

Cybersecurity in Small Businesses and Nonprofit Organizations

By Dr. Kamala Raghavan, CPA, CFF, CGMA, CFP

Most small businesses are becoming painfully aware that their small size does not provide them immunity from the risk of a cyberattack. Today's sophisticated hackers can and will attack any target. A survey by the National Cyber Security Alliance (NCSA) found that 71 percent of security breaches target small businesses, and about 50 percent of small businesses have suffered from cyberattacks. The credit data provider Experian reported that 60 percent of small businesses go out of business six months after suffering a security breach. The Department of Commerce's National Institute of Standards and Technology study also found a sharp increase in hackers and adversaries targeting small businesses in the past two years.

Small businesses and nonprofit organizations are attractive to hackers, because they tend to have lax online security. While they understand the need for cybersecurity, many have not taken sufficient measures to protect against cyberattacks. Typically, they do not take the time to develop a contingency plan or response plan to cyberattacks, and do not have the resources to recover from an incident when it happens. A cybersecurity incident could shut down an entire network for many days until the problem is researched and fixed. A small business may not be able to withstand the loss of income, or have insurance that helps to defray those costs or any liabilities that might occur as a result of the breach. A highly public breach could also damage the business's brand and lead to long-term loss of income.

NCSA's research identified three major reasons hackers target small businesses:

- they are not well equipped to handle an attack due to lack of resources;
- their partnerships with larger businesses provide back-door access to a hacker's true targets;
- they do not effectively guard the information that hackers desire such as credit card credentials, intellectual property, personal information, etc.

Small businesses and nonprofit organizations are increasingly doing business online using cloud services for expense savings, but they do not always ensure that the services use strong encryption technology. This combination provides the hacker the opportunity to easily access sensitive data. Cloud computing enables today's small businesses and their employees to work from anywhere using multiple devices. They are able to transfer files using Dropbox, videoconference globally with Skype and other sites, and remotely access work from their smartphones and tablets. But some of them have learned painfully that the price for these collaborative benefits is the potential for a serious data security

breach. If the small business or nonprofit organization has *Fortune 500* companies as customers, they provide an easy entry point to a much larger treasure trove of data.

Examples of such breaches are the incidents at Target and Home Depot where the hackers used the access of a relatively small vendor in the supply chain as the entry point to a major credit card data theft. As businesses turn to digital technologies for business solutions, the risk of a security breach continues to rise. For the last 11 years, the security of information technology (IT) and data has been rated as a top technology initiative in surveys conducted and published by the American Institute of CPAs (AICPA). In addition to concerns about the loss of data and sensitive information, the AICPA surveys identify controls for mobile devices and cloud computing as ongoing concerns.

Recommendations

Businesses of all sizes need to assume a state of compromise today so that they can avoid considerable costs from loss of data or stolen intellectual property, interruption to business operations and damage to the business's reputation. Studies have shown that a breach can increase customer churn by nearly 4 percent. All businesses need to assess their cybersecurity weaknesses so that they can develop a strategy to safeguard sensitive data. A basic question to ask: what is the most sensitive data for the business? A pharmaceutical company might have the formula for a new drug in a document that is securely stored on its hard drive, but the data has also been shared by the researchers via email without encryption. Similarly, government and nonprofit agencies have large troves of sensitive taxpayer data in their files that are loaded onto employees' laptops or flash drives for work reasons without encryption.

It is important to ask specific questions about how data is handled and transported, what media are used for data storage, where did the data originate, and who has been granted access to the networks. The data most valuable to a hacker may not reside in a business's own database, but it can provide access to their customers. Effective management of the risks requires businesses to understand these vulnerabilities.

Most small businesses do not invest in cybersecurity, due to their erroneous perception of such investment as a discretionary spending item and not as an essential defensive strategy for sustainability. Studies have shown that 89 percent of consumers avoid businesses that do not protect their online privacy, as evidenced by the sales decline at companies like Target and Home Depot. Business partners also require proof that their interests and privacy are protected. Adequate security has become a requirement for companies to collaborate or outsource work. Sixty percent of U.S. businesses have baseline standards that they expect their external partners, suppliers and vendors to meet.

While small businesses and nonprofit organizations may not have the resources and time to research the most appropriate cybersecurity tools,

a “one-size-fits-all” approach to cybersecurity by installing the bestselling package is not the answer. They need to focus more on the consequences of a wide range of potential risk events and adopt new risk management strategies, and focus less on the probability of the events. The new threats from trends of globalization, rapid technological changes and re-alignment of economies are increasing volatility in the markets, and disrupting ideas about “black swan events;” i.e., low probability, high-impact events. Small businesses that view security breach events as “black swans” and do not change their risk management practices may face big risks to their desired future state and growth strategy. They will need to view risk management as a dynamic business enabler to move the organization forward, rather than a static structure.

To understand any cyberbreach event, the motivation of the attackers needs to be understood. In today’s interconnected global marketplace, individuals have to entrust businesses with sensitive personal details on email, Facebook, text messages, etc., as well as financial details. Increasingly, businesses and individuals use cloud services for storage and transaction processing, which has helped commerce to grow exponentially, but has also provided increased gateways to launch cyberattacks. The majority of these attacks are low skill and low focus, with hackers sending spam mails out to millions of email addresses hoping that someone will click on the link. The low-skill, low-focus hackers who penetrate the networks of businesses do not care much about the individual entity, and they will move on to the next weaker prey if the business’ security protocols are strong. By having strong protection of systems, businesses can defend themselves against most of the low-skill, low-focus attacks.

However, the high-skill, low-focus attacks such as the ones suffered by Target, Home Depot, Michaels, Neiman Marcus, JP Morgan Chase and other commercial networks are more serious. These were sophisticated attacks using newly discovered “zero-day” vulnerabilities in software, systems and networks. In these attacks, the opportunist attacker got access to a large database of credit card numbers by exploiting the cybersecurity weaknesses. All networks are vulnerable to attacks by a sufficiently skilled, funded and motivated attacker, but good security can make the attacks harder, costlier and riskier. Security is a combination of prevention (protection), detection and correction (response). Prevention can defend against low-focus attacks and make targeted attacks harder, and detection can spot the attackers. Having a planned response strategy will minimize the damage and manage the fallout.

Creating a culture of cybersecurity, having current security software and creating an emergency response plan for a data breach are good first steps toward long-term protection of a business’s interests. Powerful new tools used by small businesses to reach new markets and increasing productivity and efficiency, such as broadband and cloud storage, also create a critical need for them to develop a cybersecurity framework to protect their business, customers and data from growing cybersecurity threats. Some specific steps to take are include the following.

Set the tone at the top and ensure that it is communicated across the organization. Assign a top executive to lead the charge, rally company employees, regularly update other managers, oversee IT activities, and ensure that all cybersecurity threats are reviewed and protective measures are implemented.

Define cybersecurity goals and outcomes. The security team should keep the cybersecurity goals and expected outcomes updated, and show

metrics on the tangible impact on risk reduction in the key areas. Such metrics are important for demonstrating how information security aligns with the business goals.

Raise employee awareness. Employees must understand the importance of cybersecurity in protecting their customers, colleagues, intellectual property and valuable business relationships, and stay vigilant about the risks. The main reason for security breaches is lax security awareness among employees and basic problems, such as negligence in following procedures; e.g., leaving their passwords visible or not turning off their computers before going home. Raising security awareness can be done by simple measures like using office bulletin boards and weekly emails to remind employees of basic security precautions.

Establish security policies to protect sensitive business data and practices rules for handling and protecting sensitive customer information and other vital data. Communicate them to employees on a regular basis along with the penalties for violating the business policies. Ensure that human resources and audit personnel implement legally acceptable procedures to monitor for any abnormal patterns in the Internet usage and email habits of key employees who are leaving the firm involuntarily.

Plan disaster recovery procedures. Establish cross-functional security teams, including leaders from the IT, human resources, finance, risk and legal departments who meet regularly to discuss and coordinate information security issues. The team should develop a crisis response plan detailing immediate action in the event of a security breach and run simulation exercises. The plan should outline actions to identify and mitigate the damage, such as using a call tree for contacting law enforcement, stakeholders and the media. Scenario planning exercises for crises must be tested periodically for effectiveness. Since technology touches all areas of a business, recovery from cybersecurity incidents should be treated as both a technology and a business issue.

Make regular backup copies of important business data, including word processing documents, spreadsheets, databases, financial reports, human resources files and accounts receivable/payable files residing on all equipment used in the business.

Implement barriers like a cloud-based security application and teach employees to think critically about the potential impact of their online actions.

Install and maintain strong firewalls between the business’s internal network and the Internet to prevent outsiders from accessing data on the business’s private network. Ensure that all remote access from employees’ home computers and laptops are protected by firewalls.

Establish policies and practices on Internet security in the workplace around issues like use of USB devices, social media and personal devices in the workplace.

Install software updates for all operating systems and applications automatically. Most vendors regularly provide patches and updates to their products to correct security problems and improve functionality.

Secure the Wi-Fi networks and use encryption so that passwords are required for access. Change the administrative passwords on all devices after purchase. Mask the Wi-Fi network by setting up the wireless access point or router to hide the network name (SSID).

continued on next page



INTERNAL CONTROLS CAN STRENGTHEN COMPANIES' RESILIENCE AGAINST GAME-CHANGING RISKS.



Perform due diligence on third-party security providers. Establish the standards up front, spell out the desired security level, ensure that it is included in the provider's performance contract, and test them periodically.

Control physical access to computers and network components. Prevent access or use of business computers by unauthorized individuals. Laptops and flash drives need to be "locked" when unattended.

Set up a separate account for each individual and require that strong passwords be used for each account. Administrative privileges should only be given to trusted IT staff and key personnel.

Establish rules about password practices, including regular change of passwords and acceptable websites to access from a business network. The FCC's Cybersecurity Hub at www.fcc.gov/cyberforsmallbiz has more information.

Limit employee access to data and information while considering best practices in internal control, such as segregation of duties. Employees should only be given access to the specific data systems that they need for their jobs. Limit authority to install software to specific employees with proper authorizations.

Install, use and regularly update antivirus and antispyware software on all computers used in the business to protect information, computers and networks from viruses, spyware and other malicious code. Set the antivirus software to automatically check and install updates at a scheduled time of low computer usage and do a scan. Use the latest versions of anti-spam software that can screen for vulnerable or malicious URLs and install patches as soon as they are available.

Be alert to new, affordable technologies and cybersecurity innovations that can deter attackers by quicker detection of intruders. Many vendors are developing tools to identify and circumvent zero-day threats (unknown and unpatched code flaws) before the hackers can exploit them. Such prevention and detection tools can make cybercrime less lucrative for criminals by forcing them to spend more in technology and attack capabilities.

Risk Management

Internal controls can strengthen companies' resilience against game-changing risks. However, many businesses do not have formal

processes in place to assess and prepare for circumstances that can increase their reputational, competitive, legal or operational risks. Many cyberbreaches result from weak spots in the technology and lead to faulty decision-making processes that ignore potential business consequences of technology issues. The long-term viability of any business depends on timely, uninterrupted access to vital information and IT resources, and adopting a consequences-based approach to risk management brings more focus on resilience and less on expectations.

By conducting scenario tests, managers can test the business's reaction to crises. The scenario plans should review the entire value chain, including key vendors. More businesses are beginning to establish systems that monitor and alert when the probability of a particular scenario increases, setting up cross-functional crisis management teams and identify processes to quickly react to risks when they occur. Effective internal controls can help a business maintain and test the IT contingency and disaster recovery plans. Successful risk strategies must embed risk awareness throughout the business's culture.

SEC Disclosure Guidance and Internal Control

In the fall of 2011, the Securities and Exchange Commission's (SEC) Division of Corporation Finance issued enhanced financial statement disclosure guidance for public companies, which can serve as a blueprint for small businesses and nonprofit organizations. The guidance has led to a higher level of cybersecurity awareness, monitoring and scrutiny by SEC registrants (CF Disclosure Guidance: Topic 2, Oct. 13, 2011). It was issued in response to the increase in number and severity of cybersecurity incidents experienced by SEC registrants, and the new disclosure obligations focus on both potential cybersecurity risks and actual incidents. It recognized that cyberattacks can be caused by deliberate actions by outside hackers or unintended events by internal agents like employees, contractors and vendors. It provided examples of specific attacks, including unauthorized access to sensitive data, industrial espionage, sabotage of hardware and software, infection of hardware and software with malicious software, theft of computer time and other denial of service attacks, and theft of mobile devices.

The guidance is consistent with other disclosure requirements mandated by federal securities laws and suggests that disclosures should identify specific material cybersecurity risk factors, such as risks and costs associated with a registrant's operations, outsourcing activities, undetected risks for an extended period, risks that lead to increased insurance protection, as well as past years' material cybersecurity incidents. Additional information on actual cyberattack incidents must be disclosed with details on the nature, occurrence, potential cost and related consequences so that stakeholders can understand the risks faced by the registrant and its remediation efforts. The guidance acknowledged that registrants have provided additional resources by hiring and training internal security personnel, upgrading IT systems and hiring IT security consultants.

Recognizing the reluctance of businesses to disclose the details of security breaches that can harm their reputation, lead to litigation and expose vulnerabilities to competitors, and the difficulty in estimating costs of potential breaches, the SEC offered guidance on costs that should be considered, such as remedial costs, cybersecurity costs, regulatory fines, litigation costs, loss of customers and loss of investor confidence.

Auditors' Roles

Internal control audits are governed by Auditing Standard (AS) 5, *An Audit of Internal Control over Financial Reporting that is integrated with an Audit of Financial Statements*, which requires auditors to use a “top-down approach” beginning at the financial statement level to identify controls that present a “reasonable possibility” of material financial statement misstatement. The SEC guidance can be viewed as an expansion of the scope of the integrated audit of internal control over financial reporting and the financial statements that include IT controls.

The SEC disclosure guidance requires management to identify the costs and consequences of past and potential material cybersecurity incidents and risks in the management’s discussion and analysis (MD&A) section of financial reports, including costs of litigation, prevention of cyberattacks, maintaining business relationships, loss of business and future cash flows, and impairment of goodwill and long-lived assets. Disclosures about the impact of cybersecurity risks on the business’s information systems and integrity of financial reporting should be an essential part of management’s assessment of internal controls and potential internal control deficiencies.

Internal and external auditors need to evaluate the adequacy of existing cybersecurity controls using complex, specialized models and sophisticated IT skills. Internal auditors need technical expertise to be able to analyze the data security risks, participate in selection of security systems, conduct security and disaster recovery audits to evaluate gaps, and monitor compliance with security procedures. External auditors need the skills necessary to understand and identify the client’s computer security environment and critical controls, conduct security review, identify strengths and weaknesses in a client’s security system, determine if financial statements are fairly and accurately presented, and report the audit findings, including recommendations for mitigating material weaknesses in the client’s security environment to management.

Auditors cannot assume that cyberattacks are limited to large or high-tech companies, because businesses of all sizes and in all sectors are at risk of having customer credit card numbers and other personal information stolen. The auditors should consider the SEC’s disclosure guidelines for registrants as a guide for small businesses and nonprofit organizations as well, and seek assistance from an external specialist, if needed. Information system auditors and security experts can be valuable sources of information on security risks and remedial modifications to internal control systems to bolster them and help businesses to provide expanded cybersecurity disclosures.

Beyond Protection

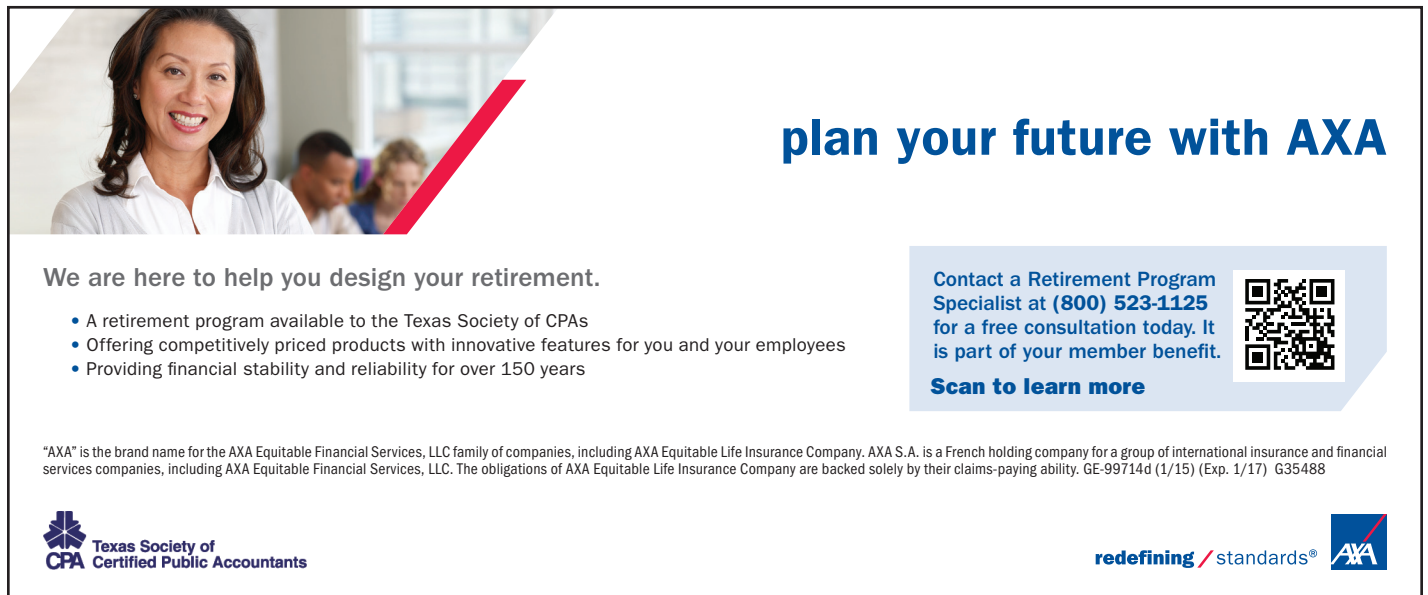
Many small businesses are realizing that in the increasingly sophisticated and interconnected global marketplace, investing in information security goes beyond protecting the business. Strong cybersecurity can position organizations for competitive advantage with their business partners and customers, as well as to allow them to take advantage of newer, affordable technologies to help their growth. Such technologies are offering stronger protections to detect intruders sooner and help businesses to implement preventive and corrective measures.

Internal and external auditors have significant roles to help and guide the small businesses and nonprofit organizations in their cybersecurity risk management. The progressive ones understand that volatility is inevitable and are rethinking their approach so that shocks to the system will not disrupt their strategy and future growth.

A culture of risk awareness throughout the business is a necessary platform for effective risk management. By adopting some of the recommended steps, small businesses and nonprofit organizations can be resilient and able to take calculated risks to pursue growth in the global marketplace. ■

Dr. Kamala Raghavan,
CPA, CFF, CGMA, CFP

is a graduate faculty member at Texas Southern University in Houston, Texas.



plan your future with AXA

We are here to help you design your retirement.

- A retirement program available to the Texas Society of CPAs
- Offering competitively priced products with innovative features for you and your employees
- Providing financial stability and reliability for over 150 years

Contact a Retirement Program Specialist at (800) 523-1125 for a free consultation today. It is part of your member benefit.

Scan to learn more

AXA is the brand name for the AXA Equitable Financial Services, LLC family of companies, including AXA Equitable Life Insurance Company. AXA S.A. is a French holding company for a group of international insurance and financial services companies, including AXA Equitable Financial Services, LLC. The obligations of AXA Equitable Life Insurance Company are backed solely by their claims-paying ability. GE-99714d (1/15) (Exp. 1/17) G35488

Texas Society of CPA Certified Public Accountants

redefining / standards® AXA