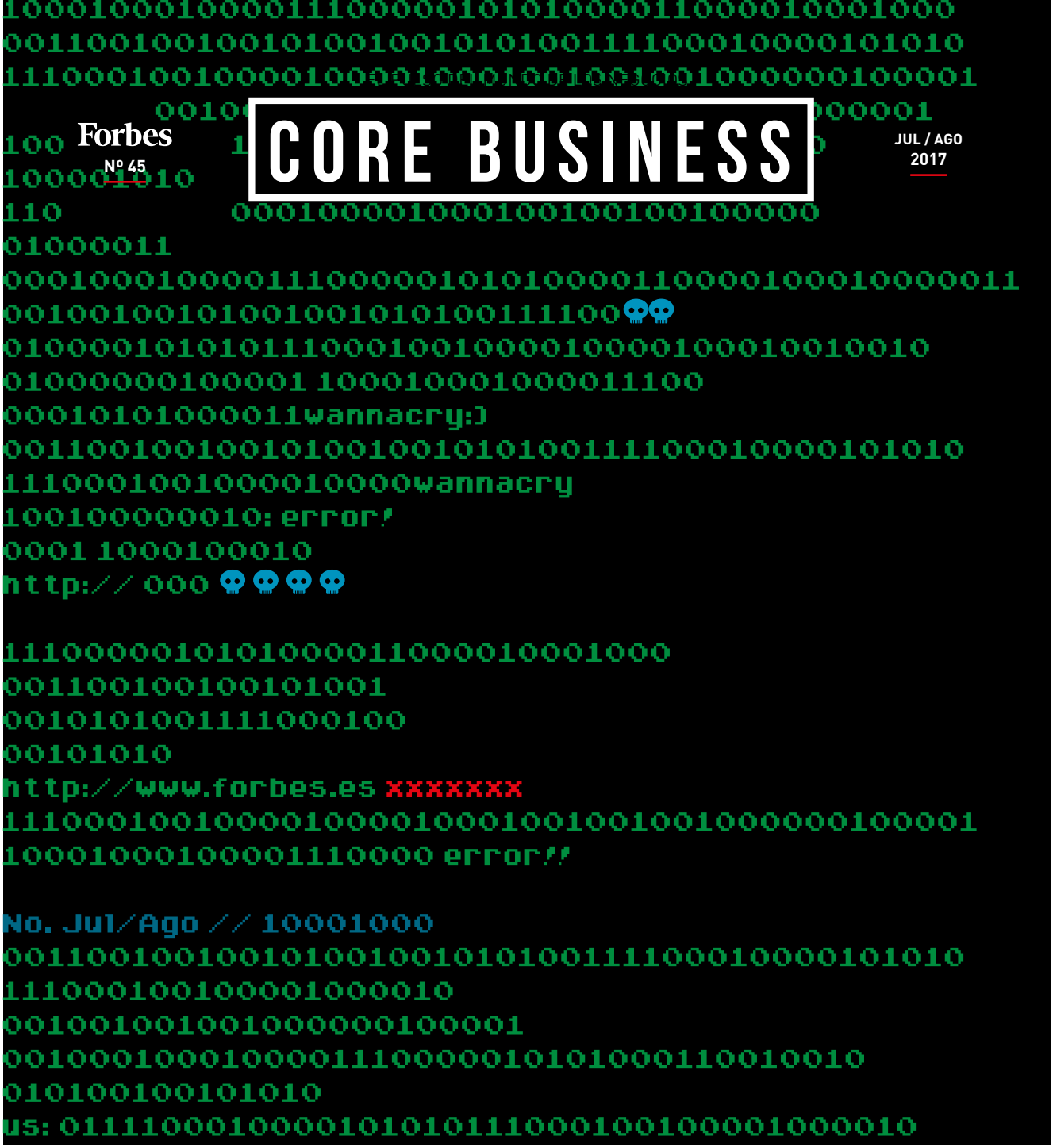


Un nuevo elemento de riesgo ha hecho aparición en la vida cotidiana para quedarse: los ciberataques. ¿Habrá que aprender a acostumbrarse a ellos?

EL ELEVADO COSTE DE LA CIBERDELINCUENCIA

LAS TECNOLOGÍAS DE LA INFORMACIÓN ESTÁN CAMBIANDO NUESTRAS VIDAS, PERO A MEDIDA QUE AUMENTA NUESTRA DEPENDENCIA DE ELLAS CRECEN LOS RIESGOS.

Los ciberataques son ya un riesgo real y tangible para empresas y personas, y protegerse de ellos mueve mucho dinero. Es incuestionable que la era tecnológica ha introducido profundas mejoras en la economía: no hay sector donde su aplicación no haya supuesto avances en la productividad; y en el ámbito del consumidor o del ciudadano han facilitado el →

ALFREDO **ARANDA**

LA COLABORACIÓN AYUDÓ A VENCER A WANNACRY

El ataque de WannaCry en España tuvo más éxito mediático que delictivo gracias a la rápida reacción de empresas e instituciones y a la colaboración desplegada, que contó también con la participación de los 'chicos buenos', según expertos informáticos. "La repercusión de dicho ataque fue mucho mayor que el impacto que tuvo, dada la forma de actuar del *malware*. La verdad es que las empresas e instituciones que fueron supuestamente atacadas reaccionaron adecuadamente y con celeridad. Es más, se coordinaron muy bien entre empresas y equipos, así como de hackers éticos españoles creando una atmósfera de colaboración sin precedentes", afirma a *Forbes* Daniel Solís, CEO de la empresa española de ciberseguridad Blueliv.

Según el Instituto Nacional de Ciberseguridad (Incibe), WannaCry afectó a menos de una decena de empresas y produjo entre 2.000 y 2.500 infecciones de las 360.000 a nivel mundial, unas cifras modestas si se compara con los 115.000 incidentes de ciberseguridad que resolvió el Instituto en 2016, de los cuales 479 tuvieron que ver con operadores estratégicos, y el resto con ciudadanos, empresas y red académica. "En lo que llevamos de 2017, hasta el 31 de abril, hemos resuelto más de 58.000 incidentes, de los cuales más de 330 tienen que ver con operadores estratégicos, y el resto, principalmente, con ciudadanos y empresas", afirma a *Forbes* Marcos Gómez, subdirector de servicios del Incibe. El Instituto calcula que el gasto en ciberseguridad en España podría ascender a unos 600 millones de euros, aunque advierte que la cifra hay que tomarla con cautela porque muchas empresas ocultan el dato. A nivel mundial podrían alcanzarse los 94.000 millones de euros en 2023.

El sector de la ciberseguridad en España incluye 533 empresas, en su mayor parte vinculadas a actividades informáticas, con un volumen de facturación de 600 millones de euros en 2014, según el Observatorio Nacional de las Telecomunicaciones. De entre la 500 empresas más innovadoras del mundo en ciberseguridad de la lista que elabora la firma estadounidense especializada en investigación Cibersecurity Ventures solo se incluye a tres españolas: Panda Security, Prot-On y Blueliv.

→ acceso a información, servicios y bienes prácticamente sin limitaciones espaciales. Pero este panorama casi paradisíaco gracias a las Tecnologías de la Información (TI) y a la velocidad con que se desarrollan y renuevan implica elevados riesgos y todos los riesgos también implican un coste. Las TI se revelan como imprescindibles hasta el punto que sería inimaginable vivir sin ellas, pero esta conclusión encierra el problema de la vulnerabilidad ante ataques de naturaleza indiscriminada o selectiva, de ejecución anónima y gran impacto económico, y que constituyen una de las principales amenazas a la economía mundial, según el World Economic Forum. Ningún estratega militar podría haber imaginado un arma tan poderosa, tan limpia, y de tan bajo presupuesto.

El reciente ataque global –de procedencia no aclarada todavía– de WannaCry, un virus del tipo *ransomware* que secuestra datos informáticos a cambio del pago de un rescate, golpeó a 360.000 equipos a nivel mundial, incluida España, según el Instituto Nacional de Ciberseguridad (Incibe), afectando fundamentalmente a empresas y a algunos servicios públicos, como al sanitario de Reino Unido. Los ataques cometidos por este tipo de virus extorsionadores no son nuevos: en los últimos cinco años se han multiplicado considerablemente, según la consultora internacional EY. Además de la alarma internacional, suscitó las inevitables preguntas sobre cuándo será el próximo y de qué virulencia será; si podrán evitarse los ataques y, en todo caso, si habrá que habituarse a vivir bajo una permanente vulnerabilidad tecnológica. Según Marc van Zadelhoff, director mundial de seguridad de IBM, sus clientes tienen que asumir que ya están siendo *hackeados*, "necesitamos vivir en permanente paranoia, y esperar lo peor permite tener un plan".

¿Deberemos acostumbrarnos a convivir con el cibercrimen? "Internet no es más que un reflejo de la sociedad y de la vida real, por lo que la respuesta es sí. Al igual que con la delincuencia fuera de internet, deberemos crear una cultura de ciberseguridad en cuanto a país, instituciones [y] países; y, ya bajando, a niveles familiares e individuales, de las personas. Lo que está claro es que el cibercrimen va a crecer y cada vez veremos mayor número de amenazas, más agresivas y efectivas", señala a *Forbes* Daniel Solís, CEO de la empresa española de ciberseguridad Blueliv. Por su parte, Ricardo Maté, Director General para España y Portugal de Sophos, otra empresa española de ciberseguridad, sostiene que "debemos reconocer la existencia y el impacto de la ciberdelincuencia, pero no acostumbrarnos a ella. El cibercrimen nos cuesta dinero, daña nuestra privacidad y potencialmente puede poner en riesgo vidas. Debemos estar preparados y motivados para luchar contra el cibercrimen como lo hacemos contra cualquier otro tipo de delitos".

Tanto los ciberdelincuentes como el sector de la ciberseguridad parecen participar de un mismo juego que les lleva a estar en continua renovación: los primeros para intentar burlar las últimas barreras y el segundo para actualizarlas continuamente. "La tecnología puede usarse –y se usa– desde ambos lados. Se parece al ajedrez: tienes que tratar de adivinar los siguientes movimientos del adversario. Los ciberdelincuentes siempre buscarán formas de saltarse las protecciones existentes y se van adaptando a las barreras que se encuentran, mientras que los fabricantes de seguridad tienen que estar preparados para los nuevos ataques que ideen los ciberdelincuentes cada vez que les impedimos el paso, señala a *Forbes* Rosa Díaz Moles, directora general de la firma de ciberseguridad Panda Security España.

Pese al impacto social y mediático que tienen los ataques globales como el acometido por WannaCry, la última encuesta anual (2017) que realizan la firma de gestión de recursos humanos Harvey Nash y la consultora internacional KPMG entre responsables tecnológicos a nivel mundial, ha revelado que el mayor incremento en términos de amenazas procede de los ataques dentro de la propia empresa (crecieron desde el 40% al 47% el año pasado). Los encuestados reconocieron que la atención a la vulnerabilidad y ciberseguridad se encuentra en cotas máximas, y un tercio de ellos afirmó que su organización ha sufrido un ciberataque importante en los últimos 24 meses, lo que resulta un incremento del 45% frente a 2013. "El ataque de WannaCry ha sido el mayor nunca visto en este tipo de virus (*ransomware*) y demuestra en tiempo real que está creciendo como problema a escala global y como un lucrativo negocio para los ciberdelincuentes", afirma Mike Fey, presidente de Symantec, una de las empresas de *software* más importantes del mundo, con sede en California, que en el último año declara haber identificado un incremento del 36% de ataques de estos virus.

LOS 'CHICOS MALOS' SE ADAPTAN A LAS BARRERAS QUE ENCUENTRAN Y LOS FABRICANTES HAN DE PREPARARSE PARA LOS NUEVOS ATAQUES QUE IDEEN

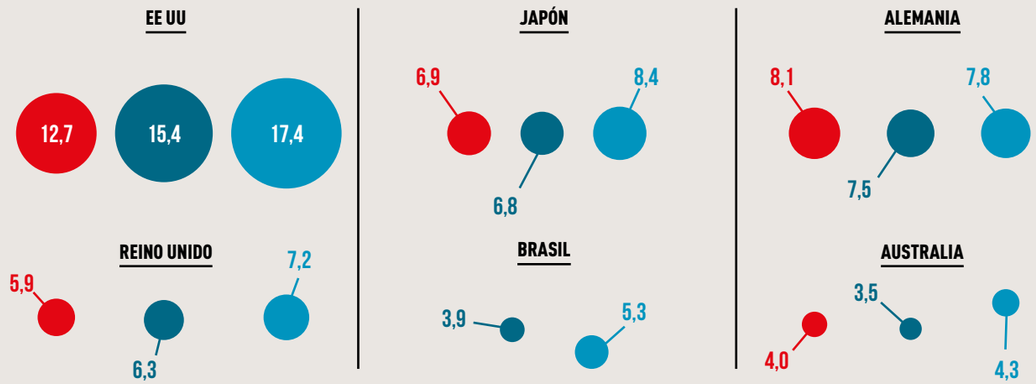
Los daños

Symantec asegura que la limpieza de los equipos atacados por WannaCry llevará meses y una factura multimillonaria, y que el rescate por víctima ha subido desde los 294 dólares (264 euros) en 2015 a alrededor de los 1.100 dólares (986 euros). Estimaciones del sector de la seguridad barajan que el impacto económico global de la acometida de WannaCry en los cuatro primeros días pudo ascender a miles de millones de dólares, incluyendo las pérdidas ocasionadas por la caída de los sistemas en grandes empresas e infraestructuras. "Es conocido que el WannaCry ha afectado a empresas españolas o que operan en nuestro país, entre ellas varias grandes firmas, pero un ataque de este tipo solo se puede analizar desde una óptica global. Los cibercriminales han logrado un amplio alcance: más de 170 países y más de 300.000 usuarios afectados, especialmente del ámbito empresarial, aunque también en el institucional. Esto es fruto de la sofisticación de WannaCry, que utiliza al menos 1.300 muestras de *malware* distintas para el cifrado de ficheros de diferentes extensiones. WannaCry escaneaba tanto la red interna de una empresa como la externa en busca de equipos no debidamente actualizados para infectarlos", dice Rosa Díaz.

La firma especializada en investigación de ciberseguridad Cibersecurity Ventures calcula en su último informe sobre el coste de los ataques informáticos que en 2017 los daños causados por los virus *ransomware* →

COSTE TOTAL DE LA CIBERDELINCUENCIA EN LOS PAÍSES INDICADOS

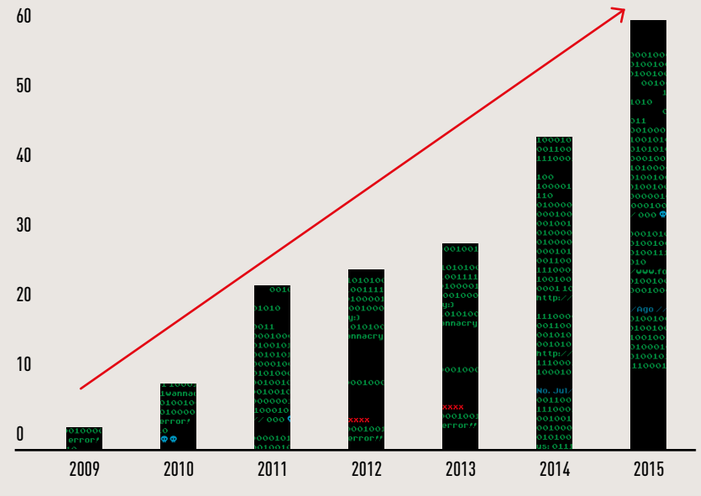
EN MILES DE MILLONES DE DÓLARES ● 2014 ● 2015 ● 2016



LA CIBERDELINCUENCIA SIGUE CRECIENDO A PESAR DEL AUMENTO DE LA INVERSIÓN EN PROTECCIÓN

● Nº TOTAL DE INCIDENTES

● INVERSIÓN EN TASA DE CRECIMIENTO ANUAL COMPUESTA



FUENTE **PONEMON INSTITUTE / PwC**

→ superarán los 5.000 millones de dólares (4.500 millones de euros) a nivel mundial, unas 15 veces más que hace dos años. "Los costes incluyen daños y destrucción (o pérdida) de datos, sistemas paralizados, productividad perdida, disrupción de la actividad empresarial tras el ataque, investigación forense, restauración y borrados de datos, daño reputacional y formación a los empleados para prepararlos ante nuevos ataques", señala. La compañía anticipa que las incursiones ganarán en virulencia y su incidencia podría cuadruplicarse en los sistemas hospitalarios para 2020.

Un negocio floreciente

La ciberdelincuencia es un negocio muy rentable. Según algunos estudios, el impacto del cibercrimen podría suponer ya entre un 0,6 y un 0,8% del PIB mundial, probablemente más que el del narcotráfico. "La magnitud del problema está todavía lejos de entenderse por una mayoría. No se está respondiendo ni con la celeridad ni la contundencia que se debe", afirmó Enrique Cubeiro Cabello, Jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa en un reciente encuentro sobre ciberseguridad. Y paralelamente genera un floreciente negocio en ciberseguridad que va en aumento por las crecientes inversiones que realizan el sector privado y el público. "El cibercrimen es una industria muy lucrativa que genera muchas cantidades de dinero. Al ser tan opaco no se puede hacer una estimación acertada porque el cibercrimen esta vinculado con otros tipos de delitos como el tráfico de armas, las guerras, el tráfico de drogas, trata de blancas, el terrorismo, etc. Lo que está claro es que los 'chicos malos' tienen modelos de negocio que funcionan y están creciendo en cuanto a ingresos de forma casi exponencial, ya sea a través del fraude, de la extorsión –como con ataques tipo *ramsomware*/WannaCry–, creando infraestructura para 'alquilar' ataques, etc. Es tal el nivel de avance del cibercrimen que invierten en I+D y colaboran entre ciberdelincuentes", detalla Daniel Solís.

La firma estadounidense de tecnologías de la información International Data Corporation (IDC) cifra en casi 82.000 millones de dólares (74.000 millones de euros) la facturación para este año de las empresas dedicadas a crear *hardware*, *software* y servicios de ciberseguridad, un aumento superior al ocho por ciento sobre 2016, y prevé que el gasto en protección se acelere ligeramente en los próximos años en torno al 9% anual hasta 2020, lo que generará unos ingresos al sector superiores a los 100.000 millones de dólares (90.000 millones de euros) cada año. Estados Unidos será el mayor mercado del mundo para productos de seguridad, con unas previsiones de inversión para este año de casi 37.000 millones de dólares (33.000 millones de euros), le seguirá Europa Occidental con unos 19.000 millones (17.000 millones de euros), y Asia-Pacífico –sin Japón–, región que registrará las mayores tasas de crecimiento del mundo hasta 2020 en inversiones en sistemas de ciberseguridad, un 18,5% anual, más del doble que en Europa Occidental, añade IDC. En contraste con este esfuerzo inversor en protección, los perpetradores de los ciberataques no tienen que asumir un elevado coste para 'trabajar', según los expertos. En particular, la acción de WannaCry solo requirió una estructura bastante elemental. "Los adversarios bien financiados (por ejemplo, un estado o el crimen organizado) pueden gastar grandes cantidades de dinero para comprometer un objetivo, pero la desafortunada realidad es que un ciberataque también puede lanzarse sin apenas suponer un gran coste (…). En el caso de WannaCry, tan sólo fue necesaria una máquina para iniciar todo el asunto.

SE ESTIMA QUE EL GASTO EN CIBERSEGURIDAD SUBA A UN RITMO DEL 9% HASTA 2020, GENERANDO UNOS 90.000 MILLONES DE EUROS ANUALES AL SECTOR

Para el pequeño ciberdelincuente todo lo que se necesita es un poco de habilidad técnica y algo de tiempo libre", afirma Ricardo Maté. "(…) en el mercado negro de las vulnerabilidades día 0 [las que son descubiertas en cualquier *software* o *hardware*] –o no conocidas– de características similares a las que usaba WannaCry, podrían oscilar entre los 10.000 y 200.000 euros, según el sistema, la plataforma, etc. Un precio irrisorio para los cibercriminales que mueven grandes cantidades de dinero y una inversión mínima para el gran beneficio económico que pueden obtener, o los daños que pueden provocar a las empresas, instituciones o países", añade Daniel Solís.

El sector de *startups* dedicadas a la ciberseguridad vive un auge en operaciones de compras y financiación desde 2013. Según datos de la consultora especializada CB Insights, en el primer trimestre de este año la inversión en este tipo de compañías creció un 20%. Gigantes como Amazon, Hewlett Packard, Huawei y Microsoft, entre otros, han adquirido varias en lo que va de año, con preferencia hacia las que investigan en Inteligencia Artificial y algoritmos de aprendizaje automático. Microsoft pagó en mayo pasado 100 millones de dólares (90 millones de euros) por una de esas compañías.

Paradójicamente, toda esta actividad en torno a la protección: inversiones en tecnología, compra de empresas innovadoras que abren nuevos caminos para combatir los ciberataques y que atraen volúmenes significativos de financiación de inversores privados no parece que estén desanimando a los *hackers*. Las cifras indican, por el contrario, que han multiplicado sus acometidas extendiéndolas por todo el globo, sin que aparentemente las murallas protectoras les disuadan de ejecutar sus campañas de extorsión o de intrusión en empresas o redes de infraestructuras públicas. Además, es previsible que el problema alcance una mayor dimensión con la diversidad de tecnologías que están formando parte de nuestra cotidianidad: ahora son los *smartphones*, pero mañana será el internet de las cosas (IoT, por sus siglas en inglés), los automóviles inteligentes, o los servicios personalizados de atención médica.

Según el banco de inversión Morgan Stanley, las pérdidas globales causadas por los ciberataques en los últimos cinco años se han duplicado, lo que le lleva a cuestionar la eficacia de los actuales sistemas, básicamente construidos a modo de arquitectura multicapa, como si de una cebolla se tratara, y propone un nuevo paradigma en seguridad cuyo foco sería trascender el actual modelo de soluciones perimetrales a otro que tuviera en cuenta la seguridad a nivel de dispositivos y servicios en la nube.

A partir de este análisis, la entidad prevé que el sector de la ciberseguridad sufrirá una profunda reestructuración conformando concentraciones para ganar escala y que resultarán en un grupo de cinco compañías en otros tantos años que controlarían el 40% del negocio desde el 26% actual. "Nosotros vemos dos tipos de ganadores: aquellos bien posicionados en proporcionar seguridad basada en la nube y aquellos que lo estén en seguridad para la nube", señala Morgan Stanley. "Pensamos que el crecimiento de aplicaciones para el IoT y el masivo incremento de accesos remotos a la red y la sensibilidad de los datos asociados llevará a incrustar chips de seguridad en muchos más dispositivos", añade.

Para Daniel Solís las amenazas todavía persistirán. "La nube no es más que un conjunto de ordenadores de otras personas/entidades. Si bien es cierto que probablemente tengan mejores medidas de seguridad que una empresa media, eso no significa que no estén expuestos en igual medida a los ataques, tal y como se ha visto en servicios *cloud* que han afectado a famosos con su privacidad, o a empresas con copias de seguridad. Al final, estamos hablando de delegar la responsabilidad de los servicios y la custodia de la información a terceros, con los riesgos que ello conlleva y teniendo en cuenta que todo sistema es vulnerable". ●