SMALL BUSINESS

The Big Effects of Cyber Attacks on Small Businesses

A look at the unique cyber vulnerabilities that SMBs face, and how they can mitigate data breaches with an inside-out approach to information security

Greg Sullivan • Jun. 11, 2014

The data breaches that most often make splashy headlines affect large companies and compromise millions of customers, such as the attacks against Target and eBay. Data possessed by small businesses can be just as valuable and, in some cases, much more so.

Small business owners and operators understand that the impact of an embarrassing or costly data breach can mean much more – up to and including loss of livelihood or the entire business enterprise. The majority of attacks target small and medium-sized businesses because they are typically much more vulnerable than large enterprises, and the effects can be devastating.

Traditionally, we stand up network or endpoint defenses, such as firewalls, spam blockers and antivirus software, intended to keep the bad guys out. But these don't always work and hardening the outside does little to protect data once an attacker inevitably breaks through those defenses, and does even less when data is acted upon by a malicious insider or for data stored in cloud-based applications like Dropbox and Salesforce.

Monitoring where files exist, where and how they are move, and by whom inside and outside the network is critical to immediately identifying an attack and preventing information loss.

The Verizon 2013 Data Breach Investigations Report found that 62 percent of breaches impacted smaller organizations, and that number is likely conservative because it assumes an organization is even aware it has been breached. Cyber attackers no longer hack systems simply to achieve notoriety. They run their operations like a business and want to find ways to maximize the return on their investments.

That makes small businesses, which typically do not have the IT resources or expertise to implement and manage security systems, prime targets. A Ponemon Institute survey reported that one-third of respondents admit they are not certain if a cyberattack occurred in the past year, and 59 percent of SMBs say they do not have sufficient IT experience.

The increased adoption of cloud-based services like Dropbox, Salesforce, and Evernote also opens organizations up to potential breaches because sensitive data is stored and accessed outside the network. Not using cloud computing services is not really an option because they do offer significant benefits in terms of improved productivity and collaboration. That's the Catch-22 of cloud computing: cost effective and easy to use, but can increase the possibility of a costly data breach.

The "Bring Your Own Device" era is another factor to consider as employees access 46 percent of an organization's business-critical applications from their mobile devices (Ponemon Institute). These devices typically sit outside the established security controls and allow cyber thieves to follow your data.

When a large company endures an embarrassing and costly data breach, it will suffer financial losses and damage to its reputation. When a small company is attacked, it may never recover. An attack can set a small business back anywhere from $54,000 to $101,000 per incident (CNBC). PCWorld in August 2013 reported that of the small businesses who suffered a breach, roughly 60 percent go out of business within six months after the attack.

Symantec's recent admission that antivirus software is "dead" is also an admission that the traditional approach of hardening the network and data center is also dying, particularly as companies move their data to cloud-based services. What's necessary now is doing the opposite and taking an inside-out approach: protect the data itself

rather than trying to block access to it. Monitor sensitive data, no matter where it is stored, to track who's sending it and where it's going based on rules set by the specific company to block unauthorized attempts to access and/or send a file.

Additionally, every business, large or small, should have a comprehensive security training program in place for employees. This involves not leaving files open or unattended, and making sure to shut down unsecured devices like a smartphone or tablet. Also, classify your employees based on what they can and cannot access on the company system. Not everyone needs to have access to all cloud applications. Additionally, each employee should have a different and strong password for all accounts or services.

In a perfect world, a prevention plan is all you would need to avoid a breach. However, the stark reality is that an attack can happen despite your best efforts. Every small business should have a crisis management plan in place that centers on transparent communication between management, employees, stakeholders, customers, and anyone else who may be affected. Choose an internal employee to be the face of the company, and who will be the go-to person for updates and information.

The way we share, store, and access data is always evolving, and it is important to keep up with the changing landscape by reviewing your system on a monthly, quarterly, or annual basis depending on your security needs. In the meantime, we should all take steps to drive to drive up the cost of doing business in our enterprise for the cyber thieves. It's possible to do this, in an affordable and straightforward manner, by paying attention to the same thing the cyber thieves do – your data.

———————

Greg Sullivan, is Chief Executive Officer for Global Velocity, a company pioneering new approaches in securing information. Mr. Sullivan is recognized as an industry expert and visionary in the field of cybersecurity.

He is the retired Founder & CEO of G. A. Sullivan formed in 1982, that he built it into a leading software development company. After managing the company's growth for more than 20 years, with operations across U.S. and Europe, he sold G. A. Sullivan to Avanade., a company jointly owned by Microsoft and Accenture. G. A. Sullivan appeared for four consecutive years on the Deloitte & Touche FAST 500 list of fastest growing technology companies in America, and three years on Inc. Magazine's Inc. 500 list of fastest growing private companies in America. Ernst & Young named Sullivan a 2000 Entrepreneur of the

Year in the software/information services category and the U.S. Small Business Administration named Sullivan the 1999 National Small Business Person of the Year.

Small Business • Technology • Global Velocity • Data Breach • Data Security • Small Business

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.