



Riesgos Globales de Seguridad de TI

Kaspersky Lab aprovecha su amplia experiencia enfrentando los riesgos de seguridad TI, el malware y las vulnerabilidades para proteger a sus clientes de la mejor manera posible. A fin de garantizar la protección más eficaz para las empresas, es importante entender lo que los administradores de tecnología de la información (TI) piensan acerca de la seguridad, cómo se enfrentan a diversos problemas y cuáles son sus principales preocupaciones. Con el fin de lograr un mejor conocimiento, nos comunicamos activamente con nuestros clientes y socios, y alineamos nuestra estrategia considerando sus comentarios. Esto nos ayuda mucho en el desarrollo de las mejores soluciones de seguridad para empresas de todos los tamaños y sectores. A fin de estudiar con mayor profundidad las necesidades de las empresas, realizamos una investigación global que abarca diversos aspectos de la seguridad informática.

La investigación fue realizada en colaboración con B2B International, una de las agencias de investigación líder a nivel mundial y con la participación de más de 1,300 profesionales de TI en 11 países. Todos ellos influyen en las políticas de TI y participan en la evaluación de riesgos de seguridad. El estudio abarca empresas de todos tamaños, desde pequeñas (de 10 a 99 personas) a medianas (100-999 personas), y grandes (más de 1000 personas). Se cubrió una amplia gama de temas relacionados con la seguridad informática, incluyendo los riesgos de negocios en general, las medidas adoptadas para proteger el negocio, y los incidentes que han ocurrido.



Índice

Principales hallazgos.....	3
La seguridad TI es la mayor preocupación.....	3
Principal amenaza externa: el malware.....	3
Precaución ante nuevos medios.....	3
El crecimiento de la movilidad laboral es el siguiente reto.....	3
Rechazo a la adopción de nuevas tecnologías.....	3
La protección anti-malware es una necesidad.....	4
Enfoques proactivos y reactivos a amenazas de seguridad.....	4
Mayor inversión en seguridad TI como parte de la solución.....	4
Resumen detallado.....	5
Detalles del estudio.....	5
TI es una de las cuatro principales preocupaciones estratégicas.....	6
Principales preocupaciones del personal de TI.....	7
Futuros riesgos.....	8
Preocupaciones específicas de TI por región.....	9
Aumento significativo en el número de ataques cibernéticos.....	10
Mayor peligro para países en desarrollo y grandes empresas.....	11
Inversión anual promedio en seguridad TI.....	12
Se requiere mayor inversión.....	13
Preparación ante los diferentes riesgos de negocio.....	14
Siete principales medidas adoptadas para evitar riesgos de seguridad.....	15
Actividades prohibidas y restringidas al usuario.....	16
Restricciones por país y por tipo de economía.....	17
Tipos de amenazas externas experimentadas.....	18
Pérdida de datos experimentada.....	19
Conocimiento de amenazas externas específicas.....	20
Conclusión y recomendaciones.....	21
Recomendaciones de Kaspersky Lab.....	21

Principales hallazgos

La seguridad TI es la mayor preocupación

La estrategia de TI es una de las principales preocupaciones para las empresas, incluso calificada más alto que las preocupaciones financieras, de mercadeo y de recursos humanos. Casi la mitad de las organizaciones consideran a las amenazas informáticas como uno de los tres principales riesgos en desarrollo. Las violaciones a la seguridad TI también pueden ser la causa de grandes riesgos para un negocio. Estos incluyen daños a las marcas, el espionaje y el robo de la propiedad intelectual. Mientras tanto, las empresas de todos los tamaños tienen que lidiar con un número cada vez mayor de dispositivos habilitados para Internet, donde la mayoría de los "endpoints" están conectados a Internet, especialmente en las grandes corporaciones. Las tres cuartas partes de todas las empresas a nivel mundial esperan un incremento en el número de dispositivos para los próximos 12 meses.

Un número significativo de empresas ya han sido víctimas de delitos cibernéticos, incluyendo ataques dirigidos, eventos de espionaje industrial y pérdida de propiedad intelectual confidencial. Esto a su vez conduce a la conclusión de que las amenazas informáticas son ahora mucho más importantes para los negocios, lo cual fue confirmado por el 46 por ciento de las organizaciones.

59 por ciento de las empresas informaron que están, como mínimo, "bien equipadas" contra las amenazas cibernéticas. Sin embargo, las pequeñas empresas indican un menor nivel de confianza. Casi la mitad de las organizaciones han experimentado un aumento en el número de ciberataques en su contra en los últimos 12 meses. Las empresas están preocupadas de que los ataques cibernéticos pueden estar vinculados con el crimen organizado y están preocupados por la interferencia del gobierno. Como resultado de ello, la prevención de las violaciones de seguridad TI fue la preocupación número 1 del personal de TI en todas las regiones.

Principal amenaza externa: el malware

En los últimos 12 meses el 91 por ciento de las empresas han experimentado al menos un evento de seguridad TI proveniente de una fuente externa. Las amenazas más comunes son los virus, spyware y otros programas maliciosos. El 31 por ciento de los ataques de malware resultaron en algún tipo de pérdida de datos, con el 10 por ciento de empresas reportando pérdida de datos corporativos confidenciales. El segundo accidente más frecuente es la intrusión en la red; el 44 por ciento de las empresas encuestadas experimentaron un problema de seguridad relacionado con las vulnerabilidades en el software existente. El 18 por ciento de las organizaciones también informó de las fugas intencionales o datos compartidos por el personal. La pérdida de datos confidenciales se produjo en casi la mitad de estos casos.

Las violaciones a la seguridad dan como resultado la pérdida de datos financieros en la mayoría de los casos, seguida de la información personal de clientes, la propiedad intelectual y la información de los empleados. Los niveles de pérdida de datos confidenciales son mucho más altos en los mercados en desarrollo. Por ejemplo, 12 por ciento de las empresas experimentaron una pérdida de información de pagos, pero en los mercados emergentes, el 19 por ciento de las organizaciones informaron sobre este tipo de incidentes. Mientras que el malware ha demostrado ser el arma más eficaz de los cibercriminales, las cinco principales amenazas a la seguridad están todas relacionadas con la seguridad TI, superando los delitos "tradicionales" como el robo de hardware.

Precaución ante nuevos medios

Debido a la falta de conocimiento sobre las amenazas de seguridad TI entre los usuarios finales, las empresas limitan las actividades de estos de alguna manera. Así, el 57 por ciento de las organizaciones estuvieron de acuerdo en que el uso de medios de comunicación social por parte de los empleados representa un riesgo significativo. El 53 por ciento de las empresas han prohibido este tipo de servicios entre los usuarios finales y un 19 por ciento adicional han restringido el acceso de alguna manera. Las redes sociales son la segunda actividad más restringida, siendo el intercambio de archivos el más restringido. En tercer lugar está el vídeo streaming, seguido por los mensajes instantáneos, correo electrónico personal y servicios de Voz sobre IP (VoIP por sus siglas en inglés). Las restricciones se aplican con mayor frecuencia en las grandes corporaciones. El intercambio de archivos y el uso de redes sociales también son considerados por el personal TI como las actividades potencialmente más peligrosas que realizan los usuarios finales.

El crecimiento de la movilidad laboral es el siguiente reto

La seguridad de los dispositivos móviles es un tema nuevo para las empresas; El 55 por ciento de éstas informaron que están mucho más preocupadas por este tema respecto al año anterior. De hecho, alrededor de un tercio de la fuerza laboral ha estado "móvil" desde hace algún tiempo. Sin embargo, sólo el 36 por ciento de las empresas tienen implementada una política completa para lidiar con la seguridad fuera de sus instalaciones. Sólo el 30 por ciento tienen políticas específicamente para los dispositivos móviles, y un número aún menor exige la encriptación de los datos móviles. Las empresas que han tomado las medidas mencionadas, las evalúan como las menos efectivas. No es de extrañar que un tercio de las empresas piense que la computación móvil es demasiado arriesgada como para adoptarla. No hay duda de que el número de personal con servicios móviles se incrementará, por lo que los dispositivos móviles deben ser vigilados bajo las mismas políticas de seguridad y soluciones que las PC tradicionales.

Rechazo a la adopción de nuevas tecnologías

Las nuevas tecnologías emergentes, tales como servicios basados en la nube son evaluadas como una posible fuente de nuevos riesgos de seguridad. El 42 por ciento de las empresas en ocasiones se muestran reacias a adoptar nuevas tecnologías debido a los riesgos que éstas implican. El "Software-as-a-Service" (SaaS), un paradigma que forma parte de la nueva tendencia de migrar a la nube, se considera como una oportunidad en términos de seguridad por el 38 por ciento de las empresas. Las compañías ven esto como una posible y efectiva manera de "subcontratar" los problemas de seguridad al proveedor del servicio. Sin embargo, algunos piensan que la computación en la nube es más que nada una amenaza. Otros no están seguros y la ven como una oportunidad y una amenaza a la vez. El número de empresas que no confían en proveedores de SaaS con la seguridad de sus datos sigue siendo alta (38 por ciento). La implementación de soluciones SaaS no significa cancelar la seguridad interna. Para los cibercriminales el lugar de donde roban sus datos no implica mayores diferencias, ya sea en la infraestructura local o de la nube. Las técnicas criminales son principalmente las mismas en ambos casos.

La protección anti-malware es una necesidad

La protección contra el malware es la medida de mayor implementación entre las organizaciones de todo el mundo. Se coloca entre las cuatro medidas básicas y es tomada por dos tercios de todas las empresas.

- Anti-malware
- Firewalls del cliente
- Respaldo de datos
- Administración de parche / actualización

Sin embargo, sólo el 70 por ciento de las compañías han implementado una protección anti-malware en toda la empresa, y 3 por ciento no tiene protección alguna. El nivel de implementación

de anti-malware varía de país a país. En los mercados emergentes el 65 por ciento de las empresas lo han adoptado, mientras que el Reino Unido y los EE.UU. muestran un 92 y 82 por ciento en los niveles de ejecución, respectivamente. Otra característica clave de la protección anti-malware es que las empresas de todos los tamaños tienden a ponerla en práctica. También es vista como la medida más eficaz junto con la copia de seguridad de datos. Dado el número de incidentes relacionados con el malware, la protección del negocio de esta amenaza es absolutamente necesaria.

Enfoques proactivos y reactivos a amenazas de seguridad

Tan sólo un poco más de la mitad de las empresas se auto-evaluaron como altamente organizadas y sistemáticas para hacerle frente a las amenazas a la seguridad TI. El 33 por ciento posee una actitud opuesta y fatalista, argumentando que muchos eventos de seguridad TI son imprevisibles y difíciles de prevenir. El 28 por ciento indicó una actitud un tanto complaciente. Para ellos, las violaciones a la seguridad TI son asuntos que le "suceden a los demás" y no a ellos mismos. El enfoque reactivo es más popular: empresas que invierten en seguridad TI sólo después de que se ha producido un incidente. La gestión de TI en las empresas que utilizan productos de Kaspersky Lab se inclina más a buscar las soluciones y tecnologías más novedosas. Pero, en general, este tipo de actitud no es lo normal. Utilizar las últimas tecnologías en seguridad TI es importante y se debe implementar protección en toda la empresa antes de que los datos confidenciales estén en peligro.

Mayor inversión en seguridad TI como parte de la solución

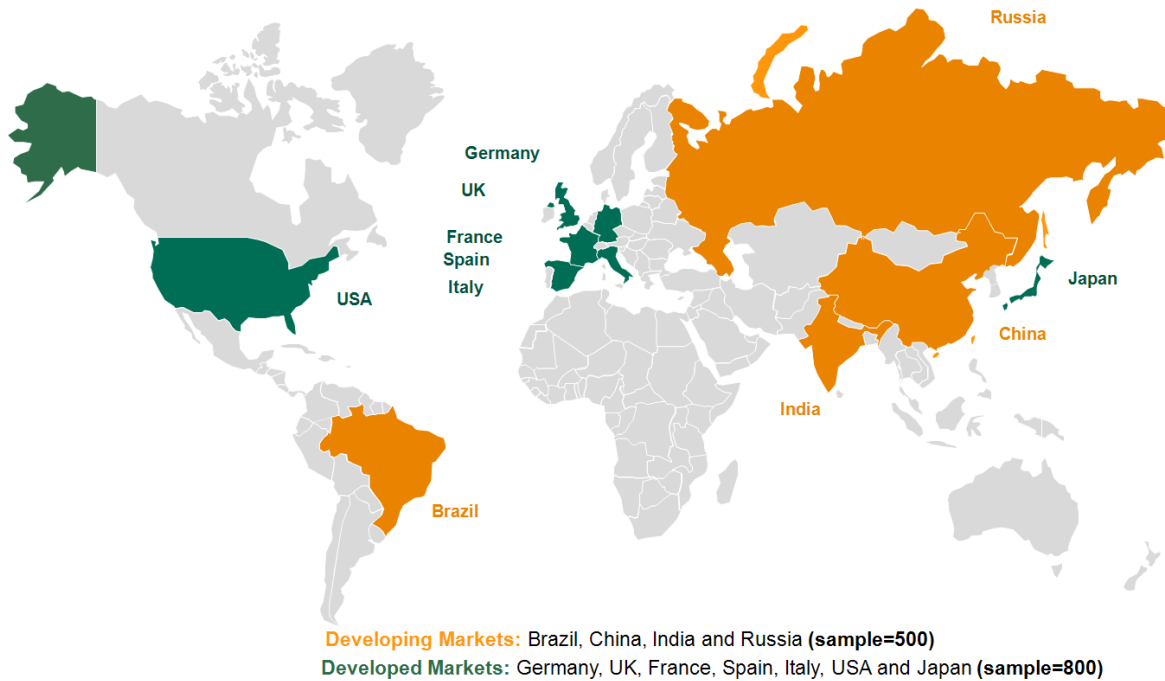
En la actualidad, la suma promedio reportada de las inversiones en seguridad TI es de USD \$7,870 o su equivalente para las pequeñas empresas, USD \$82,968 para las empresas medianas y USD \$3,290,130 millones para las grandes corporaciones. Sin embargo, la mayoría de las organizaciones piensan que un aumento del 25 por ciento o más en la inversión podría ser necesario. El 45 por ciento piensa que las actuales tasas de inversión son insuficientes. Más de dos tercios informaron insuficiencia de recursos en términos de personal, sistemas o conocimiento. El 48 por ciento mencionó las limitaciones presupuestarias como una barrera, y esta cifra es significativamente mayor en los países en desarrollo.

En general, la mayoría de las empresas considera que la inversión adicional en seguridad TI es dinero bien gastado (69 por ciento). Pero todavía hay un importante grado de desconocimiento o malinterpretación de la seguridad TI entre quienes se encargan de los presupuestos. El 34 por ciento de los representantes de las empresas cree que la alta dirección no ve la seguridad TI como un problema importante. Así mismo, hay señales de dificultad para explicar la importancia de la seguridad informática a los usuarios finales. Sólo el 42 por ciento de los encuestados reconoció que la mayoría de los empleados están preocupados por la seguridad TI. El mismo número de representantes piensa que los usuarios finales están bien informados sobre las amenazas de seguridad TI.

El estudio mostró un gran nivel de preocupación por la seguridad informática entre los gerentes de TI en todo tipo de empresas. A continuación puede encontrar los resultados detallados de la investigación de Kaspersky Lab y nuestras recomendaciones.

Resumen detallado

Detalles del estudio



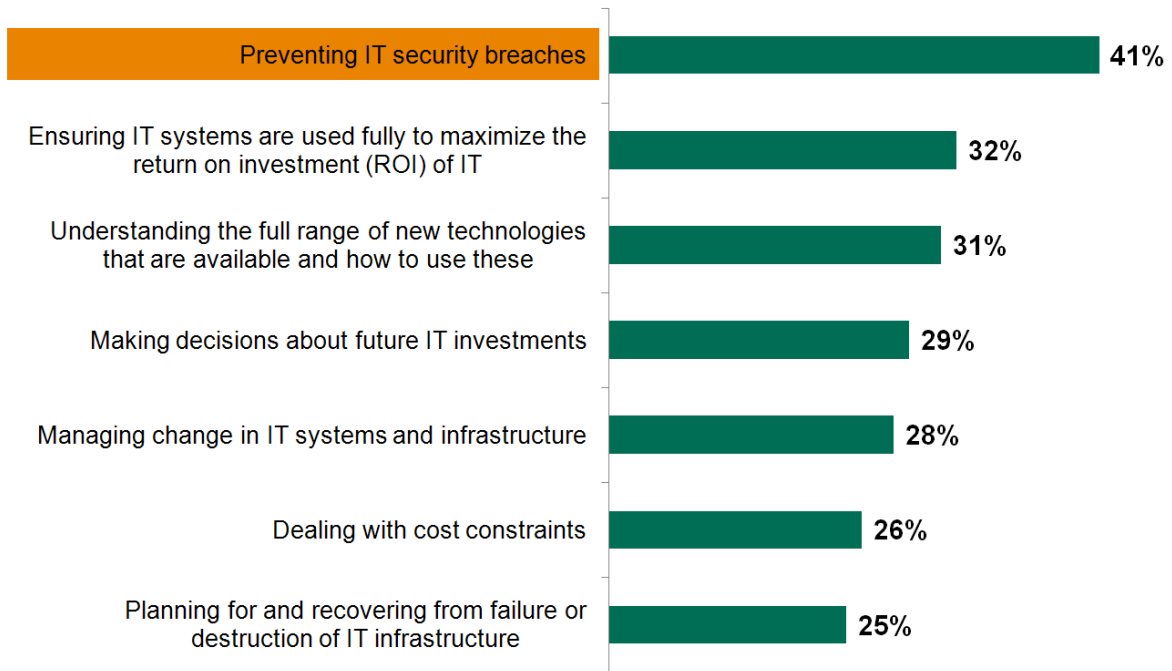
Más de 1,300 profesionales senior de TI de 11 países participaron en la encuesta. Todos los encuestados tienen influencia en la política de seguridad de TI, y un buen conocimiento tanto de los problemas de seguridad informática como con los asuntos generales de negocios (finanzas, recursos humanos, etc.). Geográficamente, la encuesta fue realizada en 11 países, incluyendo tanto a economías maduras como en desarrollo.

TI es una de las cuatro principales preocupaciones estratégicas



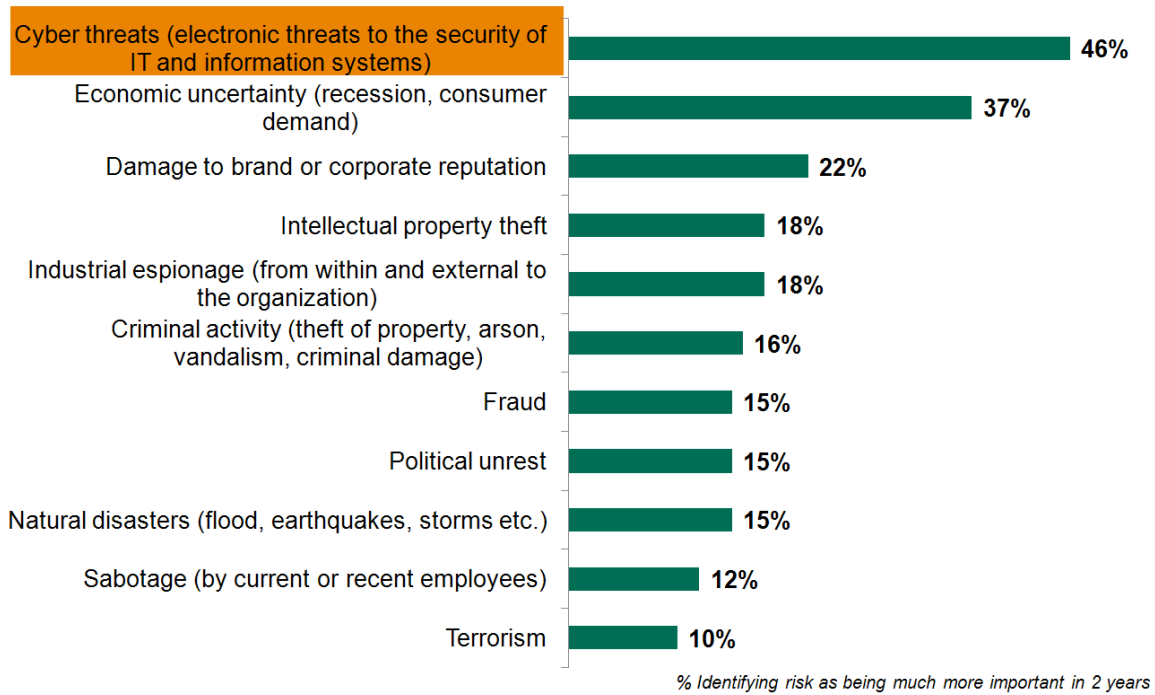
La estrategia de TI fue evaluada como una de las preocupaciones estratégicas más importantes para las empresas, junto con la de operaciones, desarrollo de nuevos productos y servicios, y la financiera.

Principales preocupaciones del personal de TI



Evitar violaciones a la seguridad es la principal preocupación de los profesionales de TI. Entender las nuevas tecnologías y encontrar posibles formas para implementarlas también se ubicaron entre las tres preocupaciones principales.

Futuros riesgos



Casi la mitad de las empresas ve a las amenazas cibernéticas como uno de los tres principales riesgos emergentes.

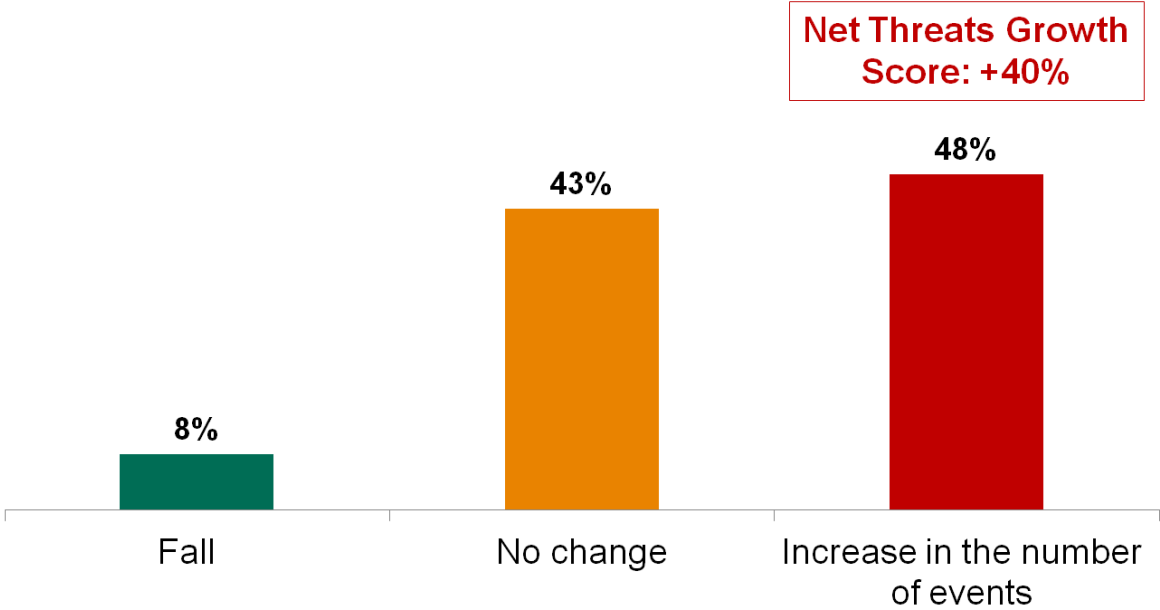
Preocupaciones específicas de TI por región

Issue	Total	Developing	Developed	Asia	Western Europe
Preventing IT security breaches	1	1	1	1	1
Ensuring IT systems are used fully to maximize the return on investment (ROI) of IT	2	3	3	3	3
Understanding the full range of new technologies that are available and how to use these	3	2	6	4	3
Making decisions about future IT investments	4	4	5	2	5
Managing change in IT systems and infrastructure	5	8	2	10	2
Dealing with cost constraints	6	10	4	5	8
Training users in how to use IT systems	7	5	8	8	5
Planning for and recovering from failure or destruction of IT infrastructure	7	7	7	8	5
Preventing misuse of computer systems by employees	9	6	9	7	9
Dealing with day-to-day unreliability of IT systems	10	8	10	6	10
Complying with industry regulations and standards	11	11	11	11	11

Table shows ranking of concerns of the IT function – Rank 1 indicates the issue selected by most respondents within a group

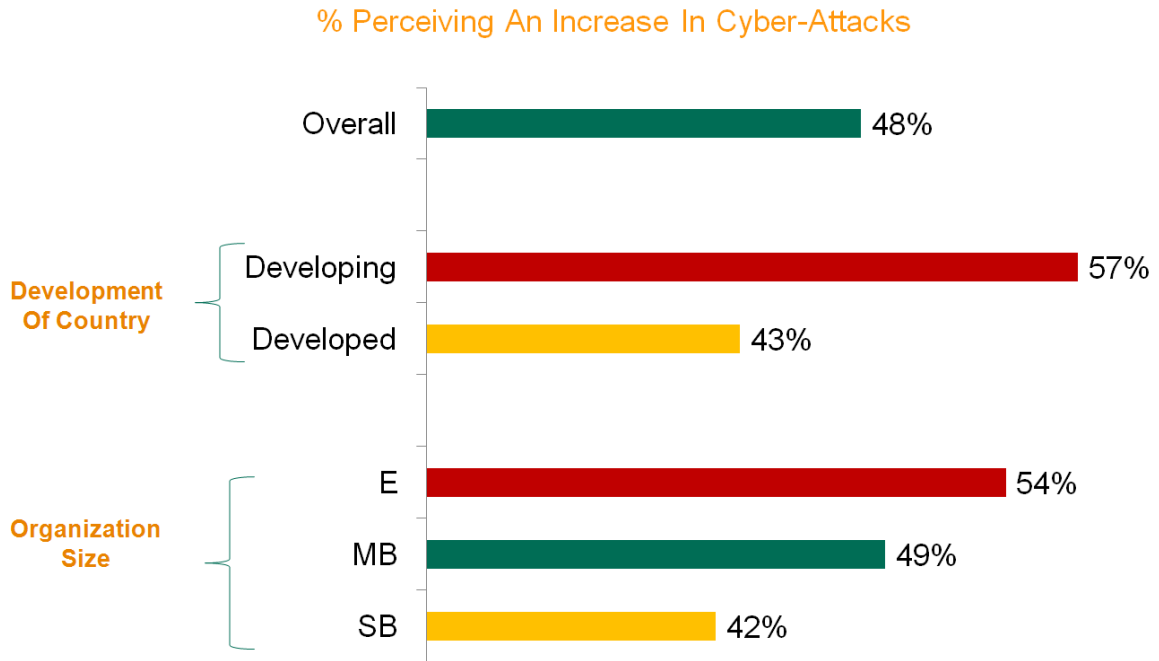
La prevención de las violaciones a la seguridad TI es la mayor preocupación en todos los países independientemente de la situación del mercado. Para otros problemas existen diferencias significativas entre los mercados emergentes y maduros. Por ejemplo, las limitaciones de costos son mucho más importantes en los países desarrollados. Al mismo tiempo, las empresas en los mercados emergentes prestan mayor atención a la capacitación de los usuarios finales en temas específicos de TI.

Aumento significativo en el número de ataques cibernéticos



Casi la mitad de los profesionales encuestados reportó un aumento en el número de accidentes de seguridad informática durante los últimos 12 meses. Por el contrario, sólo el 8 por ciento notó una disminución.

Mayor peligro para países en desarrollo y grandes empresas



Mientras que el 48 por ciento de las empresas reportó un aumento en el número de ataques cibernéticos, las cifras de los países en desarrollo y las grandes empresas son mucho más altas.

Inversión anual promedio en seguridad TI

Small Businesses

(10-99 Seats)

\$8,055

\$93/employee

Medium Businesses

(100-999 Seats)

\$83,200

\$167/employee

Enterprise Businesses

(1000+ Seats)

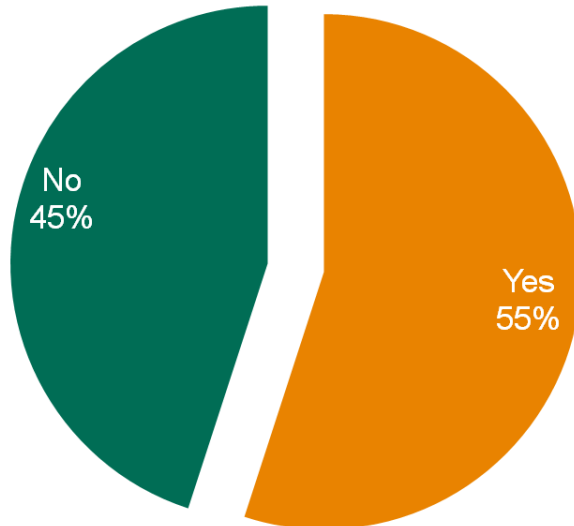
\$3,263,476

\$388/employee

La tasa de inversión en seguridad TI por empleado es más alta en las grandes empresas. La diferencia entre las pequeñas y medianas empresas es menos notable.

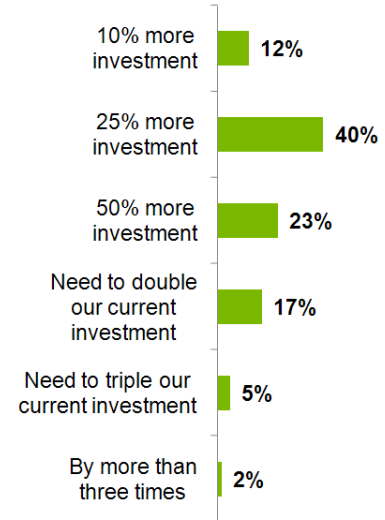
Se requiere mayor inversión

Adequate Investment In IT Security?



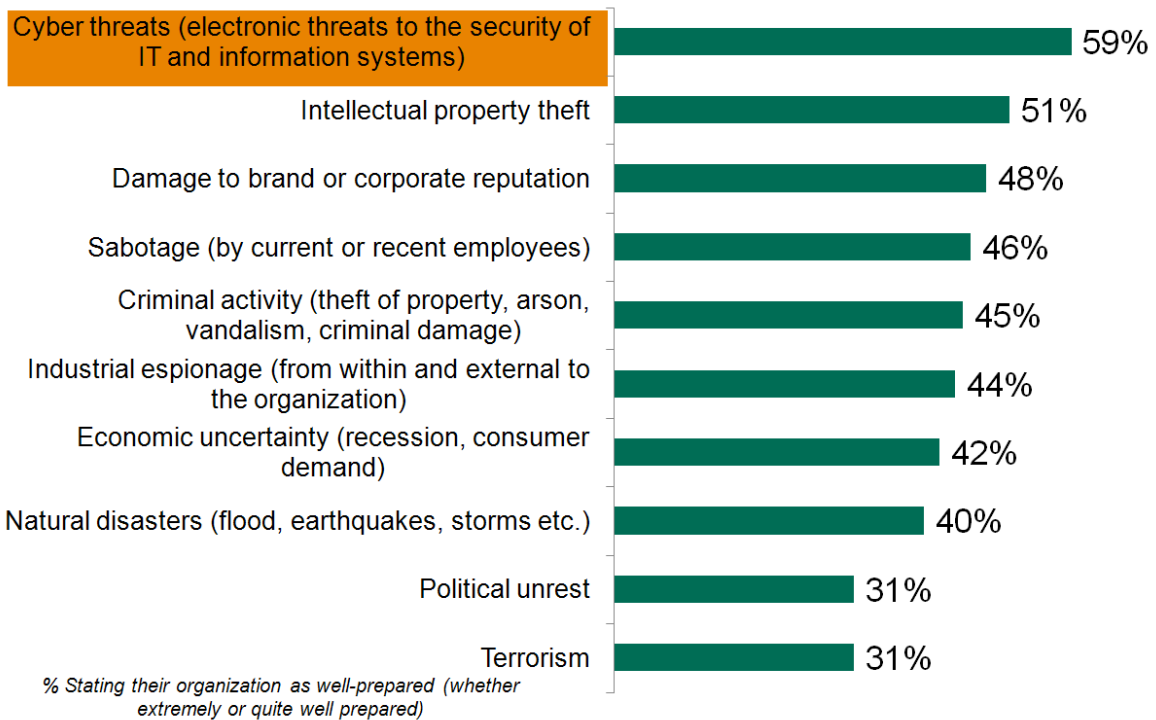
Additional Investment Required...

(Among those who feel current investment is inadequate)



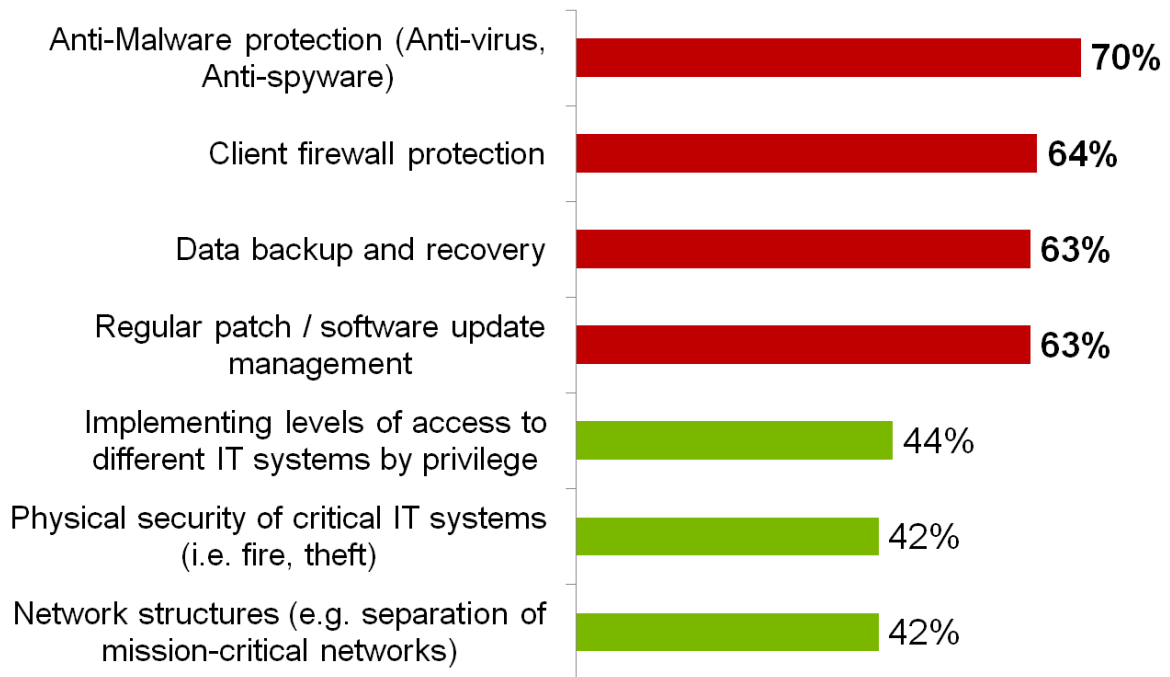
El 45 por ciento de las empresas no siente que la tasa actual de inversión en seguridad informática es suficiente. El 40 por ciento de los encuestados cree que un aumento del 25 por ciento en la inversión es necesario.

Preparación ante los diferentes riesgos de negocio



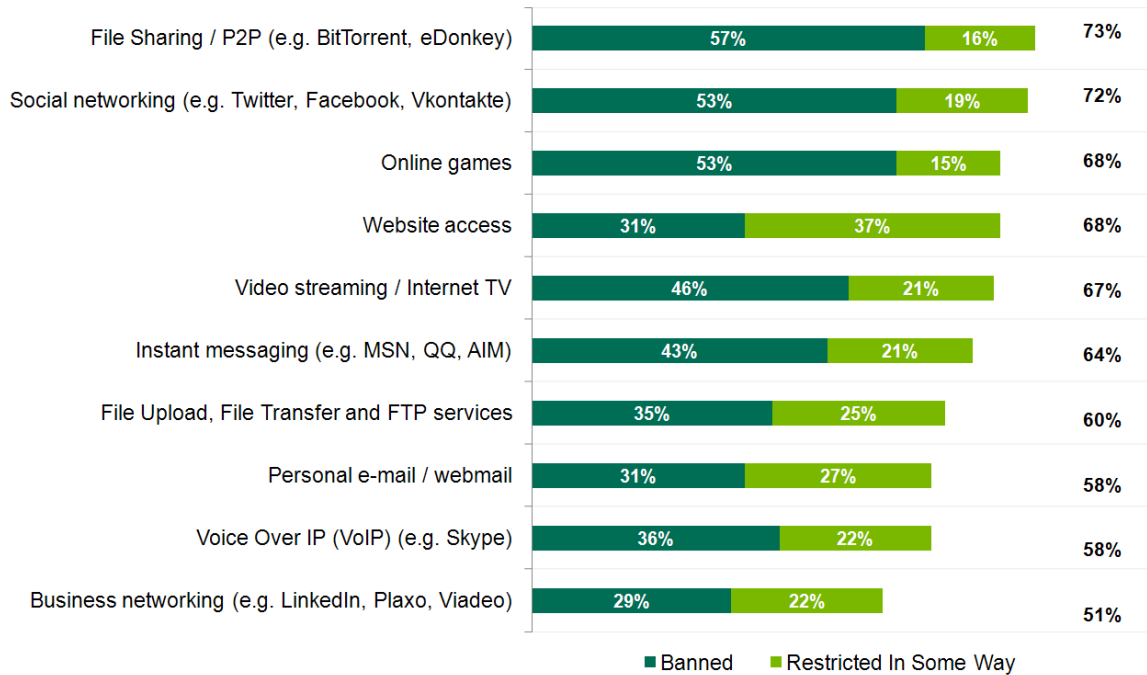
A pesar de que las amenazas cibernéticas son una de las principales preocupaciones para las empresas, sólo el 59 por ciento de las empresas sienten que están bien preparadas para ellas.

Siete principales medidas adoptadas para evitar riesgos de seguridad



La protección anti-malware es la medida de seguridad aplicada más extensamente. Sin embargo, no se ha implementado por completo en un 30 por ciento de las empresas, y 3 por ciento no tiene protección alguna. La protección firewall, el respaldo de datos y actualizaciones estándar del software también se aplican con bastante frecuencia.

Actividades prohibidas y restringidas al usuario



Las empresas son muy cautelosas sobre los nuevos medios. La mayoría de ellas prohíben o restringen el acceso a los sitios Web de las redes sociales de alguna manera. Si bien el intercambio de archivos aún es la actividad más restringida, las redes sociales superan incluso a los juegos en línea, mensajes instantáneos y la comunicación personal por correo electrónico.

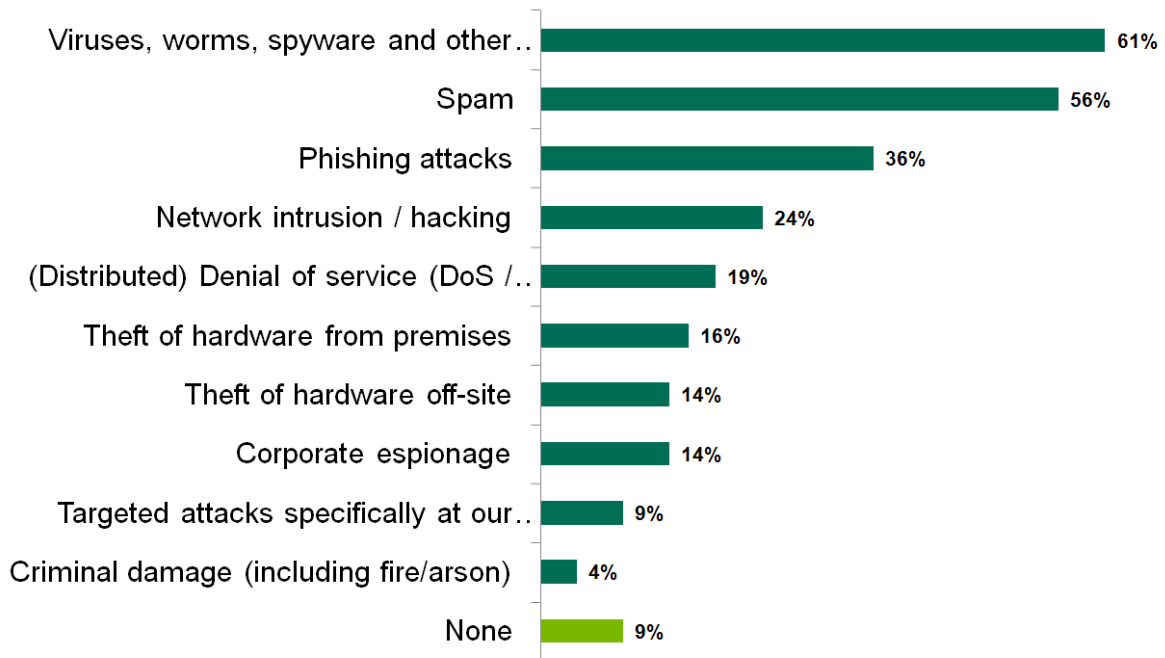
Restricciones por país y por tipo de economía

Activity / Application	Overall	Developing	Developed	United States	Russia	China	Brazil
File Sharing / P2P	55%	46%	61%	62%	50%	44%	50%
Social networking	35%	36%	35%	44%	52%	26%	41%
File Upload, File Transfer, FTP	34%	33%	34%	33%	44%	28%	38%
Website access	32%	30%	33%	35%	42%	29%	19%
Personal e-mail / webmail	31%	29%	32%	36%	22%	28%	32%
Instant messaging	23%	32%	18%	20%	19%	36%	35%
Online games	21%	21%	21%	19%	16%	21%	32%
Video streaming / Internet TV	13%	18%	10%	8%	12%	21%	14%
Business networking	11%	15%	9%	5%	4%	24%	7%
Voice Over IP (VoIP)	10%	14%	8%	5%	9%	17%	9%

Table shows the % of organizations identifying an application / activity as one of the greatest threats.

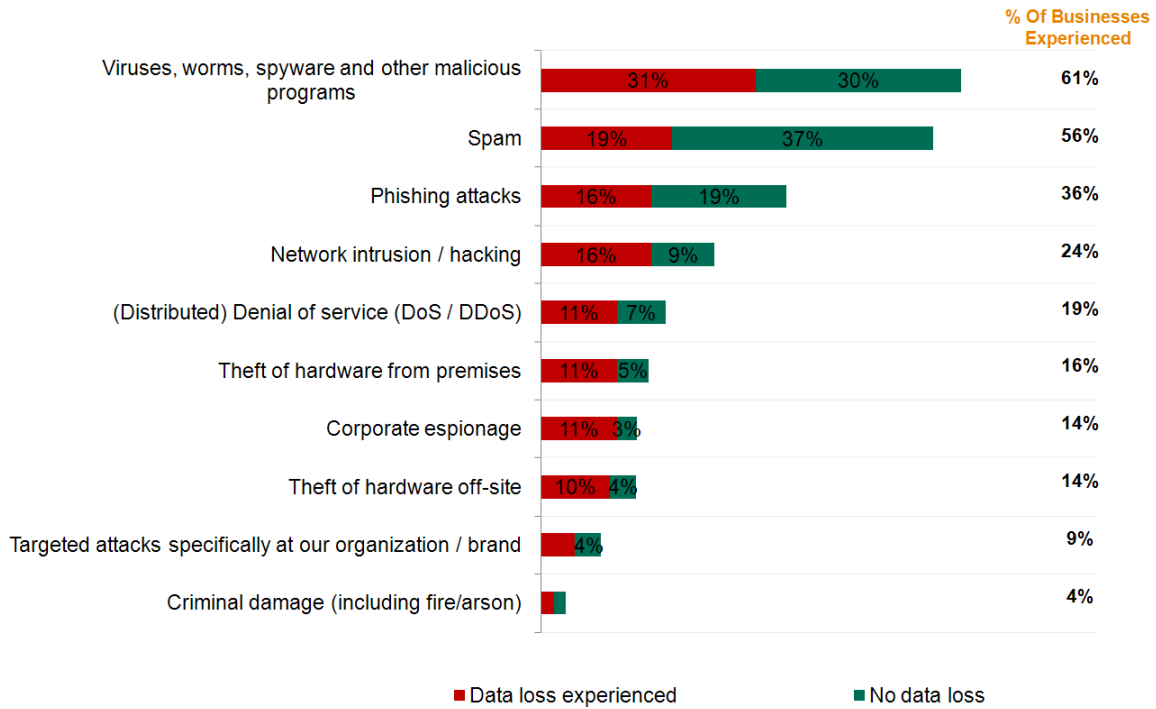
Las redes sociales son vistas como la segunda mayor amenaza mundial, especialmente en los EE.UU., Rusia y Brasil. Las empresas en países desarrollados prestan menor atención a la restricción de los mensajes instantáneos, aunque también puede convertirse en una amenaza a la seguridad.

Tipos de amenazas externas experimentadas



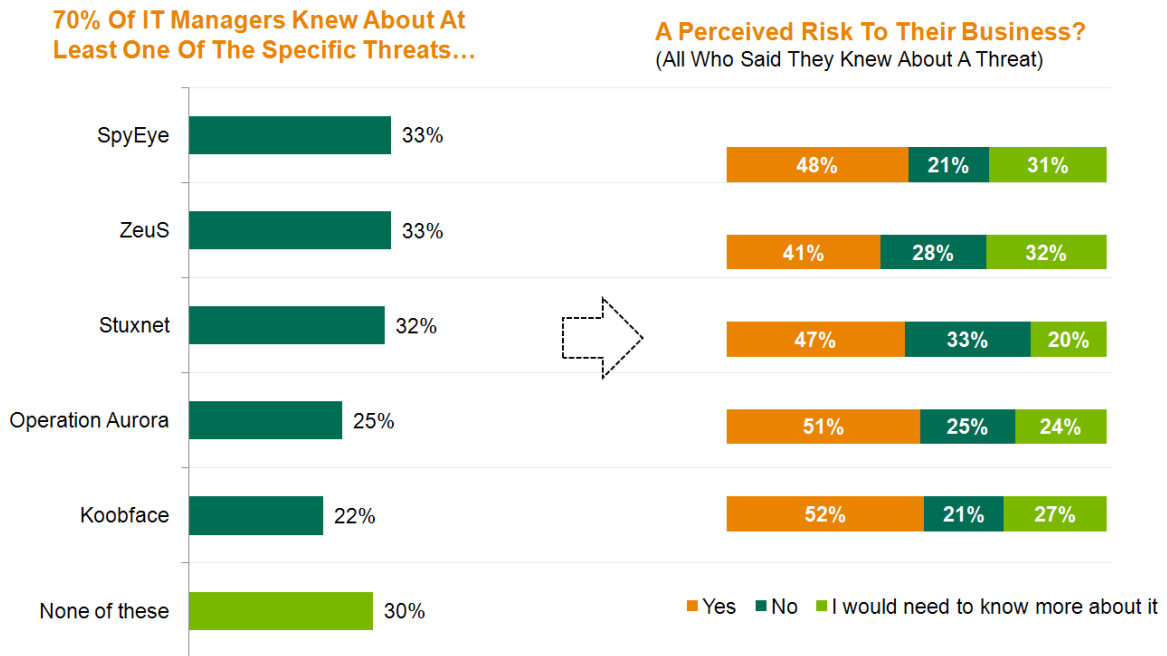
El malware es la causa más frecuente detrás de los incidentes de seguridad, superando al spam y a los ataques de phishing. Las cinco principales amenazas están relacionadas con la seguridad cibernética.

Pérdida de datos



El mayor número de incidentes de pérdida de datos también está relacionado con malware, y en el 31 por ciento de los casos la violación de la seguridad conduce a la pérdida de datos confidenciales.

Conocimiento de amenazas externas específicas



Entre las amenazas más identificadas están SpyEye, Zeus y Stuxnet. Sin embargo, sólo alrededor de la mitad de los encuestados piensa que estas amenazas ponen en peligro a su compañía.

Conclusión y recomendaciones

Entre las empresas de todos los tamaños en todo el mundo existe un buen nivel de conocimiento sobre las amenazas de seguridad TI y los riesgos correspondientes. Las amenazas cibernéticas son clasificadas como la preocupación de mayor crecimiento, confirmada por casi la mitad de los encuestados. Al mismo tiempo, una de cada dos empresas evalúa su presupuesto de seguridad TI como insuficiente, y considera necesario un aumento del 25 por ciento en la inversión. La protección anti-malware, siendo una parte esencial de la seguridad empresarial, se implementa en sólo el 70 por ciento de las organizaciones. Esto llevó a que la mayoría de las empresas experimentara una violación de seguridad TI en los últimos 12 meses, y casi un tercio de ellas perdió información de negocios.

Para evitar daños mayores a una compañía, es necesario implementar una seguridad TI sólida en todos los departamentos de la empresa y que abarque todos los endpoints. El número de amenazas cibernéticas, incluyendo los ataques dirigidos, puede conducir no sólo a la pérdida de datos confidenciales – la imagen de marca de una compañía también puede ser dañada, la cual es una importante amenaza para la mayoría de las empresas. Al menos la mitad de las compañías cree que hay más trabajo por hacer. Esto incluye el aumento del número de personal de seguridad TI, un incremento en el nivel de inversión y la aplicación de las más recientes soluciones y tecnologías para proteger el negocio de una empresa.

Recomendaciones de Kaspersky Lab

➤ **Elija una solución de seguridad que se adapte a su negocio**

La inversión en seguridad TI es importante, pero el presupuesto real siempre dependerá del tamaño de su empresa. Elija un producto que aborde todos los temas de seguridad y al mismo tiempo que se adapte perfectamente a su empresa en cuanto al número de endpoints, servidores, etc. También es necesario prepararse para el crecimiento de la empresa. Así, el producto de seguridad correcto debe ofrecerle una buena escalabilidad.

➤ **Invierta en la educación de los empleados**

En general, la seguridad TI en realidad depende de cuánto saben los usuarios finales acerca de las amenazas cibernéticas. Ellos no tienen que ser expertos, pero sería inteligente dedicar el tiempo y el presupuesto necesario para que aprendan más. Recuerde que los ataques dirigidos más dañinos no podrían llevarse a cabo sin la “ayuda” involuntaria de un empleado. En otras palabras, cuando el personal piense antes de abrir un archivo adjunto sospechoso en un correo electrónico, usted se habrá ahorrado una gran cantidad de dinero.

➤ **Asegúrese de tener protección anti-malware eficaz para todos los endpoints, incluyendo los dispositivos móviles**

Dado que el mayor número de incidentes están relacionados con el malware, la protección efectiva debe ser aplicada en todos los endpoints. Aunque la mayoría de las empresas ya utilizan algún tipo de solución anti-malware, no es común la protección de todas las áreas del negocio, dejando a algunos endpoints potencialmente vulnerables. Esta recomendación también aplica a los dispositivos móviles, los cuales cada vez más son puntos vulnerables. La solución más efectiva consiste en ampliar las políticas de seguridad de la compañía e introducir un control centralizado, así como la protección de malware para los smartphones de los empleados. También se recomienda proteger datos confidenciales en caso de pérdida o robo del dispositivo.

➤ **Establezca un sistema de gestión centralizada para todos los dispositivos de punto final**

El número de puntos finales crece rápidamente, por lo que es necesario contar con un sistema de gestión centralizada para controlar todos los dispositivos corporativos. Las pequeñas empresas no

suelen poner en práctica este sistema, y al mismo tiempo son las más vulnerables a las amenazas cibernéticas. Se recomienda el uso de soluciones especializadas para pequeñas empresas a fin de proteger y administrar los endpoints de la compañía en el caso de las pequeñas empresas.

➤ **Proteja la comunicación del usuario final en lugar de restringirlo**

Puede ser posible proteger la red corporativa contra las amenazas restringiendo aún más la actividad del usuario final. Pero es más eficaz proteger la comunicación del personal contra enlaces a sitios Web infectados y contra el phishing. Este tipo de protección debe abarcar los medios de comunicación más utilizados, incluyendo el correo electrónico y los mensajes instantáneos.