SHARING IS CARING (ABOUT GOVERNMENT COMPLIANCE)

"Information sharing is an issue that has global implications, particularly for technology companies. In the U.S., the Cybersecurity Information Sharing Act was recently enacted, a law that encourages information sharing and provides some form of liability protection for companies that meet the criteria of the law. However, on a global basis, information sharing, particularly with the U.S. government, continues to be a hot button issue— one that has, at least in part, caused some of the issues in the EU, including the invalidation of Safe Harbor. These issues are likely to come to a head in 2016, and hopefully companies will have a clearer path forward."

— Andrew Serwin, partner (San Diego), Morrison & Foerster

GOOD RISK MANAGEMENT MEANS A GOOD CRYSTAL BALL

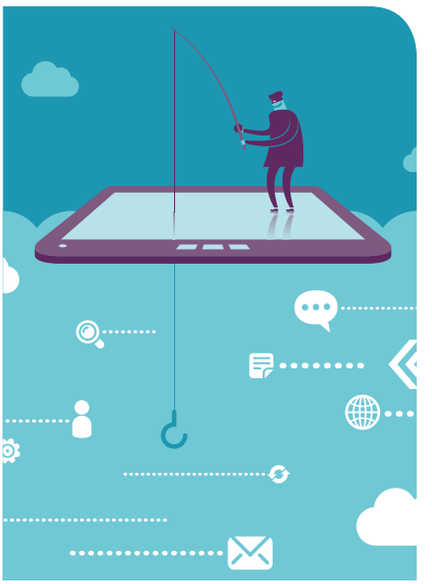
"Recent major cybersecurity breaches highlight the need for companies to not only enhance their cybersecurity to defend against an attack, but also to plan for the legal fallout from an intrusion. Through both the courts and regulatory action, companies face monetary and reputational losses from a cyberbreach. For example, for the 2015 bank stress testing exercise, the Federal Reserve required banks to improve operational risk planning for cybersecurity-related losses, including related legal losses.

Legal departments can and should be part of planning for a cybersecurity situation, including identifying the applicable law and regulatory body. Departments in industries with well-defined regulatory schemes should also consider modeling for legal losses or regulatory fines. Determining possible outcomes leads to better risk/reward decisions for cyberdefense investments. Reasonable models can be built by analyzing cybersecurity breach survey data, assessing pending litigation against peers and applying expert legal judgment."

— Ed O'Keefe, partner (Charlotte), Moore & Van Allen

ISTOCK: KAAN TANMAN; THEMACX; AKINDO

AUTOMATIC SAVING CAN CREATE AUTOMATIC HEADACHES



"Unfortunately, many companies' technology policies do not adequately address one of the greatest security and regulatory threats: data downloaded and stored on employee's personal devices (phones, tablets, etc.), including confidential medical or personal identifying information. When the phones are then stolen, sold to others, or accessed or used by spouses or children, this sensitive information can be improperly accessed or shared in violation of governing privacy laws. While certain third party applications can 'erase' a phone if lost or stolen, policies need to address personal device access, password protection, and device disposal in keeping with all governing laws and privacy standards.

The same is true of home computers, where another significant problem is the automatic saving of passwords by Web browsers such that anyone then having access to the computer can potentially access an otherwise secure intranet or website and have full access to both confidential and proprietary information. In business entities such as medical offices, law firms, and accounting firms, where patient/client confidential communications can also be exposed, this risk presents both civil and regulatory/licensing concerns."

— Robert Cutbirth, partner (San Francisco), Tucker Ellis

ISTOCK: ALEXSL; SORBETTO