It's Not The Size That Counts

Rebecca Herold, CISSP, CISM, CISA, FLMI

Pre-Edit Version for the CSI June 2006 Alert

It's Not the Size That Counts

Over the course of recent history businesses have had to deal with many regulatory requirements. For example, U.S. OSHA 29 CFR 1910.157 came out in 1972 requiring most businesses to have portable fire extinguishers within their facilities. In 1994 the U.S. FDA 21 CFR 101 established the regulations requiring applicable food packagers to label their products with nutrition information. And there have been many more.

With each new regulation come associated expenses for businesses to meet compliance. Generally the regulations do not differentiate by the size of the business; it is the product, activity, or issue involved that is central to the regulatory requirements.

Because of their size, small and medium sized businesses (SMBs) often feel the brunt of the financial impact of complying with these regulatory requirements more painfully than large organizations, who often already have initiatives, at least partially encompassing the regulatory activities, in place. However, SMBs must still pay attention to the requirements, or face fines, penalties, or civil action

SMBs Are Not Immune from Security Incidents

In a March 29, 2006 Computerworld report, Steve Cole, president and chief executive officer of the Council of Better Business Bureaus (CBBB), provided some interesting statistics:

- 56% of U.S. small businesses experienced data breaches in 2005.
- 20% of small businesses do not use virus-scanning software for email.
- 60% of small businesses do not protect wireless networks with encryption.

The report did not define specifically what was considered as a data breach, so that could be a very wide range of incidents.

So how many businesses are we talking about? The Small Business Association generally defines a small business as one that has 500 - 1000 (depending on the industry) employees. Using 999 or fewer employees as my rule of thumb, according to the U.S. Census Bureau (their range broke at 999 or less employees) there were 5,775,535 small businesses in 2003. If the number is still the same (however, I imagine there are more now), this means that based on the given percentages:

- 3,234,300 small U.S. businesses had data breaches in 2005
- 1,155,107 small U.S. businesses do not use virus-protection software to scan emails
- 3,465,321 small U.S. businesses do not use encryption with their wireless networks (if all had wireless networks)

Stunning numbers, aren't they? However, upon reflection, I'm not too surprised. I've performed a large number of business partner and outsourced vendor security program reviews over the past few years, and it is still common to find

small- to medium-sized organizations, as well as large organizations, with no documented information security policies or procedures, no encryption used anywhere, no wireless security, and, something missing from the report that is very common and critical, no documented business continuity (including backup and disaster recovery) plans.

Widespread Data Protection Practice Complacency Among SMBs
I've heard many different business leaders from SMBs discuss information security management, and there are some common opinions and comments that come up over and over again.

- **Cost issues**: There is not a budget to cover information security comprehensively, particularly using certain technologies, in many SMBs. Because of the smaller budget, many information security and compliance activities, such as providing ongoing education to personnel, using firewalls, installing malicious code scanning software and using encryption, are never seriously considered.
- **Compliance issues**: I have talked to several physicians, and overwhelmingly they have not attempted to address all the requirements of HIPAA. In fact, many of them indicate that providing the Notice of Privacy Protections is the extent of their compliance activities. Many do not know everything that is involved, and another large group of them do no think that, because they are small, the regulators will review them for compliance. It is highly likely this is the attitude of businesses in other industries as well.
- **"Small is safe" issues**: Many of the SMBs mistakenly believe that security incidents of significance only happen with large organizations. They indicate they are too small for anyone to target them, and so they do not have as much to worry about with regard to malicious code or unauthorized access attempts. This reasoning works for target shooting, but not for computers, networks or other information resources. The Internet allows a small one-trick-pony business to advertise and compete right next to the gargantuan multi-billion dollar companies with the same visibility, making them very vulnerable.

Common Information Security Problems Within SMBs
SMBs have many things in common when it comes to information security and compliance vulnerabilities and gaps. A few of the typical issues include the following.

- No accountability. In many small businesses all the staff share the same computer, or the same user ID. There is not a way to determine who has performed any of the specific activities with regard to information accesses.
- Lack of awareness of information security and privacy issues. For example, some think storing offsite backups in an employee's basement is a good idea.
- Lack of awareness of regulatory and legal requirements. Some are completely unaware of their regulatory requirements for data protection because they do not have the resources to keep up with these issues.

- No separation of duties. Most SMBs do not have the size of staff necessary for different people to perform multiple job responsibilities, some of which could lead to fraud and/or information compromise.
- Technology constraints. In many SMBs the IT systems are also the personal computers of the staff.
- No information security knowledge. In SMBs that have a small or nonexistent IT staff, they typically do not have information security specific staff or expertise.
- Outsourced processing. Many SMBs use turnkey IT solutions they have outsourced to a service provider that is also running systems for many other companies. Most do not check out the security practices of these outsourced entities before entrusting them with their business information.
- Lack of technologies. Most SMBs do not have many of the technologies necessary, such as firewalls, intrusion detection systems and malicious code prevention, to ensure information security and applicable regulatory compliance.

More Reasons for SMBs to Be Diligent with Information Security and Privacy than Ever Before

The days of the stand-alone Apple II sitting on the SMB's desk to manage the business's electronic documents are long past. The continuously evolving technologies and the ever present and growing threats, risks and vulnerabilities require SMBs to be more diligent about their data protection practices.

- More SMBs are doing online business than ever before
- More SMBs are handling huge amounts of personal information than ever before
- More SMBs are performing outsourced data processing activities for large organizations than ever before
- More SMBs are outsourcing their data processing to others than ever before
- More data protection laws and regulations exist that require appropriate data protections than ever before
- More SMBs are processing and storing all their business information on mobile computing devices and storage media than ever before
- More information risks, vulnerabilities and threats exist than ever before

More Tools Available Now Than Ever Before

There are also more tools and improvements that have been made in the past few years that give SMBs much more effective, lower cost and easier to use tools to protect their organizations' information resources. Government agencies, many nonprofits, industry groups, and even some of the large organizations make many products and services freely available to SMBs to help them with their information security efforts. A few of these include the following:

- The USPS offers seven DVDs free for the asking about information security and fraud. They are primarily targeted to consumers, but they have information useful to SMBs, and would also make a great addition to any

organization's awareness program. http://shop.usps.com/webapp/wcs/stores/servlet/ProductCategoryDisplay.

- The U.S. Treasury Department offers a free DVD called "Identity Theft; Outsmarting the Crooks" that is available to a wide audience. http://www.ustreas.gov/offices/domestic-finance/financial-institution/cip/identity-theft.shtml.
- The FTC, Department of Commerce, Department of Homeland Security, USPS and the SEC created a web site providing a large amount of information security information that can help SMBs understand cyber threats. http://onguardonline.gov/index.html
- The National Cyber Security Alliance helps SMBs learn about information security, data recovery and cyber crime reporting. http://www.staysafeonline.org/basics/small_business.html
- The Multi State ISAC provides awareness and training information. http://www.cscic.state.ny.us/msisac/ncsa/oct05/index.htm
- The US-CERT in partnership with the Department of Homeland Security provide free resources that allow businesses of all sizes receive alerts and best practices free of charge. http://www.us-cert.gov/
- The National Cyber Security Partnership provides awareness to SMBs. http://www.cyberpartnership.org/init-aware.html
- The Industry Security Alliance created an SMB "Common Sense Guide" to Cyber Security, available from the U.S. Chamber of Commerce at http://www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm.
- The U.S. Department of Homeland Security has information available on their Ready Business site that SMBs will find useful. http://www.ready.gov/business/st3-improvecyber.html
- The Council of Better Business Bureaus (CBBB) makes their customer data security toolkit available for free at http://BBB.org/securityandprivacy.
- The Office of the Privacy Commissioner of Canada makes many types of information available to help organizations secure the personal information they handle. While they are focused primarily at PIPEDA compliance, most of the activities are good to apply in any business. http://www.privcom.gc.ca/ekit/ekit_e.asp
- And there are many, many more…

Yes, for some of the free items found in the above locations you have to pay postage and provide your name and address so they can deliver it; but hey…come on! Pry enough coins from those pinched fingers for the postage; these films are generally well done and make a good addition to an awareness and training program that is typically lacking in SMBs. And any way, the materials are free, you're paying for the delivery of them to your location. Of course, if that is a concern to you, you could probably drop by your local government office to get them.

Remember, even if you are an SMB, you are still obligated to follow the regulatory requirements, and you need to protect the personal information with which you've been entrusted. So, do something about it!

Rebecca Herold, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor, and can be reached at rebeccaherold@rebeccaherold.com or http://www.rebeccaherold.com.

