SOLUTIONS FOR SMALL BUSINESS

Report Series

2010 SolutionsforSmallBusiness.com

Produced by BizTechReports.com
Editorial Director: Lane F. Cooper
Research Director: Felix Gorrio
Senior Editor: Susan Aluise

# Cyber Security Strategies for the Small Business Market

***Solutions for Small Business Reports are designed to demonstrate how new technologies enabled by cable providers help small business owners and managers address key challenges, solve problems and achieve mission critical objectives.***

***More resources, including a companion report on* Cyber Security Solutions for Small Business*, which compares cyber security services and tools offered by a variety of vendors, can be found at: solutionsforsmallbusiness.com***

## Cyber Security Strategies for the Small Businesses Market

### Introduction

It's no secret that cyber-intrusions and attacks – whether by viruses, malware, spyware, or other IT security breaches – are on the rise in corporate America. High-profile hacks on military computers and corporate domains like Google have illustrated that new cyber security challenges are emerging as fast as experts can combat them.

It's tempting to see cyber security as a problem unique to government agencies, large enterprises, or e-commerce players. While such sites are highly visible, cyber criminals are also paying closer attention than ever to so-called "soft targets" such as small businesses. Why? Because bad guys have learned they have more luck attacking unguarded small businesses than enterprise fortresses.

"Cyber crime is having enormous real consequences, which holds the potential to cripple businesses and services," says Steven Chabinsky, deputy assistant director of the FBI's Cyber Division, speaking at the GovSec/FOSE conference in Washington last March. "For those of you who aren't involved in IT security, it may be hard to understand why it is so difficult to secure an organization's computer system."

Chabinsky pointed out that businesses must address vulnerabilities both on the technical side and on the human side of the cyber security equation. On the technical side, businesses must secure a varied list of technologies, including web servers, e-mail servers, databases, firewalls, routers, embedded network devices, internal networks, remote access, custom applications, off-the-shelf applications, backup and storage areas, as well as telephone, PBX, and VoIP systems.

On the human side, organizations must secure their physical infrastructure, employee accesses and permissions, and connections to business and corporate partners. "These are just the basics on the way to a secure network, all of which need to be monitored and updated regularly, as the technologies change constantly and so do our users," Chabinsky says.

### Recognize The Risk

***The first step for small businesses is to recognize that they're at significant risk for cyber security threats and breaches.***

The first step for small businesses is to recognize that they're at significant risk. "Theft against our networks routinely occur while the front doors to our businesses and agencies remain well-guarded, the file cabinets remain locked, and the motion detectors remain undisturbed when we leave for the night," Chabinsky pointed out. "Nothing appears to have been touched, no less stolen wholesale. And, the criminals themselves don't seem to have faces or names."

As businesses large and small recognize that they are targets, more of them are rolling out IT solutions to protect their valuable assets. According to a recent study conducted by Forrester Research, 42 percent of large enterprises expect to increase IT security spending on new technologies by five percent or more this year, and 37 percent of small- and medium-size businesses (SMBs) expect to do the same.

 

"As we move out of the recession, we expect to see security investments continue to grow, although the nature of that investment is changing," noted Forrester analyst and vice president Jonathan Penn.

While data security is perennially the largest budget item for IT organizations, the greatest spending increases are in the area of network security, where 40 percent of enterprises and 36 percent of SMBs expect to spend more in 2010. More than 80 percent of businesses large and small identified the management of vulnerabilities and complex threats as a high priority in the coming year.

***The proliferation of consumer devices in the workplace means less central technology control, and increased risk of security problems.***

"The greatest concern for companies of all sizes is the proliferation of consumer devices in the workplace," Penn added. "In general, this follows the broader trend of IT losing centralized control of technology adoption, deployment, and use. It's not just consumer technology like iPods and the use of Facebook or Twitter; it also shows up in the uncontrolled proliferation of SharePoint [collaboration] sites by business groups or in the use of cloud computing services by application developers."

**Behind The Curve?**

While cyber security threats have risen dramatically, small businesses' awareness and the policies and products in place to protect them have not kept pace, according to the 2009 National Small Business Cyber Security Study. This study revealed that small businesses are increasingly holding valuable information online – 65 percent store customer data, 43 percent store financial records, 33 percent store credit card information, and 20 percent maintain intellectual property and other sensitive corporate content.

Moreover, 65 percent of businesses claimed that the Internet was critical to their success, yet they are doing very little to ensure that their employees and systems are safe from cyber security breaches. The study, co-sponsored by the National Cyber Security Alliance (NCSA) and Symantec, surveyed nearly 1,500 small-business owners across the United States about their cyber security awareness policies and practices. "While small business owners may understandably be focused on growing their business and the bottom line, it is imperative to understand that a cyber security incident can be disruptive and expensive," says NCSA Executive Director Michael Kaiser.

***Only 28 percent of U.S. small businesses have formal Internet security policies.***

NCSA found major gaps in the areas of security policies and employee education on security best practices. Only 28 percent of U.S. small businesses have formal Internet security policies and just 35 percent provide any training to employees about Internet safety and security. At the same time, 86 percent of firms do not have any staff solely focused on IT security. Among those small businesses that do provide cyber security training for staff, 63 percent offer fewer than five hours per year.

This lack of cyber security awareness and education leaves most U.S. small businesses at risk of losing vital customer and company data. The study found that more than nine out of 10 small businesses believe they are safe from malware and viruses based on the security practices they already have in place. However, only 53 percent of firms check their

 

computers on a weekly basis to ensure that anti-virus, anti-spyware, firewalls, and operating systems are up-to-date, and 11 percent never check them at all.

Small businesses are also largely unaware of the risks associated with wireless networks, NCSA found. Wireless networks are gateways for hackers and cyber criminals and must be secured by complex passwords. While 62 percent of the companies surveyed have wireless networks, 25 percent of them do not use password protection for these networks. This alone poses a significant security risk to affected businesses as hackers can easily steal information being passed through these wide-open networks.

"To the millions of very savvy entrepreneurs across our nation, our message is simple – being smart about the online safety of your employees, business and customers is a critical part of doing business," says NCSA's Kaiser. "Cyber security is not a nice thing to have for American businesses, it is critical to their survival."

**Online Banking Scams Pose Dangers For Small Business**

***Cyber criminals increasingly are targeting small businesses that conduct financial transactions online.***

"Go where the money is," the notorious bank robber Willie Sutton famously advised, "and go there often." His tech-savvy, 21st century brothers-in-arms seem to have taken that advice to heart. According to Marian Merritt, Internet Safety Advocate at Symantec, cyber criminals increasingly are targeting small businesses and nonprofits that conduct financial transactions online.

Popular tactics include what Merritt calls "spear phishing," which is similar to the common practice of phishing used against individuals, but with a twist: criminals obtain information about a small company's staff or members of a church or other nonprofit, then use those details to craft more sophisticated emails that appear more convincing. Dangerous links could be addressed to a company's administrator and contain the company's name or other details that cyber crooks can get from the company's website or via search engines like Google.

Merritt offers the following security advice to small businesses that engage in online transactions:

- Use complete and up-to-date security software.
- Ensure that operating systems and browsers are up to date, because many patches include security improvements.
- Never use links in emails to access a transaction or financial web site. Always type the URLs into browsers directly.
- Monitor online accounts regularly; set up fraud alerts and other safety measures from the bank or investment company.
- Never use a shared or public computer for financial transactions or even to check balances.
- Log out fully from a site when completing a transaction.
- Invest in a password manager such as Norton Identity Safe, which can defeat a keystroke logger by automatically filling in webpage passwords with encrypted data, or bypassing the keyboard entirely.

 

**Conclusion**

For small businesses that rely on the Internet and information technology, the cyber security challenge is one of balancing competing interests. In a tough economy, "a penny saved is a penny earned". But it's also true that "an ounce of prevention is worth a pound of cure." So how do small businesses best balance those seemingly competing interests when it comes to cyber security?

First, by coming to terms with the fact that cyber crime never sleeps. Small businesses are soft targets that increasingly are coming under attack. Here's the good news: there are affordable policies and products on the market that can make a big difference.

***The National Institute of Standards and Technology has developed ten fundamental steps to help small businesses protect their online assets.***

For example, below is a list of the ten fundamental steps developed by the National Institute of Standards and Technology (NIST) that can help small businesses to safeguard their IT "family jewels":

1. Protect information/systems/networks from damage by viruses, spyware, and other malicious code.
2. Provide security for your Internet connection.
3. Install and activate software firewalls on all your business systems.
4. Patch your operating systems and applications.
5. Make backup copies of important business data/information.
6. Control physical access to your computers and network components.
7. Secure your wireless access point and networks.
8. Train your employees in basic security principles.
9. Require individual user accounts for each employee on business computers and for business applications.
10. Limit employee access to data and information, and limit authority to install software.

**Sources:**

Business online banking
http://www.usatoday.com/tech/news/computersecurity/2009-12-30-cybercrime-small-business-online-banking_N.htm

Forrester Research
http://www.forrester.com/ER/Press/Release/0,1769,1320,00.html

National Cyber Security Alliancehttp://www.staysafeonline.org/content/2009-smb-security-study

National Institute of Standards and Technology, "Small Business Information Security: The Fundamentals"
http://csrc.nist.gov/publications/drafts/ir-7621/draft-nistir-7621.pdf

Stephen Chabinsky, deputy assistant director, Cyber Division Federal Bureau of Investigation GovSec/FOSE Keynote Speech
http://www.fbi.gov/pressrel/speeches/chabinsky032310.htm

###

 

**About Solutions for Small Business**

*Solutions for Small Business* is an initiative of CTAM, the Cable & Telecommunications Association for Marketing, which is dedicated to helping the cable business grow. Cable companies supporting the initiative include: Armstrong; Atlantic Broadband Business; Bend Broadband Business; Bresnan Business Services; Bright House Networks Business Solutions; Cable One Business; Charter Business; Comcast Business Class; Cox Business; Insight Business; Mediacom Business; Optimum Business; Suddenlink Business and Time Warner Cable Business Class. Small business owners can learn about the initiative at www.solutionsforsmallbusiness.com.

**About BizTechReports.Com**

BizTechReports.Com is an independent reporting agency with offices in Washington, DC and the San Francisco Bay Area that analyzes user trends in business technology. BizTechReports.Com explores the role that technology products and services play in the overall economy and/or in specific vertical industries. For more BizTechReports.Com white papers, case studies and research reports, visit www.biztechreports.com.

 