SSBG IT Solutions

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

Small Business IT Security: Save Money, Save Face

A few strategic steps can ensure that limited IT budgets don't increase cybersecurity risks.

By Mark Lachniet
Mark Lachniet manages CDW's Solutions Practice for Information Security.

As a security analyst and licensed private investigator, I have often performed computer forensics work in the aftermath of a security breach. The work provides up-close-and-personal views of the many consequences of cybercrime.

Gone are the days when most hackers seek to wreak havoc by defacing a victim's website or by using it to host pirated video, audio or pornographic content. Make no mistake: Cybercrime today is serious business, conducted by professional thieves with impressive technical resources and expertise. Intellectual property, sensitive financial data and valuable customer records are all at risk, and **data breaches result in direct and indirect financial losses for thousands of businesses every day**.

One statistic drives home all that small and midsized businesses are up against. As a group, they report far fewer security incidents each year than their enterprise peers, according to Verizon's "2015 Data Breach Investigations Report"; however, the impact a small business faces following such a breach usually proves far greater, with **more than 82 percent of incidents resulting in data losses**. By contrast, only **about 1 percent of larger enterprises** suffer the same fate (see Page 3 of the report for details). That reality is particularly disconcerting for smaller companies without extensive IT staffs or deep security expertise (and healthy budgets). SMBs can't afford to — and shouldn't — settle for second-best security. Here I'll share four guidelines to help small business owners understand where their greatest vulnerabilities lie, and how to budget more strategically to see the greatest results.

1. Can you identify what's at risk?

Identify the most important assets that, if stolen, would cause the most harm. Consider direct financial costs from stolen bank account information, as well as the loss of trade secrets that may give competitors an unfair edge. **A breach may cause productivity to plummet** by forcing a company to shut down a mission-critical system, making it impossible to deliver products or services.
Don't forget about contract violations: An organization that can't deliver on time may face stiff financial penalties. **Compliance violations related to PCI DSS, HIPAA or other regulations are also possible**. One good way to identify these resources that is often used in Business Continuity Planning is to perform a Business Impact Analysis or BIA. Many examples of BIA methodologies are easily found, including those from ISACA.org, which maintains the Certified Information Systems Auditor program.

2. Hack yourself, before someone else does

I strongly recommend that SMBs hire a trusted partner to perform a penetration test, which can uncover a wealth of valuable information, starting with the business systems that are most vulnerable to thieves breaking in via the Internet. Our CDW security experts have proved themselves alarmingly successful when they perform such tests — **they gain administrator access nearly 95 percent of the time when connected to the target's internal network**, even in the case of large and well-organized companies. Once that happens, they essentially have the keys to the kingdom, including access to the most sensitive data.

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

Penetration tests look at far more than missing patches and tend to emphasize vulnerabilities in technologies and user behavior such as trust relationships and poor passwords.

3. Perform a gap analysis

A penetration test can identify the areas that require the most security-based attention. Responses may include **enacting better procedures to ensure that software patching will be performed** on a more consistent or more thorough basis, or updating user provisioning and access policies. Other improvements may involve shoring up data backups and continuity of operations to limit the damage of a successful breach. Company leaders should gain a clear understanding of just where to put their attention and how best to focus security spending.

4. Take advantage of free resources

The National Institute of Standards and Technology, a federal agency, offers a wide range of detailed cybersecurity guidelines. Two of those are of particular importance to SMBs: NIST 800-30, a comprehensive guide for conducting risk assessments, and NIST 800-53, which details the security and privacy controls used by the federal government. Both can **help IT managers improve their own comprehensive security strategies** or more thoroughly evaluate partners they're considering to hire for the task. (To learn more about this process, check out the CDW white paper "Running a Successful Security Assessment Project.")

No matter what course of action they take, SMBs should not allow a limited budget to limit their security planning, especially when many steps can be taken for little or no cost.

To learn more about the four key technology trends small businesses should be following this year, check out, "Small Businesses Must Heed Cloud, Security, Mobility and IT Services Trends in 2016."

About the author:
Mark has a long experience focused on computer security and crime. His objective is to assimilate new topics and academic pursuits, and finally to make this information readily accessible to others through presentations, whitepapers, etc.

Specialties:Vulnerability assessments and penetration testing, Web Application security, security policy development, incident response and forensic analysis, interfacing with legal and law enforcement professionals, teaching, Linux and open source software

From his LinkedIn profile:
https://www.linkedin.com/in/mark-lachniet-225b5a3

Original Article published - http://www.biztechmagazine.com/article/2016/03/small-business-it-security-save-money-save-face - March 2016