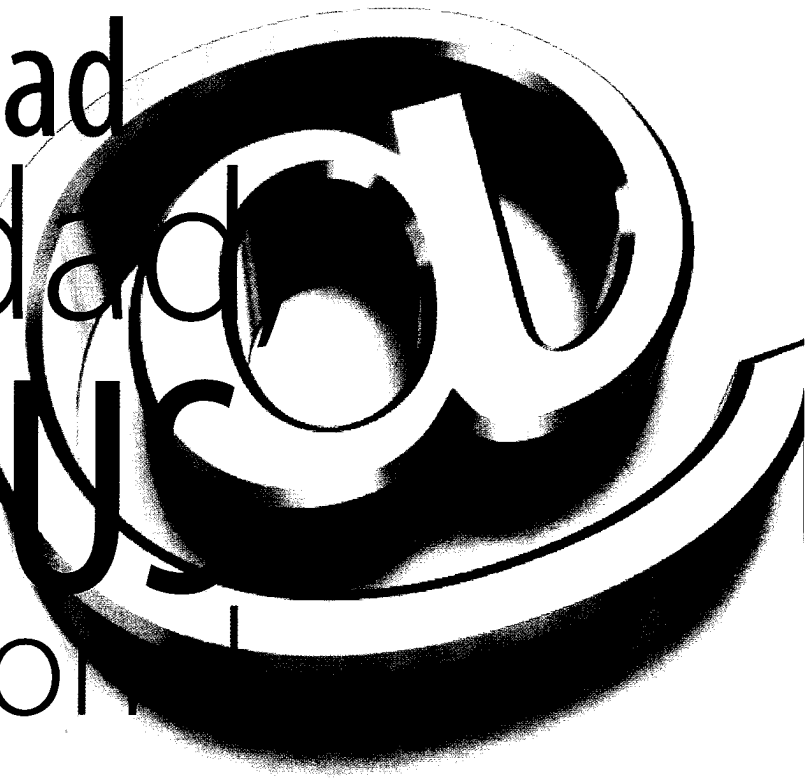
La vulnerabilidad privacidad UN VIRUS organizacional



Vivimos en un entorno en constante cambio, en el que el progreso se torna ambiguo y paradójico. Y una de las constantes, producto del exceso de información al que estamos expuestos, es la tendencia a la pérdida de la privacidad. En principio, esta surgió con temor. Sin embargo, con el paso del tiempo este miedo se ha ido disipando y nos hemos ido acostumbrando y adaptando al nuevo medio, en el cual la barrera entre lo privado y lo público se ha roto. "Vivimos en una vitrina y parece no afectarnos". La expansión masiva de las tecnologías, en especial las de la información, han erigido un mundo en el que son tan imprescindibles como impredecibles.

La información se ha convertido en eje promotor de cambios, y la expansión exponencial de las Tecnologías de la Información y las Comunicaciones (TIC) ha impactado de manera sustancial, al punto de hacer manifiesta la importancia del conocimiento, como el pilar y el activo de mayor trascendencia de una organización, pues a la postre "Toda institución reposa sobre una montaña de secretos" (André Maurois). De esta manera, el canal más adecuado y eficiente para filtrar y transmitir información es, sin duda, la tecnología. El fenómeno es inevitable. La pérdida de privacidad en un mundo en constante interconexión en donde prolifera la información instantánea es un hecho. Por esto las organizaciones afrontan un nuevo problema, pues los riesgos de que su confidencialidad sea vulnerada son cada vez mayores.

La empresa en promedio es atacada dos veces por semana y pierde 8.9 millones de dólares al año.

El término hacker es empleado para referirse al causan- [illegible] los cibercrímenes y sus métodos [illegible] ción de los usuarios para [illegible] de seguridad a través de técni[illegible] persuasión), han adquirido gran [illegible] riedad y rentabilidad, al punto de ser aún más provechosos que el negocio del narcotráfico, según un informe del

FBI, y sin el riesgo implícito, pues tan sólo el 5% son capturados y procesados, de acuerdo a datos de Microsoft.

Los hackers se han diversificado. Entre ellos se encuentran los hacktivistas (que pretenden corregir injusticias percibidas), los patrocinados por el Estado y los ciberdelincuentes, entre otros. Son estos últimos los de mayor peso en el ámbito empresarial por su creciente interés en un beneficio económico, que según un estudio de Ponemon Institute (líder en investigaciones independientes sobre privacidad, protección de datos y políticas de seguridad de la información), a causa de la ciberdelincuencia la empresa promedio es atacada dos veces por semana y pierde 8,9 millones de dólares al año.

Sin embargo, no es un fenómeno local que solo afecta a una minoría. Lo desconcertante es su carácter global, el gran impacto que genera en las organizaciones y la dificultad para controlarlo. Un reciente estudio de Iron Mountain (líder mundial en servicios de la administración de la información) revela que más de la mitad de las empresas europeas espera perder datos. A su vez, Ernst & Young (líder global en servicios de aseguramiento, impuestos, transacciones y asesoría) concluye que hay tres factores que influyen la dirección de la privacidad en las organizaciones: el fraude, la economía y las regulaciones. El fraude hace referencia al abuso de la información, la economía a la incertidumbre y el seguimiento financiero, y las regulaciones hacen alusión a mantener un ambiente de control conocido y estable.

"Hoy en día los cibercriminales buscan un beneficio económico, ya no es solo el reconocimiento mundial como hace algunos años, además hay mayor conocimiento sobre el funcionamiento de las entidades financieras, las empresas y los gobiernos, lo que hace aún más ›

"La tecnología hace posible que la gente pueda tener control sobre todo, excepto sobre la tecnología", John Tudor.

vulnerables los sistemas", explicó Andrés Velásquez, director general de Mattica, firma especialista en análisis de la seguridad informática.

Es así como el camino trepidante del nuevo mundo nos lleva al capitalismo del conocimiento, en el cual la innovación ha marcado la pauta para una tendencia generalizada, donde el conocimiento es redituable y tiene un costo de gran magnitud. Por esta razón, la relación es meramente comercial y el conocimiento se ha convertido en una mercancía. Su valor es determinado con base en el grado que proporciona o puede llegar a proporcionar, así como sus ventajas comparativas y competitivas. Según el Centro de Registros de Direcciones de Internet para América Latina, los ataques informáticos especializados causan pérdidas de más de 93.000 millones de dólares, lo que afecta a cerca de 2500 bancos en la región. Colombia es el tercer país en Latinoamérica donde más se cometen dichos ataques, de acuerdo con un estudio realizado por el Colegio Colombiano de Juristas.

Por tanto, la información debe siempre estar protegida con herramientas técnicas (regulación) y legales tales como pactos de confidencialidad y medios de organización, clasificación y acceso a la información. Sin embargo, a pesar de múltiples esfuerzos por mitigar y prevenir estas consecuencias, las medidas legales carecen de aplicabilidad con respecto a este tipo de delitos frente al ingenio, la creatividad y el conocimiento, pues la variable de mayor peso y complejidad por determinar es "quién lo efectúa", lo cual suele resultar más costoso y dispendioso que la prevención misma. Incluso al margen de un marco legal, casi global (Organización Mundial del Comercio), es imposible controlar y predecir el avance tecnológico, lo que hace el entorno organizacional cada vez más inestable y resalta la cualidad adaptativa como la más apropiada en este ambiente vertiginoso que ha causado pérdidas millonarias a múltiples empresas y no sólo pone en riesgo la confidencialidad empresarial: también juega con la integridad física de los empleados y la capacidad de mantener soportes informáticos estables.

PC World (una de las revistas de mayor importancia en informática), clasificó las nueve peores violaciones digitales del siglo XXI, entre las que se encuentran:

- En julio de 2007, Fidelity National Information Services (el mayor proveedor del mundo dedicado a la banca y tecnologías de pagos) protagonizó un escándalo en donde un empleado robó 3,2 millones de registros de clientes, incluyendo información bancaria y personal.

- A mediados de 2009 Google, Yahoo, y docenas de otras empresas de Silicon Valley se vieron inmersas en un acto de espionaje industrial, en el que el gobierno chino lanzó un ataque masivo y sin precedentes. Los hackers chinos aprovecharon una debilidad en una versión antigua de Internet Explorer para obtener acceso a las redes internas, lo que dio paso a una violación inédita de la propiedad intelectual.

Es así como la tecnología implica riesgos. Las empresas tienen un trabajo arduo en materia de prevención, en la que el proceso adaptativo y la disponibilidad de la información son indispensables frente a las decisiones venideras, en las cuales el conocimiento es el pilar sobre el que se fundan las organizaciones del mañana. Por lo tanto, la complejidad de la dirección de la privacidad debe evolucionar en términos de efectividad y eficiencia para minimizar aquellos riesgos que puedan llegar a comprometer el negocio.

Santiago Moncayo Vanegas
Estudiante Administración de Empresas

"Toda institución reposa sobre una montaña de secretos", André Maurois.