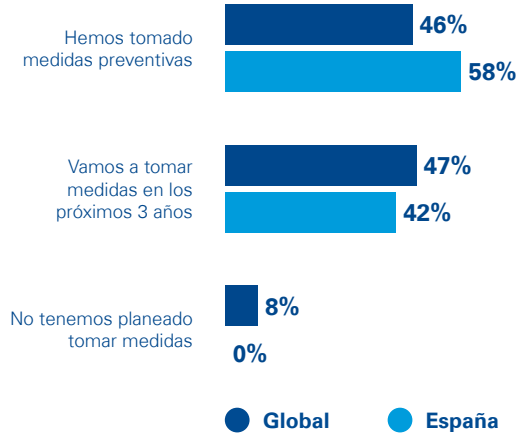
Nombrar a un directivo o crear un equipo de ciberseguridad



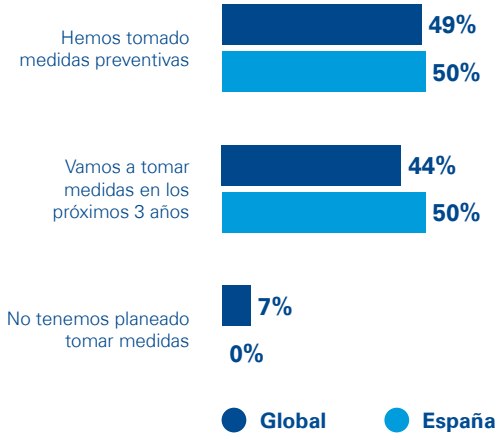
Organizar múltiples reuniones con el equipo de ciberseguridad



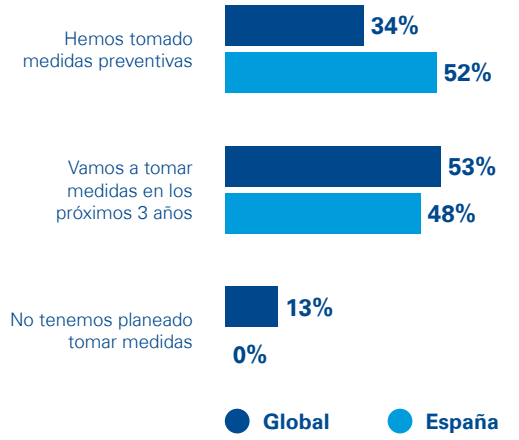
Convocar numerosas reuniones con el consejo de administración para hablar sobre ciberseguridad



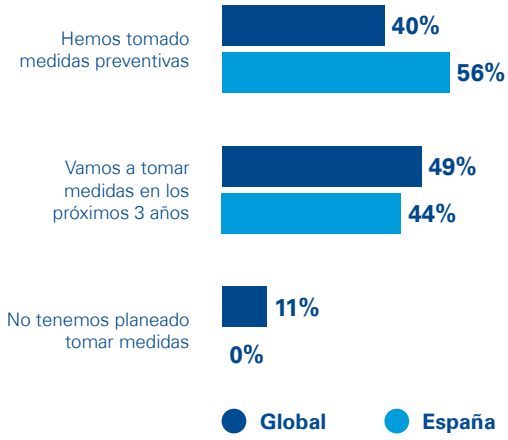
Actualizar las tecnologías actuales



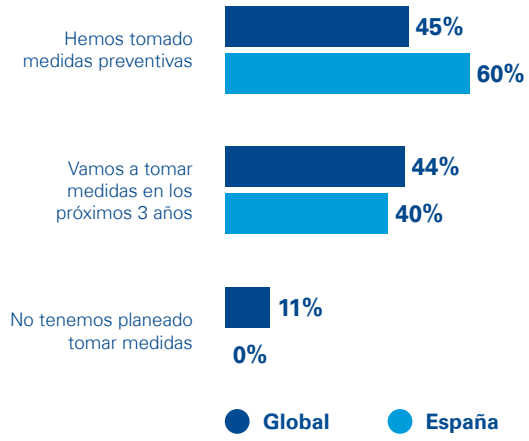
Cambiar procesos externos (recopilación de datos, procesamiento de transacciones, intercambio de datos, etc.)



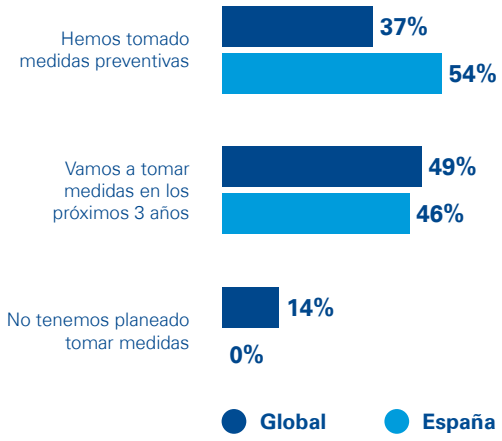
Implantar nuevas tecnologías



Cambiar procesos internos (intercambio de datos, uso de dispositivos, etc.)



Contratar a un consultor en ciberseguridad



El talento, tan importante como el conocimiento

De todo este entorno surge una importante cuestión: ¿existe un número adecuado de profesionales con talento capaces de hacer frente a los desafíos de la ciberseguridad? En la encuesta internacional, los CEOs que se declararon no preparados ante un incidente de cibersguridad se mostraron más proclives a aumentar la plantilla en los próximos tres años y la mitad de ellos esperaba que en este periodo se hiciera sentir la escasez de profesionales cualificados.

Algunos estudios a nivel internacional estiman que el 23% de los puestos de trabajo en el área de ciberseguridad tardan más de seis meses en cubrirse y que otro 10% quedan vacantes. Según la Oficina de Estadísticas de Empleo estadounidense (Bureau of Labour Statistics), en agosto de 2015 existían unas 300.000 vacantes en el área de ciberseguridad en el país. Esta escasez se agrava aún más en el caso de que, a la búsqueda de características técnicas, se añadan otras como habilidades en el ámbito empresarial, de gestión, de riesgos o de ciencias sociales.

En general, encontrar buenos profesionales para el área de TI es complicado, asegura Marc Martínez, y especialmente para proyectos en los que se trabaje con la experiencia del cliente. "Todo el mundo comprende que es necesario tener a expertos en seguridad en el back-end", señala, "pero, para desarrollar nuevos productos, incorporar nuevas tecnologías y entrar en otros mercados con un elevado nivel de confianza hay que contar con buenos profesionales desde el comienzo de los proyectos, que trabajen con los diseñadores y los profesionales de Marketing. Las empresas necesitan de talento que garantice una agradable experiencia de cliente y que evite una ***ciberpesadilla***".

El directivo cibernético con conocimientos empresariales

Otra de las preguntas que se plantean es: ¿quién ha de ser el responsable en última instancia de la ciberseguridad dentro de la organización? En la encuesta a nivel internacional, cuatro de cada diez CEOs aseguraron que esperaban que la función del CIO (máximo responsable de TI) adquiriera más importancia en los próximos años, un porcentaje que se eleva al 54% en el caso español. No obstante, la realidad es que muchos CIOs no forman parte del equipo de alta dirección ni son respetados como interlocutores de negocio.

Además, trasladar toda la responsabilidad al CIO tiene sus desventajas, pues se corre el riesgo de que el resto de la organización se desentienda y no se integren los principios de la ciberseguridad en el conjunto de conductas y procesos de la organización.

Para Marshall, es necesaria una implicación que vaya más allá. "Recomendaría que algún miembro del consejo de administración y un alto directivo que no sea el CIO asuman también responsabilidades, en concreto, la de supervisar cómo se integra la ciberseguridad en el negocio, tanto desde la perspectiva de los riesgos como de las oportunidades", apunta. Así, el mensaje que se lanza a la organización es que la seguridad no solo es responsabilidad del departamento de TI.

En muchas empresas bien gestionadas existe la figura del CISO o *Chief Information Security Officer*, máximo responsable de seguridad de la información y que suele reportar al CIO. No obstante, a medida que las empresas asumen que la ciberseguridad es un riesgo empresarial que podría afectar al conjunto de la empresa, surgen otras alternativas. Algunos CISOs están empezando a reportar a otros altos cargos, como el COO (director de operaciones), el CFO (director financiero), el director jurídico o incluso el CEO. Toda empresa que reconozca que existen riesgos en ciberseguridad en fusiones y adquisiciones, así como en el diseño de productos, tendrá claro que la responsabilidad debería recaer en la alta dirección.

Obviamente, la estructura jerárquica es solo uno de los ámbitos que hay que trabajar para conseguir que la empresa tenga un perfil de ciberseguridad sólido. Por su puesto, esto también dependerá del perfil de las personas que ocupen esos cargos. "Es un tema demasiado importante como para no dejarlo en manos de un experto", comenta Marshall. "No obstante, si el CISO tiene importantes dotes de liderazgo, de modo que pueda inspirar y dirigir a expertos en la materia con gran talento, no es necesario que él mismo sea un experto en seguridad", apunta.

"El CISO debería poder mantener un diálogo fluido con la alta dirección y con el consejo de administración", indica Marc Martínez, "Son demasiados los CISOs que intentan trasladar los matices de los riesgos tecnológicos sin éxito ante un público con un perfil distinto al suyo que no comprende la jerga técnica. "La conversación es mucho más eficaz si la persona que lidera el área de ciberseguridad habla de los riesgos empresariales como una implicación de los ciberriesgos", matiza.

Las herramientas adecuadas

Además de en las personas adecuadas, las organizaciones deben invertir en las herramientas precisas. Lo primero será detectar si la organización está siendo atacada, pues, sin este diagnóstico, es imposible conocer si existen deficiencias en la seguridad o debilidades en la infraestructura. Muchas organizaciones han estado en peligro durante años y solo han sido conscientes de ello tras sufrir un daño concreto.

Una forma de ampliar el expertise de la empresa es utilizar lo que se conoce como *security intelligence* (inteligencia de seguridad) para detectar problemas, anomalías o actividades inusuales o sospechosas. La inteligencia puede ayudar en dos sentidos. En primer lugar, puede contribuir a establecer un servicio de alerta temprana para reducir el intervalo de amenaza de la vulnerabilidad (el tiempo que transcurre entre detectar y subsanar un ataque). En segundo lugar, a obtener una visión conjunta de las amenazas globales más allá de lo que una organización puede detectar por sí misma. La ciberseguridad es un ecosistema y las organizaciones deben conocer qué está ocurriendo tanto en el interior como en el exterior de su compañía.

Intercambio de inteligencia sobre amenazas

Las organizaciones pueden ampliar los datos de su propio sistema de inteligencia compartiendo información sobre las amenazas que les afectan con sus homólogos y competidores. Aunque en la teoría esta idea funciona, la realidad es que muchas empresas no están dispuestas a intercambiar información con sus competidores o a hacer públicas sus debilidades y fallos a no ser que la ley les obligue.

El sector financiero es, sin duda, una excepción: sus infraestructuras están tan interconectadas que las entidades tienden a actuar basándose en la idea de que todas en conjunto se hundirán o sobrevivirán si llega un ataque.

No obstante, no son muchos los sectores que se basan en la cultura del compartir.

Otro de los enfoques para abordar esta necesidad es crear redes de colaboración que ofrezcan, por ejemplo, recompensas a piratas informáticos "de sombrero blanco" (piratas informáticos que utilizan su poder para hacer el bien, no el mal) para que ayuden a encontrar debilidades en la arquitectura. Los directivos que los contratan suelen sorprenderse por la velocidad (a menudo es cuestión de minutos) a la consiguen infiltrarse en sus sistemas.

No obstante, la cobertura en seguridad nunca puede ser completa. Las organizaciones tienen que desarrollar un enfoque proactivo y predictivo respecto a la ciberseguridad, en lugar de confiar demasiado en tecnologías reactivas como los cortafuegos o la prevención de intrusiones. Comprobar constantemente los puntos débiles es una forma de adelantarse a los malhechores. Comprender el entorno de amenazas y conocer al enemigo gracias a la inteligencia sobre seguridad es otro método. Lo que no puedes prevenir, deberías poder detectarlo. Y, ante lo que no puedes detectar, deberías estar preparado para responder rápidamente. Esa es la máxima.

Las cuatro reglas de oro de la ciberseguridad

Lo básico primero

Más del 75% de los ataques aprovechan fallos de seguridad básicos que podrían prevenirse con medidas muy sencillas.

Cuida las joyas de la corona

Es preciso priorizar la inversión en defensa, así que conviene construir una fortaleza en torno a los activos más preciados.

Haz los deberes y conoce al enemigo

Es importante invertir en comprender quién podría atacarte, por qué y cómo para poder anticiparse a los escenarios más probables y defender los activos que tienen más probabilidades de ser atacados.

Trata los ciberriesgos como una oportunidad para examinar detenidamente el negocio.

La seguridad y la resiliencia pueden afectar a prácticamente el conjunto de la organización. Las estrategias para proteger la seguridad de las Tecnologías de la Información y la resiliencia de la empresa deberían estar en consonancia con las metas más generales de la organización: desde proteger la propiedad intelectual hasta maximizar la productividad, pasando por encontrar nuevas formas de satisfacer a los clientes.

Las empresas más innovadoras han reconocido que la ciberseguridad es una experiencia más del cliente y una oportunidad de obtener ingresos, no solo un riesgo que debe gestionarse. Para ellas, alcanzar un alto grado de preparación, integrando la seguridad en los nuevos productos a través de la fase de diseño, es contemplado como una ventaja competitiva, nunca como un coste. Asimismo, entienden que la ciberseguridad no es una cuestión que compete solo al área de TI, sino que debe abordarse en toda la organización y como un ecosistema.

Metodología

Los datos publicados en este informe se basan en una encuesta realizada a 1.276 altos directivos de España, Australia, China, Francia, Alemania, India, Italia, Japón, Reino Unido y Estados Unidos. Están representados nueve sectores de actividad clave: automoción, banca, seguros, gestión de activos, inversiones, sanidad, tecnología, mercados de consumo/minoristas y energía/utilities. En total, 347 CEOs proceden de empresas con ingresos de entre 500 y 999 millones de dólares, 626 de empresas con ingresos de entre 1.000 y 9.900 millones de dólares y 303 de empresas con ingresos iguales o superiores a los 10.000 millones de dólares y 303 de empresas con ingresos iguales o superiores a 10.000 millones de USD. La encuesta se realizó entre los meses de abril y mayo de 2015.

Los datos relativos a España reflejan la opinión de 50 CEOs de grandes empresas de los sectores de banca, seguros, automoción, manufacturas, tecnología, consumo y retail, sanidad, energía y gestión de activos. De estos, el 20% son CEOs de empresas con una facturación de entre 500 y 999 millones de euros, el 40% de entre 1.000 y 9.900 y otro 40% a partir de 10.000 millones.

Contacto

Marc Martínez
Socio responsable de Ciberseguridad de KPMG en España
T: +34 91 451 31 39
E: marcmartinez@kpmg.es

Javier Santos
Director de Ciberseguridad de KPMG en España
T: +34 91 456 59 04
E: javiersantos@kpmg.es

kpmg.es