News & Media

Attacking Cybersecurity from the Inside Out: A Four Part Series
11/8/2016
Articles & Alerts

In a world where the nature of cyber attacks are changing nearly every day, the ability to keep up with the latest information and cybersecurity best practices can be challenging, even for cybersecurity experts. As we launch Buchanan's online cybersecurity portal, the Buchanan BreachCoach®, we want to give you an inside look at some of the content we'll be sharing on this portal through a four part email series, "Attacking Cybersecurity from the Inside Out."

One of the critical things to understand about cybersecurity is that no business is immune from being attacked. But while it's impossible to completely negate the threat, having systems in place to minimize risk and to respond more appropriately when attacks happen can make a huge difference to a company's legal exposure and its bottom line. In this series, we will look at specific areas where businesses can improve their cybersecurity strategy -- not by investing in the latest technology, but by improving their own internal processes.

"IT" Starts at the Top: The Need for Management and Board Oversight

While board and executive oversight of cyber issues is improving, cybersecurity is still not viewed as an enterprise-wide risk management issue at many companies. According to PwC's 2016 Global State of Information Security report, 46 percent of companies do not have a Chief Information Security Officer (CISO), and 55 percent of corporate boards do not participate in the overall security strategy of their companies. It doesn't take much digging through recent headlines to understand why these numbers are concerning. Even for non-technology companies, breaches of sensitive or proprietary information can threaten to upend deals, damage reputations or even bring down a business.

Needless to say, executives and boards need to make cybersecurity a top priority. Here we will outline four critical steps every company's executive team and board should take to prioritize cybersecurity and mitigate the risks of a cybersecurity breach.

1. **Develop a cyber risk management plan**. Every company should have a comprehensive cyber risk management plan in place that identifies the company's critical data, maps the flow of that data within a company's mainframe, analyzes potential risks and establishes cyber attack response plans. This one-stop document provides leadership with a clear picture of a company's cybersecurity universe, making it easier to identify weak spots and bolster defenses.
2. **Establish a cyber risk management team**. Too often, the responsibility for managing cybersecurity falls on a company's IT team. In reality, cybersecurity is a significant business issue, and a full risk management team should be established to address cybersecurity specifically. The team should include representatives from different business functions, including legal, human resources and communications. It should meet regularly and brief the full board and executive team to ensure everyone at the top understands the company's security protocols, current risks and response plans.
3. **Put together an outside network of expert adv**isors. It's unrealistic to think that any business on its own can be up-to-date on every emerging trend in cybersecurity, especially if its core business is not technology. Outside consultants in technology, law and risk management should be part of the mix in addressing cybersecurity needs and challenges. They can help stay on top of the latest happenings so executives don't have to.
4. **Collaborate with others within your industry**. Outside experts can give you insight into new strategies and approaches, but others within your industry can more easily relate to the internal challenges you face. While there is often reluctance for many business leaders to work with competitors, when it comes to cybersecurity, everyone is better off with open sharing of information. Executives should talk regularly with other business leaders within their industry about cybersecurity

Related Information

Professionals

Matthew H. Meade

Sue C. Friedberg

Pamela E. Hepp

Katelyn L. Diehl

G. Calvin Hayes

Practices

Cybersecurity & Data Protection

issues. These other leaders may be able to offer more specific advice on threats they've faced and how to deal with them.

For a company to be vigilant about cybersecurity, the board and executive team need to set the tone. When they make cybersecurity a priority, it becomes a priority for the company as a whole. Though the threat of cyber attack cannot be completely eliminated, by taking the steps outlined above, a company can minimize the risks and, in the event of an attack, be positioned to address the threat quickly.

Next week, we'll take a look at how a company's own employees might be its biggest cyber risk and provide strategies for managing them appropriately.

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.