BY SAJAY RAI + PHILIP CHUKWUMA EDITED BY STEVE MAR

MUST-HAVE CONTROLS FOR SMBS

Five controls can help small and mid-sized businesses protect themselves against cyber breaches.

Although most cyber breaches reported in the news have struck large companies such as Target and Yahoo, small and mid-sized businesses (SMBs) suffer a far greater number of cyber incidents. These breaches often involve organizations such as local health-care providers or regional insurance brokers. Although the number of breached records an SMB may have is in the hundreds or thousands, rather than the millions, the cost of these breaches can be higher for SMBs because they may not be able to address the incidents on their own.

Many SMBs have limited or no resources committed to cybersecurity, and some don't have an internal audit department to provide assurance. For these organizations, the questions are "Where should we focus when it comes to cybersecurity?" and "What are the minimum controls we must have to protect the sensitive information?" Internal auditors at SMBs can help answer these questions by checking that their organization has five essential cybersecurity controls.

1. Scan the Network

Regardless of the organization's industry, SMBs must ensure their network perimeter is protected. The first step is identifying the vulnerabilities by performing an external network scan at least quarterly. SMBs can either hire an outside company to perform these scans, or they can license software to run the scans, themselves.

Moreover, SMBs need a process in place to remedy the critical, high, and medium vulnerabilities within three months of the scan run date, while low vulnerabilities are less of a priority. The fewer vulnerabilities the perimeter network has, the less chance that an external hacker will breach the organization's network.

2. Train Employees

Educating employees about their cybersecurity responsibilities is not a simple checkbox matter. SMBs not only need to implement an effective information security policy, they also need to ensure employees are aware of the policy and their responsibilities. The policy and training should cover:

- Awareness of phishing attacks.
- Training on ransomware management.
- Travel tips.
- Potential threats of social engineering.
- Password protection.
- Risks of storing sensitive data in the cloud.
- Accessing corporate information from home computers.
- Awareness of tools the organization provides for securely sending emails or sharing large files.
- Protection of mobile devices.
- Awareness of CEO spoofing attacks.

SEND ITAUDIT ARTICLE IDEAS to Steve Mar at steve_mar2003@msn.com

TO COMMENT on this article,
EMAIL the author at sajay.rai@theiia.org

In addition, SMBs should verify employees' level of awareness by conducting simulation exercises. These can be in the form of a phishing exercise in which SMBs send fake emails to employees to see if they will click on a web link, or a social engineering exercise in which a hired individual tries to enter the organization's physical location and steal sensitive information such as passwords written near the computer screen.

3. Protect Sensitive Information

Management and internal audit should identify and protect the organization's sensitive data. Even in small organizations, sensitive information tends to proliferate across various platforms and folders. For example, employees' personal information typically resides in human resources software or with a cloud service provider, but through various downloads and reports, the information can proliferate to shared drives and folders, laptops, emails, and even cloud folders like Dropbox.

Internal auditors at SMBs should check that the organization has performed these tasks to make sure it has a good handle on the organization's sensitive information:

- Inventory all sensitive business processes and the related IT systems. Depending on the organization's industry, this information could include customer information, pricing data, customers' credit card information, patients' health information, engineering data, or financial data.

> Auditors should check whether the organization has built a layered defense.

- For each business process, identify an information owner who has complete authority to approve user access to that information.
- Ensure that the information owner periodically reviews access to all the information he or she owns and updates the access list.

4. Segment the Network

Organizations should make it hard to get to their sensitive data by building layers or network segments. Although the network perimeter is an organization's first line of defense, the probability of the network being penetrated is at an all-time high. Internal auditors should check whether the organization has built a layered defense to protect its sensitive information.

Once the organization has identified its sensitive information, management should work with the IT department to segment those servers that run its sensitive applications. This segmentation will result in an additional layer of protection for these servers, typically by adding another firewall for the segment. Faced with having to penetrate another layer of defense, an intruder may decide to go elsewhere in the network where less sensitive information is stored.

5. Deploy Extra Protection for Endpoints

An organization's electronic business front door also can be the entrance for criminals or bad actors. Most of today's malware enters through the network but proliferates through the endpoints such as laptops and desktops. At a minimum, internal auditors at SMBs must ensure that all the endpoints are running anti-malware/anti-virus software. Also, they should check that this software's firewall features are enabled. Moreover, all laptop hard drives should be encrypted.

A Stronger Defense

In addition to making sure their organization has implemented these five core controls, internal auditors should advise SMB executives to consider other protective controls:

- *Monitor the network.* Network monitoring products and services can provide real-time alerts in case there is an intrusion.
- *Manage service providers.* Organizations should inventory all key service providers and review all contracts for appropriate security, privacy, and data breach notification language.
- *Protect smart devices.* Increasingly, company information is stored on mobile devices. Several solutions can manage and protect the information on these devices. SMBs should make sure they are able to wipe the sensitive information from these devices if they are lost or stolen.
- *Monitor activity related to sensitive information.* SMBs should log activities against their sensitive information and keep an audit log in case an incident occurs and they need to review the logs to evaluate the incident.

Combined with the five essential controls, these controls can help SMBs reduce the probability of a data breach. But a security program is only as strong as its weakest link. Through their assurance and advisory work, internal auditors can help identify these weaknesses and suggest ways to strengthen their organization's defenses.

Sajay Rai, CPA, CISSP, CISM, *is president and CEO of Securely Yours LLC in Bloomfield Hills, Mich.*
Philip Chukwuma, CISSP, *is chief technology officer of Securely Yours.*