Business Magazine Greenville

Your Business Resource for Greenville Metro and Upstate South Carolina

SC Department of Revenue Security Breach Eye-Opener

By **Dana W. Todd**
November 30, 2012

When you turn out the lights at the office each night, do you lock the door? Do you activate a security system as you exit the building? Is your password-protected computer shut down?

What happens when 3 a.m. rolls around and a thief jiggles the door handle, flashes a light in the office window, or sits down at a laptop to decode your server password? Is your company protected? Many businesses may have a false sense of security.

Whether you own or work for a small or large business, it's mandatory to take precautions to protect company property and customer details. An increasingly large percentage of that precious property is electronic.

The SC Department of Revenue (SCDOR) and Gov. Nikki Haley's office are trying to mitigate the effects of the recently successful hacker attempt and subsequent extraction of 3.8 million South Carolinians' personal tax returns and financial information, as well as 657,000 business tax returns from the Revenue agency's databases. Were the best protocols in place to protect sensitive information of the agency's customer base, an entire state full of taxpayers? Time will tell as investigations proceed, but there are lessons to be learned from this debacle that can be applied to businesses.

Jim Lippard, EarthLink's senior product manager for security and technical editor of "Extreme Exploits: Advanced Defenses against Hardcore Hacks," says there are two areas of concern regarding the SCDOR security breach.

"I would be concerned about the delay from the compromise to the discovery and the fact it was a third party [Secret Service] that notified them," Lippard says. "That is indicative the monitoring and analysis in place was not adequate to discover it themselves. That's something very common in businesses. I think what we're starting to see now is that organized crime is very active in going after specific targets as well as targets of opportunity.

"It has become evident to security professionals over the last decade that the old model to build our walls and our defenses, put them in place, and just assume we could forget about them is not OK. It has become very evident we need to have monitoring capability … something that is being checked regularly. Before, we would just put a security device at the perimeter of the network and monitor the traffic going in and out. If it detected something, we would respond. Now we know we really need to monitor things internally as well and collect logs from different systems. We need to understand what the normal traffic and behavior of our systems looks like so we can see when strange things happen."

It is difficult to ascertain what monitoring was ongoing at SCDOR, as agency spokesperson Samantha Cheek responded to questions about security staffing, budgeting, and procedures via an email stating, "Certain details cannot be disclosed at this time as the criminal investigation is still ongoing."

The agency apparently has some compliance with the PCI data security standard, which requires all organizations accepting credit cards to implement specific security measures to protect that information, including encryption or number truncation, where only the last four or first four digits of the card appear in the database. Gov. Haley reported the vast majority of compromised credit cards were encrypted. Of those unencrypted, she confirmed at an October 30 press conference they were all expired cards.

"There's a difference between compliance – which is doing what is necessary to meet a regulatory requirement – and security," Lippard says. "What weren't encrypted were the Social Security numbers and tax returns. This shows there is value in applying security even if there's not a specific compliance requirement that you do so. Part of best practices is to identify the pieces of information that are critical to you as a business and to your

customers that they're going to feel violated if it gets exposed. You want to consider all of those things as part of a security program."

"If credit cards are exposed, there is no liability. Social Security numbers are the keys to our identities and the keys to applying for open accounts. You could spend months paying for a breach," says Derek Brink, vice president and IT Security research fellow with Aberdeen Group, an international analyst research firm. "I do find it to be irresponsible," he says about the SCDOR's lack of encryption of the database(s) containing Social Security numbers.

Many businesses have a firewall-and-forget-it mentality, which no longer works, says Brink.

"For many organizations, network security consists of a firewall, and endpoint security consists of anti-virus software," Brink says. "Literally everyone has a firewall today. Over time, firewalls have holes punched in them from every email and web traffic occurrence. Cloud computing [where applications and data reside on third-party servers for remote access] pokes hole through the firewall. A traditional firewall is a porous perimeter. Network security based on firewalls alone is not enough."

In an April 2012 Aberdeen Group white paper, the firm surveyed 146 companies to compare information security practices. Firewall-only companies spent four times more on information security due to inherent inefficiencies as compared to their corporate counterparts who implemented additional network security measures such as intrusion prevention systems. Similarly, a related white paper shows companies that only install anti-virus software spend 1.5 times more to protect their data.

"One of the main ways that hackers are gaining access to environments is by contacting employees through email, through IM [instant messaging], and through social networking and getting them to click on something. Then the local workstation is infected and the hacker is inside the environment," Lippard says.

Lippard, however, says small businesses may be at risk because of the high cost of technological solutions to protect data, the cost of the large network capacity necessary to effectively monitor traffic, and the high cost of hiring employees that know how to analyze the data captured by security software and systems. For those small companies, he says a managed security solution provider may be the answer.

According to attorneys, researchers, and experts in the information security industry, companies (and government agencies) should spend time focused on specific best practices in data security to protect information repositories.

Tom Vanderbloemen, partner at the Gallivan, White & Boyd law firm, advises his clients on legal best practices when dealing with personal information that requires protection:

(1) Understand the laws. Each industry and each state have different statutes and regulations that govern how organizations collect, store, and disseminate personal or financial data. The healthcare industry, for example, requires electronic patient health data to be protected under the Health Insurance Portability and Accountability (HIPAA) Act.
(2) Understand how customer information is handled internally. Who has access to the information stored in databases and on mobile devices? How is it managed?
(3) Communicate with customers. Transparency in operations enables customers to acknowledge they want and need services in the manner in which the company is providing them.

"Organizations should expect to be attacked and be proactively trying to protect data. A consistent theme in this discussion is that companies should not simply push this problem onto IT staff and forget about it," says Vanderbloemen, who focuses his practice on electronic discovery, governmental liability, and intellectual property. "The help of competent IT professionals is certainly critical, but the risks involved deserve the attention of the highest levels of business."

Lippard stresses best practices in information security should address:

- A defense against known attacks and attackers.
- Multiple layers of security.
- An ability to detect abnormal activity, the key area that led to the SCDOR breach.
- Physical security, which includes cloud computing servers at third-party vendor sites and systems within the company's physical boundaries.
- Access control, or management of who is accessing what information internally.

He estimates through his work with companies and government organizations of all sizes that an average security-savvy company spends from one to five percent of its total technology budget on information security.

"Look at what you are spending on IT. Are you spending at least one percent for some kind of protection, whether that's a managed security service, monitoring software, or security equipment?" Lippard says. "If you see what you're spending on security is 0, you might want to think again about what you're doing."

Waging War

“It is a constant battle between attackers and defenders. Attackers generally have the easier time of it because as new technologies are rolled out, we discover what the security issues are. Then we develop the methods of securing them,” says Lippard. “I think we’re going to see a lot more of a hybrid approach where software developers and security end up being combined in interesting ways. Unfortunately, that’s a skill that’s rare – the combination of being a good developer and having the security-breaking mindset.”

Although Gov. Haley’s assertion that, “No one person in DOR could have avoided this hack” may be a stretch, Lippard agrees with Gov. Haley’s assessment that, “It’s the new life we live in.”

“There’s not a company on the planet that doesn’t have vulnerable systems out there,” he says. The problem is that organized crime is a few years ahead of companies because hacking into databases is a business model priority. Government agencies are probably a few years behind corporations in learning how to thwart breach attempts, according to Lippard.

Waging a cyber war requires savvy soldiers, but with a shortage of qualified IT professionals – especially those who have added information security expertise – hiring is difficult. It’s even more difficult to find IT employees who talk the language of business executives. Without a common understanding of security risks and monitoring/prevention solutions, proper security analysis and implementation may suffer, according to Brink.

For business owners and HR managers responsible for hiring, Lippard advises looking for security certification verification beyond job candidates’ résumés, searching online to find out about their reputations, and talking to former customers.

“If you can find somebody that can act in a trusted advisor role, that’s also incredibly valuable,” he adds. “Having a division between the person who is building the technical solution for you and the person who’s evaluating it or making the recommendation – that kind of division of responsibility is a helpful thing.”

Being prepared and vigilant is the only way to win the daily battle to protect corporate and government information from those who would steal it. The investment to secure data is an unrewarded risk, but it’s a choice organizations make by the budget they spend, the people they hire, and the procedures they establish to deal with personal data. In the IT world, regulatory compliance doesn’t equal security. Budgets must be allocated to deliver superior results against what hackers can do to erode your customers’ level of trust in your organization.

According to “Best Practices for Managing Information Security” by IT Policy Compliance Group, organizations with the best outcomes against attempted hacker attacks have a few things in common, including: a chief information security officer who is in charge of all information security, standardized and automated procedures and controls, a quality assurance program, and measurement and reporting that occurs daily, weekly, and monthly.

In a September 28 blog post, Brink writes, “I have bemoaned the fact that as end users, we clearly should stop being so stupid and eliminate the likes of ‘password’ and ‘abc123’ as our passwords. At the same time, however, we really should expect world-class brands … to implement the most basic best practices and protections for our data, including **salting and hashing for our passwords**, and scanning and testing to find and fix the most common application vulnerabilities. And yet the natural forces between buyers and sellers did not cause this to be – until after a breach.

“I asked the larger question: is industry capable of self-regulation on these matters, or will corporate incompetence and indifference continue to invite stronger regulatory mandates?”

Submit a comment

Comments (0)

View All | **Editor recommended** | **Reader recommended**

Home | **People** | **Companies** | **Industries** | **Opinions** | **Resources** | **Directories** | **Events** | **Magazine**

Support: support@greenvillebusinessmag.com