El lado oscuro de la tecnología

Chris Wellisz

Los beneficios de la era digital están opacados por los riesgos

LA TECNOLOGÍA digital nos ha traído beneficios que en la generación pasada habría sido difícil imaginar. Internet les ahorra a estudiantes y estudiosos muchas horas de tediosa investigación en la biblioteca y permite la comunicación oral, visual y escrita instantánea prácticamente gratis. Con el GPS de un teléfono inteligente podemos evitar perdernos en una ciudad que no conocemos. Podemos hacer compras y transacciones bancarias en línea. Los médicos pueden hacer diagnósticos con ayuda de computadoras. Son tales los prodigios de esta era digital que los economistas Erik Brynjolfsson y Andrew McAfee la denominaron la "segunda era de las máquinas", pues sostienen que lo que la computadora hace por nuestra capacidad mental es lo que el motor a vapor hizo por la fuerza muscular.

No obstante, este progreso tiene desventajas. Por ejemplo, se critica la capacidad que unos pocos medios de información gigantes tienen para formar la opinión pública. Ciertas patologías como el ciberacoso y la pornografía en Internet provocan inquietud. También preocupa la posible pérdida de privacidad y los riesgos para la libertad civil, dado que prácticamente todos nuestros movimientos, llamadas telefónicas y mensajes electrónicos dejan una huella digital que puede usar un vecino entrometido o un gobierno.

Estas inquietudes son legítimas, pero imposibles de cuantificar. No obstante, ciertos aspectos de la tecnología digital imponen costos medibles sobre las empresas y economías que contrarrestan, en parte, las eficiencias de la era digital.

Los ciberpiratas pueden asumir control de un automóvil o paralizar una red de energía eléctrica. Los ciberladrones roban datos personales para saquear cuentas bancarias o hacer compras fraudulentas en línea. El correo electrónico, el teléfono móvil y los medios de comunicación social, si bien han revolucionado las comunicaciones, reducen la productividad de los empleados de oficina adictos a los tuits o la mensajería instantánea.

Riesgos de ciberseguridad

Cuando un grupo de exfuncionarios de la Unidad 8200 —la unidad de inteligencia israelí encargada de la captación de señales— se propuso poner en marcha una empresa privada de seguridad informática, su meta era el automóvil conectado a Internet.

"Observaron lo que pasaba en los mercados y concluyeron que pronto habría millones de automóviles conectados en la carretera", explica Yoni Heilbronn, Vicepresidente de Marketing de la empresa Argus Cyber Security Ltd.

Tres años más tarde, Argus, que tiene su sede en Tel Aviv, cuenta con oficinas en Alemania, Estados Unidos y Japón. La empresa prospera porque el público escucha historias sobre ciberpiratas que toman el control de los vehículos y eso centra su atención en la necesidad de mejorar la ciberseguridad vehicular.

Esta es la Internet de las cosas, la red de objetos interconectados que pueden intercambiar datos. Esta red se está ampliando e incluirá una amplia gama de aparatos, desde el equipo hospitalario de diagnóstico hasta las máquinas de café y otros aparatos domésticos. Según Gartner Inc., una empresa de investigación y asesoramiento en tecnología de la información, este año el número de dispositivos con acceso a Internet aumentará en un 30% (a 6.400 millones). El gasto mundial en seguridad para esta red aumentará en un 24% (a USD 348 millones).

Un mundo conectado ofrece nuevas oportunidades a los ciberdelincuentes para recopilar datos personales que pueden usarse para hacer transacciones fraudulentas, o para usar programas maliciosos que pueden inmovilizar aparatos o cifrar datos y exigir dinero a cambio de la clave para descifrarlos.

"Es un nuevo punto de acceso para los estafadores", dice Bradley J. Wiskirchen, Gerente General de Kount, una empresa de seguridad en Internet con sede en Boise, Idaho. "Si me pueden piratear la impresora o el refrigerador para obtener mis datos personales, no necesitan entrar en mi computadora".

El ciberpirateo de artefactos domésticos con acceso a Internet es fácil porque los sistemas de seguridad que puedan llevar incorporados son endebles. Empresas como Nest Labs en Palo Alto, California, que fabrica artefactos inteligentes con dispositivos de seguridad complejos, son la excepción.

"Muchas de las otras empresas instalan *software* de cualquier tipo, sin darle mayor importancia a la seguridad", dice Chris King, analista de vulnerabilidades del CERT Coordination Center de la Universidad Carnegie Mellon. Es posible piratear hasta los juguetes con conexión inalámbrica como la muñeca Hello Barbie.

La lista de aparatos vulnerables aumenta a medida que el mundo conectado se amplía. Según King, los ciberpiratas han apagado el sistema de diagnóstico de hospitales para exigir rescates. El año pasado paralizaron una red de energía eléctrica en la región occidental de Ucrania que dejó sin electricidad a más de 200.000 personas. En Alemania, una acería sufrió daños enormes tras ser atacada por cibervándalos.

> Los ciberdelincuentes recopilan datos personales para realizar transacciones fraudulentas o para usar *software* malicioso.

La posibilidad de que los automóviles puedan ser controlados por ciberpiratas es especialmente inquietante porque pueden producirse accidentes fatales. Gartner estima que en 2020 unos 250 millones de automóviles en todo el mundo tendrán algún tipo de conectividad inalámbrica.

Prácticamente todos los componentes de un automóvil moderno —frenos, dirección, presión de los neumáticos, luces— usan controles computarizados, conectados entre sí con un sistema de comunicaciones que se inventó antes de la era de Internet. Este sistema es intrínsecamente inseguro, como muchos otros dispositivos del automóvil.

"Un sistema que no fue diseñado para conectarlo a Internet ahora está conectado y expuesto a todas estas cosas que los diseñadores nunca consideraron", señala King.

Los fabricantes de automóviles y componentes —que reconocen la gravedad de estos riesgos— empezaron a mejorar la seguridad tras un par de ataques muy publicitados.

Los investigadores de Argus piratearon un dispositivo inalámbrico denominado Zubie, que sigue el rendimiento de un automóvil y descarga datos en tiempo real en el teléfono inteligente del conductor a través de la nube. Los investigadores lograron controlar el sistema de dirección, los frenos y el motor. La empresa que fabrica Zubie fue informada e indicó que el problema se había resuelto.

El año pasado, Fiat Chrysler anunció que retiraría 1,4 millones de vehículos cuando la revista *Wired* informó que investigadores habían usado una computadora portátil para controlar un Jeep Cherokee a través de la computadora instalada en el tablero de instrumentos.

"Cuando los automóviles están conectados, hay que protegerlos", señala Heilbronn en Argus.

Ciberrobo

Magnus Carlsson estaba en su oficina en Bethesda, Maryland, cuando recibió un mensaje electrónico: su jefe, el Director Gerente de la Asociación de Profesionales Financieros, necesitaba ayuda para hacer una transferencia de fondos.

Cuando pulsó la tecla para responder, Carlsson no reconoció la dirección de correo electrónico que apareció en la ventanilla de Outlook. "Me di cuenta inmediatamente de que era un intento de fraude", señaló. De hecho, parte de su misión, como Director de Tesorería y Pagos de un grupo global de industrias que representa a ejecutivos de finanzas, es advertir a sus miembros sobre posibles fuentes de fraude financiero, incluido el fraude en Internet.

Esta táctica, que se conoce como intervención de correos de empresas, está ganando popularidad rápidamente entre los

Ciberdelincuentes *(continuación)*

ciberdelincuentes como método para inducir a los empleados de una empresa a hacer transferencias a un proveedor o acreedor simulado. Normalmente, el empleado recibe un mensaje electrónico falso con la orden de un superior para efectuar la transferencia. El 64% de los miembros de la asociación indicaron que habían recibido estos mensajes.

Ciberdelincuentes empeñados en crear caos pueden derribar el sistema financiero mundial.

Esta es solo una hebra en una creciente red de ciberfraude que incluye tácticas e instrumentos con nombres tanto ocurrentes como siniestros: secuestro digital (*ransomware), phishing* y troyanos. Los ciberdelincuentes son cada vez más astutos y audaces, y persiguen presas de gran magnitud, como JPMorgan Chase, British Airways, la Comisión Electoral de Filipinas y el Servicio de Impuestos Internos estadounidense. Cuando los organismos más grandes destinan mayores recursos a la seguridad informática, los delincuentes se lanzan sobre presas más fáciles a un nivel más bajo de la cadena alimentaria empresarial.

El ciberdelito "aumenta porque es fácil. Los países y las empresas que se conectan a Internet con estrategias inadecuadas de ciberseguridad serán un objetivo fácil", señala James Andrew Lewis, Vicepresidente Principal del Center for Strategic & International Studies en la ciudad de Washington, que ha escrito profusamente sobre el ciberfraude. "La aplicación de la ley es increíblemente desigual en el mundo. Por consiguiente, si es inteligente, un ciberpirata vivirá en un país donde la ley no se aplica".

Lewis estima que el daño producido por el ciberdelito asciende a USD 500.000 millones al año en todo el mundo, monto superior al PIB de Suecia. Esa cifra incluye el dinero y la propiedad intelectual robados, el costo de reparar el daño y las pérdidas en materia de innovación, comercio y crecimiento económico.

Las empresas financieras son un objetivo especialmente tentador, como lo demostró este año el robo de USD 81 millones del Banco Central de Bangladesh, donde los ciberpiratas usaron las credenciales de un empleado para enviar más de 30 solicitudes de transferencia fraudulentas al Banco de la Reserva Federal de Nueva York.

Para un país como Bangladesh, la pérdida financiera fue enorme, pero a los organismos reguladores les preocupa un riesgo mucho más grave: ciberdelincuentes empeñados en crear caos pueden derribar el sistema financiero mundial, desencadenando una crisis económica comparable a la de 2007–2008.

"Esto podría impedir a los participantes el acceso a mecanismos esenciales del sistema de mercado", observa Greg Medcraft, Presidente de la Australian Securities and Investment Commission. "Los ciberataques probablemente son el próximo cisne negro para la economía mundial".

En un estudio conducido por Depository Trust & Clearing Corporation, el 25% de los participantes opinó que el ciberdelito representa el principal riesgo para la estabilidad financiera mundial. Ese porcentaje es inferior al 46% registrado el año pasado, en parte debido a que las instituciones financieras están invirtiendo en medidas de protección, y también porque otros riesgos, como la desaceleración del crecimiento de Asia, han ganado prominencia.

No obstante, los organismos reguladores no están dejando nada al azar. Los sistemas de pago y liquidación —componentes clave del sistema financiero mundial— deberán contar con planes de defensa frente a los ciberataques y un funcionario a cargo de supervisarlos, de conformidad con las directrices publicadas en junio por el Banco de Pagos Internacionales y la Organización Internacional de Comisiones de Valores.

El ciberdelito es el tipo más común de delito en las empresas tras la malversación, de acuerdo con un estudio de PwC. No obstante, aunque el 61% de los gerentes generales señalaron que les preocupa la ciberseguridad, solo el 37% de las organizaciones declaran que cuentan con un plan de acción.

Los delitos en Internet se sitúan en dos categorías generales. La primera abarca ataques monetizables, como el robo de identidad o tarjetas de pago. La segunda, el ciberespionaje: el robo de secretos comerciales, estrategias de negociación e información sobre productos.

El año pasado el número de identidades expuestas aumentó en un 23% (a 429 millones), según el informe anual de Symantec Corporation sobre amenazas a la seguridad en Internet. El número real probablemente supere los 500 millones pues muchas empresas no notifican estas violaciones.

Tras la filtración en gran escala de datos en empresas como eBay y Anthem, se ha expuesto la identidad de casi toda la población de Estados Unidos, según Wiskirchen.

"Prácticamente todos hemos quedado expuestos", afirma. Las identidades robadas se comercian en un floreciente mercado negro electrónico, en sitios web bien diseñados que ofrecen garantías de reembolso, descuentos por grandes cantidades y cursos breves.

En promedio, el costo de una filtración de datos aumentó de USD 3,79 millones a USD 4 millones, según un estudio reciente de 383 empresas en 12 países efectuado por IBM y el Instituto Ponemon. Brasil y Sudáfrica tienen la probabilidad más alta de un ataque, y Australia y Alemania, la más baja.

El ataque a JPMorgan Chase en 2014 expuso los datos de 83 millones de clientes, incluidos nombres, direcciones postales y electrónicas, y números de teléfono. Este ha sido el mayor ataque a una institución financiera en Estados Unidos. El banco no indicó qué costo tuvo, pero anunció planes para invertir otros USD 250 millones al año en medidas de seguridad.

El costo del robo de propiedad intelectual es más difícil de estimar, aunque las pérdidas económicas podrían ser mayores. Según Lewis, estos robos, que abarcan desde fórmulas para pintura hasta misiles, reducen las utilidades de la innovación.

"La rentabilidad financiera incentiva a las personas a inventar cosas nuevas, y si no la obtienen, dejarán de hacerlo".

El resultado es la subinversión en nueva tecnología y la pérdida de empleos y crecimiento económico. Incluso los países que se benefician terminan perdiendo, pues al depender de tecnologías robadas no aprenden a crear las propias. "Esto reduce el ritmo de crecimiento en todo el mundo", señala Lewis.

Lewis estima que el costo global del ciberdelito, incluido el robo de propiedad intelectual, equivale en promedio al 0,5% del PIB mundial. En los países de ingreso alto, donde la importancia económica de la innovación es mayor, puede ser de hasta un 0,9%. En las economías en desarrollo es cercano al 0,2%.

Esto promueve un incremento extraordinario de la demanda de servicios de ciberseguridad, que según un pronóstico de Cybersecurity Ventures, una empresa de investigación e información de mercados, aumentará de USD 75.000 millones el año pasado a USD 170.000 millones en 2020.

Según Wiskirchen, el incremento porcentual anual del volumen de transacciones de Kount es de tres dígitos "y apenas hemos empezado a explorar las oportunidades disponibles". "Desafortunadamente", agrega, "trabajo en un sector de muy fuerte crecimiento".

Distracción digital

Un día, cuando Laurie Voss era programador en Silicon Valley, se le asignó un proyecto excepcionalmente aburrido y nada gratificante que debía finalizar en un mes. "Fue una labor ingrata", dice. "Ese mes pasé mucho tiempo en Twitter".

Según Voss —que actualmente es Director de Tecnología de su propia empresa, NPM— el tuiteo en la oficina es la versión moderna de un fenómeno tan antiguo como el mundo: dejar las cosas para mañana.

La sobrecarga de información y la distracción digital reducen considerablemente la productividad.

Los nuevos dispositivos y aplicaciones ofrecen oportunidades irresistibles para perder tiempo. En todo el mundo, los empleados de oficina son acosados por un flujo interminable de señales en la computadora, el teléfono móvil y la tableta. La sobrecarga de información y la distracción digital reducen considerablemente la productividad a medida que se propagan las nuevas tecnologías y se expande la economía del conocimiento.

En Estados Unidos, tres de cada cuatro empleadores señalan que se pierden dos o más horas al día porque los empleados se distraen, según un estudio publicado en junio por CareerBuilder, una firma consultora para recursos humanos con sede en Chicago.

Los empleadores indican que el teléfono móvil y los mensajes de texto provocan la mayor pérdida de tiempo, seguidos por Internet, el chismorreo y los medios de comunicación social. Esto afecta la calidad del trabajo y causa la frustración de los empleados que deben terminar el trabajo de los colegas distraídos y el incumplimiento con los plazos.

Según Nathan Zeldes, un consultor de organización que trabaja en Jerusalén, el correo electrónico causa las mayores pérdidas de tiempo, y culpa a los empleadores por no limitar su uso. Observa que un empleado de oficina probablemente recibe entre 50 y 300 mensajes de trabajo al día.

"Es imposible leerlos o procesarlos de manera inteligente, y la avalancha es interminable", indica.

Mediante un estudio que dirigió en 2006, cuando trabajaba para el fabricante de chips Intel, Zeldes determinó que en promedio un trabajador de ese ámbito pierde un día por semana debido a los mensajes e interrupciones innecesarios. Para una empresa con 50.000 empleados, esto tiene un costo anual de alrededor de USD 1.000 millones.

El correo electrónico es difícil de resistir, dice Zeldes. Los empleados se sienten obligados a leer y responder mensajes a cualquier hora del día o la noche por temor a perderse algo importante, o para crear una buena impresión entre sus colegas o superiores.

"Lo comparo con el dilema del prisionero", dice. "Todos querríamos reducir los mensajes e irnos a la casa más temprano, pero nadie se atreve a hacerlo primero".

Gloria Mark, una PhD en psicología que enseña en el Departamento de Informática de la Universidad de California en Irvine, usa una analogía para describir la forma en que las personas se condicionan al uso del correo electrónico.

"Lo llamo el fenómeno de Las Vegas", señala. El jugador de tragamonedas gana a intervalos aleatorios. La posibilidad de ganar de nuevo basta para mantenerlo jugando.

"El comportamiento que se refuerza al azar es el más difícil de erradicar", dice Mark.

En 2012, Mark comprobó que, en promedio, los empleados solo se concentraban en la pantalla de computadora por 75,5 segundos, tras lo cual empezaban a hacer otra cosa. En 2015, la concentración se había reducido a 47 segundos.

Los empleados y sus superiores han creado diversas estrategias para combatir la distracción y la sobrecarga. Muchos reservan un espacio de tiempo para el correo electrónico, sin prestarle atención el resto del día.

"Paso mucho tiempo optimizando mi uso del correo electrónico", dice Voss. Su estrategia consiste en "filtrar despiadadamente" los mensajes que no necesita leer.

"Desconecte los sistemas de notificación. Desactive las notificaciones automáticas", recomienda Cliff Williams, jefe de diseño de Nextdoor, una empresa con sede en San Francisco que se promueve como "una red social privada para su barrio".

No obstante, Williams reconoce que debe "esforzarse continuamente" por evitar las distracciones.

"Es como hacer dieta", agrega. "A veces uno pierde peso y a veces lo recupera". ■

Chris Wellisz es un periodista de finanzas que trabaja en la ciudad de Washington.