American Land Title Association
Protect your property rights

Cybersecurity Outlook and Tips to Protect Data

February 4, 2016

As the cybersecurity and data privacy landscapes continue to shift, the importance of companies in the title and settlement services industries to understand the threats and respond in strategic and coordinated efforts will be greater than ever in 2016.

In its 2016 outlook, the law firm Mayer Brown recently highlighted five priorities companies should consider as they assess, refine and operate their cybersecurity and data privacy programs.

The first is increasing global governance of cybersecurity and data privacy. Mayer Brown says that many of the most significant cybersecurity and data privacy developments for U.S. companies may well be seen outside the United States in 2016.

"A company's data may very well cross borders—whether to be stored at an international data center (e.g., for a private cloud) or to be processed remotely (e.g., by a payroll service)—even for otherwise domestic businesses," the law firm reported.

Second, expansion of regulatory and enforcement activity is expected. Businesses face a growing patchwork of regulatory requirements—a trend that is set to continue in 2016, Mayer Brown reports. The likely common denominators of these are more expansive and detailed rules and more frequent enforcement of those rules. As an example, the U.S. Court of Appeals for the Third Circuit affirmed last year the FTC's ability to regulate cybersecurity practices through its "unfairness" authority under Section 5 of the FTC Act. Meanwhile, the trend of financial services regulators aggressively acting aggressively in the cyber area will continue. The New York State Department of Financial Services is set to embark on a major rulemaking in 2016. The chartered-bank regulator is expected to propose new requirements regarding cybersecurity policies and procedures, management of third-party service providers, multi-factor authentication, appointment of a chief information security officer, application security, audits and notice in the event of a cybersecurity incident. Companies also should expect the patchwork of state data security and breach notification laws to continue. California revised its data breach laws effective Jan. 1, 2016, to expand and clarify the existing notice requirements and to specify forms for notices.

Mayer Brown also expects growth in litigation for cybersecurity and data privacy. The law firm pointed to significant court cases such as the U.S. Court of Appeals for the Seventh Circuit's decision arising from the Neiman Marcus breach and the U.S. Supreme Court hearing arguments in Spokeo v. Robins, which considers whether the violation of a right that triggers statutory damages can substitute for injury-in-fact for purposes of Article III standing. Plaintiffs filed nearly 250 class actions involving some 35 different data breached last year, according to Mayer Brown.

Fourth, companies should develop productive relationships with relevant authorities before a cyber crisis arises. Mayer Brown reports that the number of cybercrime investigations and prosecutions is expected to increase in 2016 and continue the long-term trend of growing collaboration among domestic and foreign agencies to target threat actors around the world. The U.S. Department of Justice plans to disrupt and dismantle 1,000 cyber threat actors and to resolve 90 percent of national security and criminal cyber cases during the next fiscal year. The law firm also reports that:

- Since 2002, the FBI's number of cyber intrusion investigations has grown by more than 80 percent
- Since 2010, the U.S. Secret Service's cybercrime investigations have resulted in more than 5,000 arrests associated with more than $12 billion in actual and potential fraud loss

Lastly, Mayer Brown said cybersecurity and data privacy issues attracted national and global attention. Policy developments in 2016 likely will continue this trend. For example, according to Mayer Brown, it is expected that:

1. industry will take advantage of significant legal authorities approved in 2015, such as the Cybersecurity Information Sharing Act and new "cyber sanctions," both of which will require effective collaboration between the private sector and government

2. long-standing debates about privacy and security will be moved to the global stage (and likely become more political as the U.S. presidential election approaches
3. proliferation of toys, devices and machines that are connected to the Internet will present new cybersecurity and data privacy challenges

“Cybersecurity and data privacy present novel, complex and global issues across the legal, policy and regulatory spectrum,” Mayer Brown reported. “These developments pose challenges that demand a proactive, risk-based response. Businesses must address these risks in a holistic fashion that reflects the strategic interests of their organizations and is effectively coordinated across their enterprises.

According to the Ponemon Institute’s 2015 global breach survey, on a global basis the average cost of a breach was $3.8 million, with a cost of $154 per individual record lost or compromised. Small and large companies run the risk of a data breach. The implications can be grave. In its 2016 Data Protection and Breach Readiness Guide, Online Trust Alliance (OTA) outlined advice to help businesses optimize privacy and security practices to help reduce the risk of data loss.

Data loss and identity theft occur from an increasing level of deceptive practices. Social engineering, forged email, malvertising, phishing and fraudulent acquisition of Internet domains are rising, according to OTA. Because of this, OTA recommends businesses implement the following to protect data:

- Encrypt data at rest and in transit
- Enforce effective password management policies
- Implement a Least Privilege User Access (LUA) security strategy
- Conduct regular security design and code reviews including penetration test and vulnerability scans
- Secure client devices by deploying multi-layered firewall
- Require email authentication on all inbound and outbound mail servers
- Implement a mobile device management program
- Monitor security in real-time
- Deploy web-application firewalls
- Permit only authorized wireless devices
- Implement Always On Secure Socket Layer
- Review server certificates and vulnerabilities
- Develop, test and continually refine data breach response plan
- Establish and manage vulnerability/threat intelligence reporting program

“Whether you are a Fortune 500 company or local merchant, if you collect data then you are at risk,” Online Trust Alliance said in its report. “Data security and privacy must become part of an organization’s culture. Being prepared will help protect your data, detect a loss and quickly mitigate the impact. The responsibility cannot be assigned to a single group or person. It is everyone’s responsibility.”

The third pillar of ALTA’s Title Insurance and Settlement Company Best Practices addresses policies and procedures to protect data.

American Land Title Association (ALTA)
1800 M Street
Suite 300 South
Washington, DC 20036
Phone: 202-296-3671
E-Mail: service@alta.org
Web: http://www.alta.org