SURVEY REPORT: CYBER SECURITY

Cybersecurity Report on Small Business: Study Shows Gap between Needs and Actions

Confidence in a connected world.

Executive summary

An online survey revealed that while U.S. small businesses rely heavily on the Internet and routinely handle confidential and proprietary data, many lack the internal resources, formal policies, employee training, and technologies they need to protect their critical information.

Fewer than one third of surveyed businesses have formal policies governing online security—falling behind policy defenses for privacy, company data, and confidential personal information. And although almost all business owners believe that they are protected against online threats and that their employees understand how to defend against them, most offer employees no Internet security training at all—and a substantial minority lack even elementary protection for wireless and remote network access.

It doesn't take much time or money for a small business to reduce security risks substantially. Security awareness is the first essential step, based on clear policies and followed by implementation of automated technologies to protect critical business information against a growing array of internal and external threats.

The survey

In October 2009, Symantec sponsored the National Small Business Cybersecurity Study (**www.staysafeonline.info/files/2009SMBStudy/FullSMBStudy2009%20FINAL.pdf**) for the National Cyber Security Alliance, a public-private partnership that collaborates with the U.S. Department of Homeland Security, industry sponsors, and other nonprofit organizations to raise awareness of cyber security issues among businesses and citizens. The online survey, conducted by polling experts Zogby International, measured 1,500 U.S. small business owners' assessments and opinions of their IT security activities, risks, and preparedness.

Survey findings

Internet use

Businesses participating in the survey are broadly active on the Internet—66% use it daily for internal and external communications, research, and more. More than half have their own web sites—usually self-managed—to support customer product research, service requests, and, in 30% of the cases, online purchases. These companies understand the importance of their online connection: a majority see their businesses as very or somewhat dependent on the Internet for day-to-day operations.

Business information

In addition to conducting business online, survey participants handle a wide variety of confidential information, as seen in Figure 1. Two-thirds retain information about their customers, followed by financial records, credit-card information, and other confidential or proprietary information about customers, employees, and the businesses themselves.

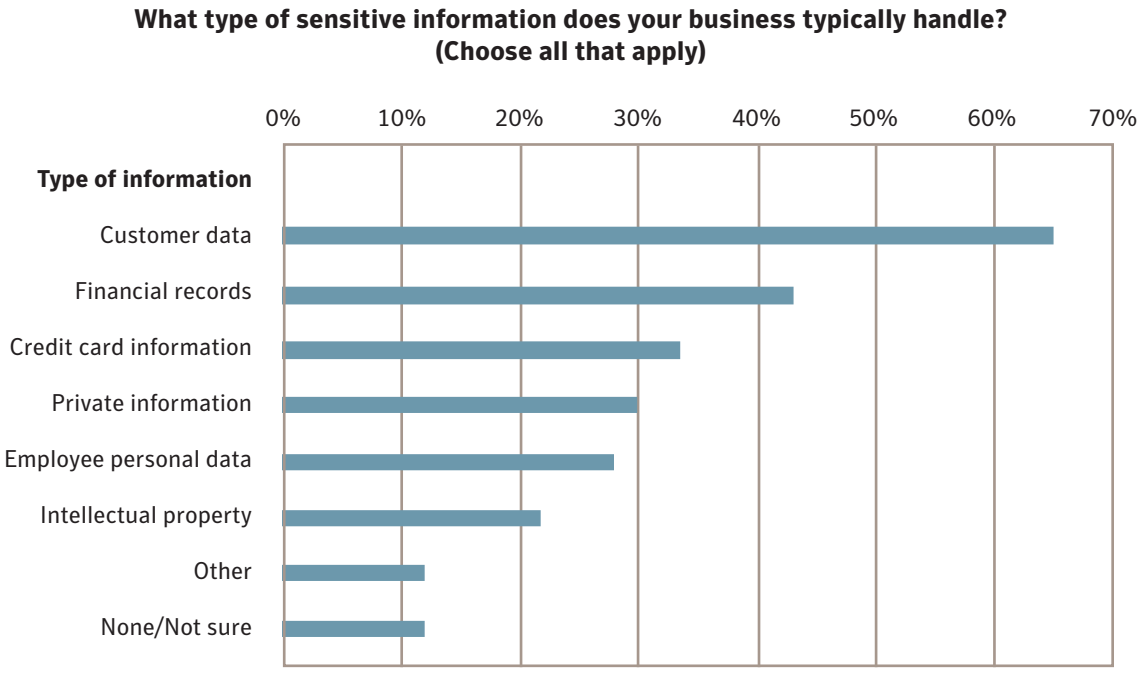

Figure 1. Participating businesses handle one or more categories of confidential information, most often customer data.

IT and security management

Yet for most survey participants, only limited information technology (IT) resources are available to protect these communications, transactions, and records. Staff time is the most important constraint: 86% have no internal manager dedicated to backup and recovery, email and website management, software updates, and other IT administration and maintenance. And for most of the participants, IT is the responsibility of the business owner—competing for time and attention with a long list of other responsibilities for running the actual business.

One consequence of these constraints may be that policies governing Internet security are less common than those protecting confidential customer, company, and employee data, as shown in Figure 2:

Do you have a privacy policy that your employees must comply with when they handle customer information? Which of the following Internet network usage policies does your business have in place? Does your company have a formal Internet security policy?

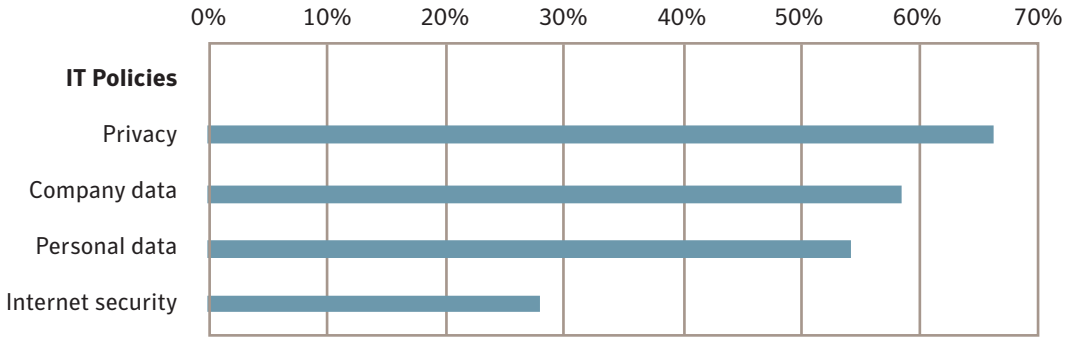

Figure 2. Policies governing Internet security are less common than those protecting proprietary and confidential information.

Shortfalls in security practices are consistent with these policy gaps: only about half of surveyed companies restrict employee access to some parts of their network, or check antivirus, firewall, and operating system status at least weekly.

Wireless and mobile practices

Small businesses are embracing the convenience of remote and wireless computing technologies: 62% have a wireless router at the office, and about a third allow employees to take business data off site in laptops or PDAs, or work from home. But almost a quarter of the surveyed companies lack even elementary password protection on their wireless networks, and allow remote data access without any security protection at all—only half use up-to-date methods such as virtual private networks or encryption to provide such protection.

Security information

Almost all (93%) of the surveyed businesses are satisfied with their security measures, and 92% believe their company is safe from hackers, viruses, malware, and other cyber security breaches. Two-thirds believe that they would know if their networks had been compromised, and roughly the same number would responsibly inform their customers if they had.

Most (60%), however, do not communicate their security measures as part of the value proposition they present to customers. And almost five times as many participants are primarily concerned about external threats like viruses, spyware, and malware than internal threats, including loss of customer information—despite evidence that internal threats are more frequent and more costly. This finding suggests that the information on which these businesses are basing their security plans and policies—primarily from peers and business associates—may be out of date.

More significantly, companies do not communicate security policy information to their employees: 59% provide no employee Internet security training for employees—and yet 97% are very or somewhat confident that their employees understand their Internet security policy and practices.

Five tips for a security-aware business

As online threats multiply and IT budgets shrink, security-aware employees—guided by clear policies and backed by appropriate technologies—are your best defense against exploitation, attack, information theft, and fraud:

1. **Educate employees**—make security awareness a top priority. Train and require employees to use passwords that mix letters and numbers, change them often, and avoid file-sharing programs and downloads from unknown sources.
2. **Support policies with technologies**—protection against today's threats requires multiple layers of defense. Easy-to-maintain commercial suites combine antivirus, intrusion-prevention, and privacy protection for gap-free coverage across servers, desktops, and laptops.
3. **Protect your mobile workforce**—perimeter defenses aren't enough. Employees take devices and data out, contractors bring them in, and walls don't stop wireless networks. Monitor network computers and traffic for malicious activity, block unauthorized applications, and insist on secure practices by remote workers.
4. **Back up valuable data**—your information is your business. Guard against accidents and disasters with regular backups, and keep copies off site. Train employees to back up data themselves, or use automated solutions that run in the background. Test recovery processes at least once a year.
5. **Stay informed and up to date**—security requires vigilance. Monitor reports and newsletters to keep up with new threats and technologies, and be sure that the automatic update features of your operating systems and antivirus, intrusion-prevention, firewall, and other security software are all turned on and working properly.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

About The National Cyber Security Alliance

The National Cyber Security Alliance is a nonprofit organization. Through collaboration with the government, corporate, nonprofit, and academic sectors, the mission of the NCSA is to empower a digital citizenry to use the Internet securely and safely, protecting themselves, the networks they use, and the cyber infrastructure. NCSA works to create a culture of cyber security and safety through education and awareness activities. Visit **www.staysafeonline.org** for more information.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934
www.symantec.com

11/09 20783021