UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

29th Annual Technology Law Conference

May 26-27, 2016
Austin, Texas

Development and Testing of Incident Response Plans

Christopher M. Koa

Bill F. Odom

R. Jason Straight

Luke Tenery

An ALM Website

March 2, 2015

CORPORATE COUNSEL

4 Ways to Improve Cybersecurity via Corporate Culture

From the Experts

Jason Straight

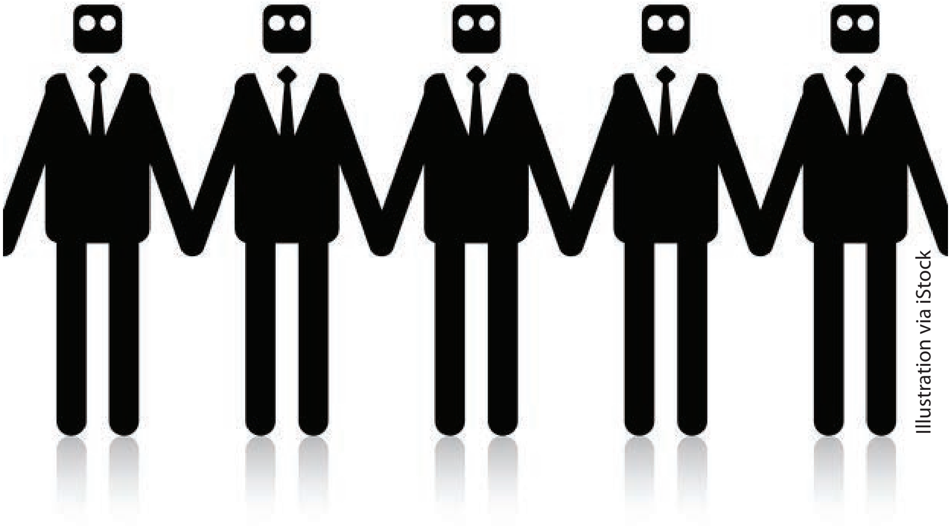

Illustration via iStock

Recent high-profile data breaches at large corporations like Sony Corp., Target Corp., JPMorgan Chase & Co. and The Home Depot dispel a persistent fallacy about cybersecurity—that protection of data is a technical problem for the IT department to solve. Many companies already have ramped up spending on technology and IT staff to protect their data, yet there's little evidence that such a strategy alone is sufficient to addresses the risks. Often it is not until a major incident occurs and other business stakeholders—most notably the legal department—recognize the full impact a data breach can have on an organization.

Security technology is important, but focusing on tactical defenses can allow you to overlook the fact that skilled, committed attackers almost always will be able to find a way into your network. After all, an attacker only needs to be right once to get in; the defender, on the other hand, needs to be right every time to prevent an incursion. Companies that are serious about reducing the risks associated with data breaches must look beyond their narrow preoccupation with the next line of technological defense and shift their focus to anticipating and containing the damage once a breach occurs. Improvement in this area requires input from other business leaders and, in many instances, is driven most effectively by corporate counsel.

Close analyses of catastrophic cybersecurity failures have repeatedly revealed that company culture and human behavior are at least as culpable as technology. Most breaches—even those perpetrated by sophisticated outside attackers—begin by exploiting what is for most companies the most persistent network vulnerability—the human layer. Attack after attack is enabled by an insider falling prey to a spear-phishing email, using a default or easy-to-guess password or other failure to practice basic cybersecurity hygiene. Recent mega-breaches also have demonstrated that actions taken—again by humans—immediately following a breach are at least as important as the defensive measures implemented to prevent or detect attacks.

This reinforces a fundamental principle that cannot be emphasized enough: Cybersecurity can no longer be regarded simply as an IT challenge. Examples like the recent Sony breach, as well as the Target ruling allowing banks' lawsuits against the retailer to continue, demonstrate the breadth of business and legal implications a data breach can have on a company for months, even years, after the event occurs.

Rethinking Cybersecurity

Thinking about cybersecurity as a business problem that extends across the entire enterprise is a good way to begin the long-overdue process of re-examining your cybersecurity posture and assessing the alignment among IT, legal and other key business stakeholders with respect to digital risk management. What's needed is a profound cultural change—driven from the top—that mandates active, ongoing collaboration across departmental, divisional and geographical boundaries within the organization. As a basic first step, legal and IT security functions should be tightly aligned so that the incident response process can be coordinated quickly and effectively before a breach gets out of hand.

What can you do to cultivate a collaborative cybersecurity culture and get a better handle on the associated risks? Here are four suggestions.

1. Identify Your Organization's Critical Data Assets and Determine Your Risk Profile

Assemble a team of stakeholders comprising IT, legal, risk, compliance and human resources professionals, as well as C-suite executives. From these diverse perspectives, identify the top three most significant information security and data privacy risks faced by your organization. Is your information security framework tailored to defend against these threats? Are you retaining too much data for too long? Does your organization have a security incident response plan in place? Who "owns" the data security risk function in the organization, and how does each individual stakeholder understand his/her role in the cybersecurity arena?

Developing formal responses to questions like these will help you determine next steps in managing risk.

2. Reduce Risks Associated with Behavior Through Better Education, Awareness and Training

While hackers receive the most attention from the press, data and/or device misuse by well-intentioned insiders is still a leading cause of compromised information. Trusted insiders often are granted access to an organization's most sensitive data without a proper understanding of the information security policies and procedures that govern usage. This problem can be remediated by an effective security awareness training program, which can transform a serious vulnerability represented by ill-informed employees into an important asset.

Employees should be aware of common attack vectors specific to their industry, and they should be provided with examples of attempted or successful attacks on their company and on similar organizations. They should be aware of the potentially far-reaching consequences of a data breach, and they should be taught to recognize suspicious behavior, suspect emails and other signs of potential trouble. Putting employees through regular mock breach scenarios can be a good way to determine the adequacy of response times and to evaluate existing procedures.

3. Implement Best Practices for Enterprise-wide Collaboration on Cybersecurity Protocols and Processes

If you experience a major breach, you can be sure that regulators will scrutinize your cybersecurity program in agonizing detail. Proactive organizations will have instituted a series of best practices based on industry standards and regulatory guidance. Do you have a thorough and up-to-date information security policy and business continuity plan? Can you provide detailed documentation of your organization's identification and assessment of cybersecurity risks? What policies and procedures govern risks associated with third-party vendors? Do you adhere to published cybersecurity risk management process standards in protecting your network?

If your organization cannot provide clear answers to these and other questions, and quickly produce detailed documentation to back it up, you still have work to do.

4. Defuse Any Potential Competition Among Business Units for Budget and Other Resources Related to Cybersecurity

Ideally budgets, personnel and other resources should be allocated specifically for cybersecurity and incident response, rather than being subsumed under the umbrella of IT or another department. Territorial fights within the organization undermine the goal of a creating a collaborative culture and a unified, proactive approach to addressing information security risks. Stakeholders need to recognize that a serious data breach puts the entire company at risk. The responsibility for managing that risk must be shared across functions and departments.

Jason Straight is the senior vice president and chief privacy officer at UnitedLex. He has more than a decade of experience assisting clients in managing information security risks, data breach incidents, data privacy obligations and complex electronic discovery challenges. Prior to joining UnitedLex, he held numerous leadership positions at a leading global investigations and cybersecurity company, most recently as a managing director in the cyber-investigations practice. He began his career as an attorney at Fried, Frank, Harris, Shriver & Jacobsen in New York. As a recognized domain expert and Certified Information Privacy Professional (CIPP), he is a frequent speaker and author on topics relating to data privacy, cybersecurity, data breach response and computer forensics.

UNITEDLEX

information@unitedlex.com