Cybersecurity

Matthew H. Meade / Sue C. Friedberg / Pamela E. Hepp /
Katelyn L. Diehl / G. Calvin Hayes

Attacking Cybersecurity from the Inside Out

No Business Is Immune, But Having Systems in Place to Minimize Risk and Respond Appropriately Can Make a Huge Difference

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 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

All five co-authors work in the Cybersecurity & Data Protection Practice of Buchanan Ingersoll & Rooney. **Matthew H. Meade** can be reached at 412/562-5271 or by email at matthew.meade@bipc.com. **Sue C. Friedberg** can be reached at 412/562-8436 or by email at sue.friedberg@bipc.com. **Pamela E. Hepp** can be reached at 412/562-1418 or by email at pamela.hepp@bipc.com. **Katelyn L. Diehl** can be reached at 412/562-1883 or by email at katelyn.diehl@bipc.com. **G. Calvin Hayes** can be reached at 813/222-1136 or by email at calvin.hayes@bipc.com. For more information, go to www.bipc.com/Cybersecurity.

The information in this article is for informational purposes only. It is intended to alert the recipients to developments in the law and does not constitute legal advice or a legal opinion on any specific facts or circumstances. The contents are intended as general information only. You are urged to consult your own lawyer concerning your situation and specific legal questions you may have.

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 advisors.** 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 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.

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.

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.

Your Friend Or Your Worst Enemy: The Risks of 3rd Party Contractors

According to PwC's 2016 Global State of Information Security report, third-party contractors are the biggest source of security incidents outside of a company's employees. In fact, the well-publicized Target hack of a few years ago was made possible thanks to system vulnerabilities of one of the company's third-party contractors. The result was 40 million exposed customer credit card numbers and cost Target well into the hundreds of millions of dollars.

As we've said throughout this series, there is no cybersecurity silver bullet, but there are critical administrative actions company executives can and should mandate that are as important to thwarting cyber risks as technical IT protections such as firewalls and intrusion detection software. When it comes to cyber risk mitigation with third-party contractors, here are the straight A's of best practices.

- **Analyze Potential Third Parties' Security Capabilities** — Performing a risk analysis of a potential vendor is a necessary part of the vetting process. A company should establish upfront what kind of access the contractor will have to their system and make sure the company maintains full oversight of that access. A potential vendor who will have significant access to legally-protected or company confidential information should have a cybersecurity program that is certified by a reputable and independent certification organization. A vendor that has not obtained such a certification is not a qualified candidate, regardless of their capabilities and costs. The risks are just too great.
- **Adopt Service Level Agreements** — Before a company begins working with a third-party contractor, a service level agreement (SLA) should be created and agreed upon. An SLA is more than just a bare bones definition of the work to be done. It's a company's opportunity to demonstrate that cybersecurity is a priority and articulate what the vendor needs to do to meet the company's security expectations. Spelling out specific security obligations is important to ensuring the third-party knows and fully understands what is required of them. This list of specifics should include information privacy, confidentiality and security representations, indemnity, internal risk analysis expectations, audit rights, breach notification requirements, cyber liability insurance, and the parameters of network and data access controls.
- **Assess Third-Party Vendors Regularly** — Although the SLA should give the company the right to audit a vendor's security, many companies are not in a position either to conduct a vendor audit or engage an independent expert to do it for them. Requiring a current independent security certification is a reasonable way for the company to have confidence that its vendor is maintaining appropriate security measures. A company also should establish an internal list of "triggers" — actions that, if perpetrated by the third-party vendor, prompt a closer review of the vendor's security measures. Triggers are actions that are symptomatic of an organizational problem, such as a performance issue or indication of financial distress, that could signal the development of a cybersecurity risk.

Establishing and monitoring a company's own cybersecurity program is one challenge; ensuring that each of a company's third-party contractors is doing the same is another. By following the steps outlined above, every company can be best prepared to mitigate third-party cybersecurity threats. These steps, along with those outlined for employees and executive management, come together to form the strongest trio of defenses any company can have when it comes to cybersecurity.

This article features parts one, two, and three of a four-part series on cybersecurity by Buchanan Ingersoll & Rooney. The final installment of this series looks at the real costs to a company — financial, reputational, and operational — of a cyber breach and can be accessed at www.bipc.com/cybersecurity.