Paradigm

INTERNATIONAL SOCIETY OF PRIMERUS LAW FIRMS

FALL 2016

Clients Join Primerus to Propel Mission

Primerus Client Resource Institute: Making Clients Part of the Family

+

Current Legal Topics:

Asia Pacific

Europe, Middle East & Africa

Latin America & Caribbean

North America

Overcoming Statistical Overload: Establishing the First Steps of a Cybersecurity Program

In the cybersecurity realm, businesses are frequently confronted with a confusing array of seemingly solid (and sometimes contradictory) statistics. For example, the Identity Theft Resource Center (ITRC) Data Breach report states that there were 780 publicized data breaches in 2015. On the other hand, the 2016 Verizon Data Breach Investigations Report considers a worldwide 2015 data set of 100,000 data "incidents," of which 3,141 were "confirmed data breaches" with the majority of the breaches occurring in the U.S.

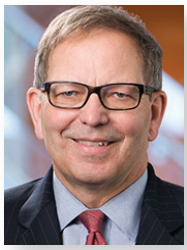
An IBM/Ponemon Institute report (based on 383 companies in 12 countries) states that the average global cost of each lost or stolen record was $158 and that data breaches cost the most in the U.S. ($221). Various reports and surveys also state that 71 percent of respondents' networks were breached in 2014; 52 percent of respondents believed a "successful attack" was likely in 2015; that 74 percent of Chief Information Security Officers are concerned about employees stealing sensitive company information; and that only 38 percent of global organizations claim they are prepared to handle a sophisticated cyberattack.

Which of these statistics are trustworthy? Even more fundamentally, are any statistics reliable in the rapidly changing cybersecurity space? And, if no statistics are absolutely reliable, does this mean that businesses are justified in not acting to prevent cybersecurity incidents until there is more solid and consistent evidence?

Despite the sometimes contradictory nature of statistics, it would be a mistake to ignore cybersecurity. There are, of course, statistics to support that view as well! A study conducted by ISACA – a leading security organization – showed that 82 percent of security professionals stated that their boards of directors were very concerned about cybersecurity. But notwithstanding these concerns (which are echoed in numerous surveys regarding cybersecurity awareness), there is also said to be a gap between general awareness of the problem and implementation of solutions, particularly on the part of small to medium size businesses (SMBs), who frequently are concerned about the cost of such implementation. Cisco reported in 2015 that a smaller percentage (29 percent) of SMBs were using standard patching and configuration tools for preventing security breaches than had done so in the prior year (39 percent) – a troubling statistic given the increase in cybersecurity attacks. Moreover, the Cisco report also found that SMBs often do not have an executive in place that is responsible for security and that "nearly one-quarter do not believe their businesses are high-value targets for online criminals."

Although SMBs may not see themselves as targets, as Cisco states, they "may not realize that their own vulnerability translates to risks for larger enterprise customers and their networks." Indeed, SMBs may be the weakest link in protecting proprietary information of their clients, as exemplified by the fact that the massive Target breach was supposedly effected through an HVAC contractor.

A consistent message in the myriad of surveys and reports cited above is that cybersecurity threats continue to grow not only in number but in extent. Any business that has data of its own, stores or processes the data of others, or provides an access point to the data of a third party, is a potential target for hacking and potential extortion. The reasons for this are clear. As the 2016 Verizon Data Breach Investigations Report indicates, 89 percent of phishing attacks are perpetrated by organized crime syndicates (often located abroad), who have the time, motivation



Timothy Toohey

Timothy Toohey leads Greenberg Glusker's cybersecurity practice, working to assure that his clients' proprietary, personal, customer and employee information, and other sensitive data is fully protected and serves its intended purposes. He is a United States and European Union Certified Information Privacy Professional and a Certified Information Privacy Manager.

Greenberg Glusker
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067

310.734.1965 Phone
310.553.0687 Fax

greenbergglusker.com
ttoohey@greenbergglusker.com

and patience to exploit any vulnerability that may lead to financial gain. Moreover, the targets of these perpetrators are the highly fallible humans who are prompted to open e-mails or respond to the supposed instruction of an executive to wire money to an overseas bank account. A recent Experian/Ponemon Institute survey found that 66 percent of respondents believed that employees are the weakest link in creating strong security and that 55 percent suffered a security incident due to a malicious or negligent employee.

Perfect cybersecurity should not be the enemy of good security based on incremental (and frequently relatively inexpensive) steps. Rather than being seen as exotic (or as the purview solely of the largest enterprises), cybersecurity protection for businesses should be as fundamental as protecting against fire, water or wind for the simple reason that data in the wrong hands can be as destructive as any of these elements.

Understanding that perfect security is unachievable, even for the largest enterprises, what basic steps should a business take?

- As a good first step, a business should analyze the nature of the specific risks it confronts. If it has not already done so, it should conduct an inventory of key data assets and analyze existing restrictions placed on access to such data by its personnel.
- A business should put in place basic written procedures and policies regarding use of computer systems and data. Although these policies need not be elaborate, they must realistically reflect the risk environment in which the business operates. Key policies and procedures may include: controlling access to computer systems, password controls, procedures for updating software, implementing protections against internal threats and monitoring access to sensitive or valuable information.
- A business should conduct cybersecurity and privacy awareness for all personnel, including executives. All employees should be made aware of the potential attacks, including ransomware, phishing attacks, and attempts to steal key data or extort or wrongfully transfer money, and also of the ways that such attacks may be prevented.
- An enterprise should purchase cyber insurance coverage appropriate for the risks it faces. Because cybersecurity insurance is a relatively new product and policy terms vary, a business should consult with a trusted advisor, such as an attorney or insurance broker, as to what coverage is best for it.
- Finally, all businesses should put in place technical protective measures to help guard against its own specific risks, such as storing credit card, health or personal data. In addition to traditional tools, such as firewalls and anti-virus software, businesses should consider implementing encryption, filtering e-mails for phishing and extortion threats, and implementing measures to guard against ransomware.

Involving counsel in many of these activities is advisable. Lawyers are well equipped to help analyze cybersecurity problems in the context of the myriad of applicable laws, regulations and best practices. Although many businesses will likely find it necessary to consult technical personnel, including a company's own IT department or outside consultants, trusted legal counsel can help ensure that the technical advice provided by such personnel is presented to executives in a manner that will maximize its impact. Involving lawyers also helps ensure that executives will see cybersecurity not as a technical issue best left to IT, but as a part of an overall risk management strategy.

Involving lawyers in cybersecurity matters also provides attorney-client privilege protection for sensitive issues, such as the location and protection of personal and proprietary data, gaps in security and privacy protection, and the vulnerability to outside attacks, as well as communications with outside consultants. Because of the complex array of global regulatory and legal requirements, counsel should be engaged if a business must remediate a data breach, respond to a regulatory inquiry, or transfer data internationally.

Although, as Mark Twain stated, "There are three kind of lies: lies, damned lies, and statistics," enterprises of all size should not let the wide array of cybersecurity statistics prevent them from taking the necessary and often relatively inexpensive first steps needed to protect against data incidents and breaches. P