plante moran

audit • tax • consulting • wealth management

Securing Your Information Assets

Dec 01, 2015

The majority of data breaches are avoidable, requiring an enterprise-level approach to protect your network.

The news headlines are replete with companies falling victim to cyber crime. Malicious intrusions and thefts have affected some of the largest brands, agencies, and institutions. Over the past several years, The Home Depot, Target, Neiman Marcus, eBay, Sony, JP Morgan Chase, Anthem Health Insurance, and the Internal Revenue Service (among thousands of others) have all incurred breaches that collectively compromised customer data associated with hundreds of millions of customer records, at great cost to both the company and consumer.

For Target Corp., whose 2013 data breach affected more than 40 million credit- and debit-card accounts, the tally continues to escalate more than two years later. In early 2015, retail experts estimated the company's net expense at addressing the breach at nearly $200 million—and that was several months before the retailer had reached a $67 million

reimbursement with Visa to compensate financial institutions for their associated costs.

Then there's Heartland Payment Systems, which agreed to pay the major card companies $100 million to settle its 2008 data breach. The list of business goes on, as do their associated costs.

According to the Ponemon Institute, an organization that conducts research on privacy, data protection, and information security policy, the average cost of a data breach last year totaled $174 for each compromised record — a 9 percent jump from 2013.

"With the increasing cost and volume of data breaches, IT security is quickly moving from being considered by business leaders as a pure technology issue to a larger business risk," Ponemon announced. "This shift has spurred increased interest in cyber insurance."

It was against this backdrop that Joe Oleksak, Plante Moran information technology consulting partner, cautioned attendees at the firm's Sixth Annual Insurance Conference, held Oct. 22, 2015, at the University Club of Chicago. "There are vulnerabilities that we know are out there and we're still getting bit by them," he said.

The problem is pervasive, Oleksak said, with a cost per-record stolen ranging from nine cents to $254. And in less time than it takes to refresh your browser, attackers can infiltrate a network. "In 38 percent of cases, it took attackers just seconds to compromise systems," he said, "and a great number then exfiltrate that data in just minutes."

Compounding that vulnerability is an inability to detect the breach, which can take days or even months. "The detection deficit continues to grow," Oleksak said. "In more than a quarter of cases, it took several days [or] months for organizations to discover a breach."

And the technical disadvantage exists irrespective of company size.

Indeed, in 2014, Verizon discovered vulnerabilities that were seven years old. “We’re having trouble doing something about it because we don’t notice them,” Oleksak said. “We have detection and intrusion protections but those are all signature-based. And between 70 and 90 percent of malware have unique signatures, making systematic detection almost impossible.”

Victims of Opportunity

The vast majority of breaches — 97 percent, according to a Verizon Data Breach Investigations Report — are avoidable and the result of three major lapses: user ignorance, a weak infrastructure, and vulnerable technology.

User Ignorance

“Employees are exercising poor judgment by using weak passwords,” Oleksak said, the No. 1 lapse that leads to system vulnerability. There is a great deal of uncertainty about what it means to create a secure password, which isn’t a reflection of obscure symbols and alternating letter cases. Because cracking systems today can generate over 300 billion attempts per second to guess a password, even the most random sequence of uninterrupted characters can be hacked within 24 hours. “On the other hand, it might take several years to guess a password that’s a phrase, such as ‘Apples taste better than grapes!,’” he said.

Additionally, phishing attacks are successful when vigilance wanes. “Teach your employees to stop clicking random links,” Oleksak advised. “You don’t have an opportunity

of a lifetime, and you didn't win the Malaysian lottery. Hit delete."

Weak Infrastructure

"Most companies have a flat network that is easy to compromise," Oleksak said, "making it easy for a hacker to explore and take what they want." To counter this, Oleksak recommends segregating internal networks into zones (VLAN) based on data sensitivity, multi-factor user authentication, and encryption technology where appropriate, and then periodically testing your people, processes, and technologies (information security) to understand your current exposure. He also recommends avoiding free cloud sharing platforms such as Dropbox and Google Drive, public portals that easily enable unintentional and unintended data loss.

Vulnerable Technology

While owning the latest and greatest tech gadget would seemingly imply advanced security, Oleksak said that's not necessarily the case. "Attacks on mobile devices are rising." Whether that's through malicious code integrated into an app or by an operating system that has not installed the latest security updates, hackers have created a cat-and-mouse game where, to date, they have managed to stay ahead of the game.

Enterprise-Level Approach

While some companies will become a target of cybercriminals regardless of their safeguards, "most become a target because of what they don't do related to security," Oleksak stressed. And there are a handful of best practices for monitoring and maintaining the security of your network. "Most victims aren't overpowered by unknowable and unstoppable attacks. We know them well enough and we also know how to stop them."

The approach is not reserved for a dedicated IT department, though; rather, Oleksak maintains that “to be truly effective, information security must be embraced at the enterprise level and not relegated to the IT department. Executive management especially must embrace that directive.”

To accomplish that, Oleksak recommends following a five-step approach that combines equal parts reactive and proactive processes:

1. Identify what you have
2. Protect what you identify
3. Detect direct and indirect attacks
4. Respond accordingly
5. Recover appropriately

“Information security is not an IT issue but a business issue,” Oleksak stated. “As such, it must include people, technology, and processes.” To ensure success, the company must allocate adequate funding to implement the requisite security protections and procedures.

There is no “one size fits all” or “set it and forget it” solution. Anyone who says they have a product like that is just selling you something. It’s an ongoing process, one that extends far beyond technology. “Information security does not end,” Oleksak said. “It can only be maintained, which comes about through constant vigilance, training, and reassessment.”