L

os medios de comunicación están refiriéndose, cada vez con más frecuencia, a los ataques cibernéticos. Los usuarios de tecnología, el personal de sistemas, los consultores en ésta área y los auditores especializados, están hablando de los peligros que acechan, de los controles que se deberían establecer y de las acciones que convendría desarrollar si hubiese un siniestro. Esta problemática incumbe a las empresas grandes y medianas, en mayor porcentaje que a las pequeñas y a las micro - entidades. En la misma medida en que avanza la tecnología, crecen los peligros. Como se dice popularmente “hecha la ley, hecha la trampa”. La vulnerabilidad de los datos tiene varias perspectivas. Por ejemplo, una cosa es la pérdida del dato, otra la extracción o introducción de datos falsos dentro de una base o biblioteca y otra la simple lectura de datos de un conjunto que se supone confidencial.

Las grandes firmas de consultoría, dentro de las cuales se encuentran muchas firmas de contadores, han realizado varias encuestas para diagnosticar el estado de la cuestión. Hay todo tipo de respuestas. Recientemente ISACA divulgó un documento dedicado a comentar la [Cybersecurity Act of 2015](http://www.isaca.org/cyber/Documents/CSX-Special-Report_misc_Eng_0116.pdf) (P. L. 114-113) promulgada el 18 de diciembre de 2015, que, entre otras cosas, propone la colaboración del sector privado con el sector gobierno para atacar los delitos cibernéticos. En su [ISACA’s January 2016 Cybersecurity Snapshot](http://www.isaca.org/pages/2016-cybersecurity-snapshot.aspx), consta que el 63% contestó no a la pregunta “*Do you believe governments should have backdoor access to encrypted information systems?”* De otra parte el 52% opinó que los mayores ataques provendrán de la llamada *Social engineering.* En cuanto al [recurso humano](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2016/Pages/ISACA-Cybersecurity-Snapshot-Survey.aspx) necesario para combatir esta situación “(…) *Close to half (45%) of those surveyed worldwide report that they are hiring more cybersecurity professionals in 2016, yet fully 94% of those hiring say it will be difficult to find skilled candidates. Identifying who has adequate skills and knowledge will also be difficult, say more than six in 10 survey participants.* (…)”.

Como si se tratara de un búmeran, que va y vuelve, cada cierto tiempo reaparece la idea de permitir que el Estado tenga acceso a la información privada. A veces esto se presenta en forma seductora, como cuando nuestro gobierno propuso que se le autoriza para poner un programa contable en “la nube” que pudieran utilizar los que quisieran. Esto significaba ahorrarse los costos asociados al programa, pero implicaba que el Estado tendría en su poder todos los datos sobre todas las transacciones registradas en la contabilidad. La idea recibió tan alto rechazo como la propuesta de crear una puerta por atrás que permitiera el Estado penetrar los datos encriptados.

Parece ser que ha llegado el momento en el cual es imprescindible la formación en seguridad informática, debido a la alta confianza que necesariamente se deposita en los programas de computación que procesan la información empresarial. Esta es otra faceta de la formación en tecnología de la información, componente que ha resaltado IFAC.

*Hernando Bermúdez Gómez*