News & Media

Attacking Cybersecurity from the Inside Out: Part II
11/14/2016
Articles & Alerts

Last week in the first installment of our *Attacking Cybersecurity from the Inside Out* series, we outlined the steps a company's board and executive leadership should take to prioritize cybersecurity. In this second installment of the series, in conjunction with the launch of Buchanan's online cybersecurity portal, the Buchanan BreachCoach®, we will explore how businesses can improve their cybersecurity strategy by enhancing their processes and cyber protocols at the employee level.

Vulnerabilities in the Human Firewall: Investing in People Not Just Technology

Cyber breaches and attacks aren't just about losing data, they're about losing dollars. IBM's 2016 Ponemon Cost of Data Breach Study found that every cybersecurity incident costs a company about $4 million. It's a number that may encourage businesses to go out and spend more on bolstering their cyber defenses. But, most cyber breaches are not the result of malicious outside attackers cleverly circumventing security systems. In fact, current and former employees are the largest source of cybersecurity incidents according to PwC's 2016 Global State of Information Security report. Whether a cybersecurity risk stems from accidental exposure or intentional theft, businesses that invest heavily in cybersecurity technology but neglect to engage with, educate and train employees are missing a critical component in their cybersecurity plan.

Ultimately, the effective management of employees to ensure increased cybersecurity can be boiled down to a strategy using the following three "I's."

- **Invest** - Most companies rarely hesitate to invest in new security systems and software. They believe this is the most essential part of preventing cyber-attacks. But the same investment made in technology needs to be made in employee trainings and awareness. A robust technical firewall will not protect you from an employee who unwittingly downloads a suspicious attachment or shares a work-related password. Employees need to be educated on what behaviors are risk-enhancing and what specifically they should be doing to diminish cyber risk. Outside consultants can help with this task, but even a company's own internal IT team can be empowered to run sessions and meetings to educate other employees.
- **Insulate** - Once an investment has been made to train employees on basic best practices, companies need to put strict rules in place to make sure that those best practices are followed. This will further insulate the company from breaches. Safeguards, such as a ban on unapproved software downloads, can have a significant impact in minimizing cyber risk. Policies should also regulate the use of hardware to make sure that it is not used on unprotected networks or handled carelessly on trips or at home. These policies and procedures shouldn't be limited to placing rules on current employees. Departing employees need to be given clear guidelines on what information or sensitive data is proprietary before they leave the company. Additionally, companies can put protocols in place to make sure that IT teams quickly and efficiently reset passwords, remove access and lock out departing employees from networks and programs. This will protect from the rogue former employee that may look to steal company information or files for their own gain.
- **Integrate** - Policies and best practices aren't worth much if they are not reinforced and reviewed regularly. Constantly reminding employees of cybersecurity policies and protocol keeps these measures top-of-mind. Posters can be put up in the office or emails can be sent out weekly with cybersecurity tips and rules. When employees are also informed of current risks and emerging trends in the cybersecurity space, they are more likely to integrate protection procedures into their daily routines and be able to identify potential cybersecurity threats before they become a true crisis. The ultimate achievement for a company is to have a culture in which every employee takes personal responsibility for their own cyber behavior and talks about cybersecurity regularly with others. This is true integration, and it only becomes possible with constant reinforcement over time.

Related Information

Professionals

Matthew H. Meade

Sue C. Friedberg

Pamela E. Hepp

Katelyn L. Diehl

G. Calvin Hayes

Practices

Cybersecurity & Data Protection

Employees who are educated in cybersecurity protocols and policies become an asset instead of a liability for companies. Without the practices described above, they can become the source of cyber-insecurity, knowingly or unknowingly. Though the threat of a cyber-attack can never be fully eliminated, by integrating these best practices, a company can minimize the risk of an employee-enabled cyber breach.

Next week, we'll take a look at the cybersecurity risks introduced by third-party contractors and how a company can mitigate those threats.

Buchanan BreachCoach® is a new online portal providing you with the latest articles, tools and insights to help protect your business from cyber attacks and their aftermath. Through the Buchanan BreachCoach®, you'll have direct access to our team of cybersecurity lawyers as well as helpful tools like our data breach cost calculator, which will give you a better understanding of the negative financial impact a data breach could have on your business.