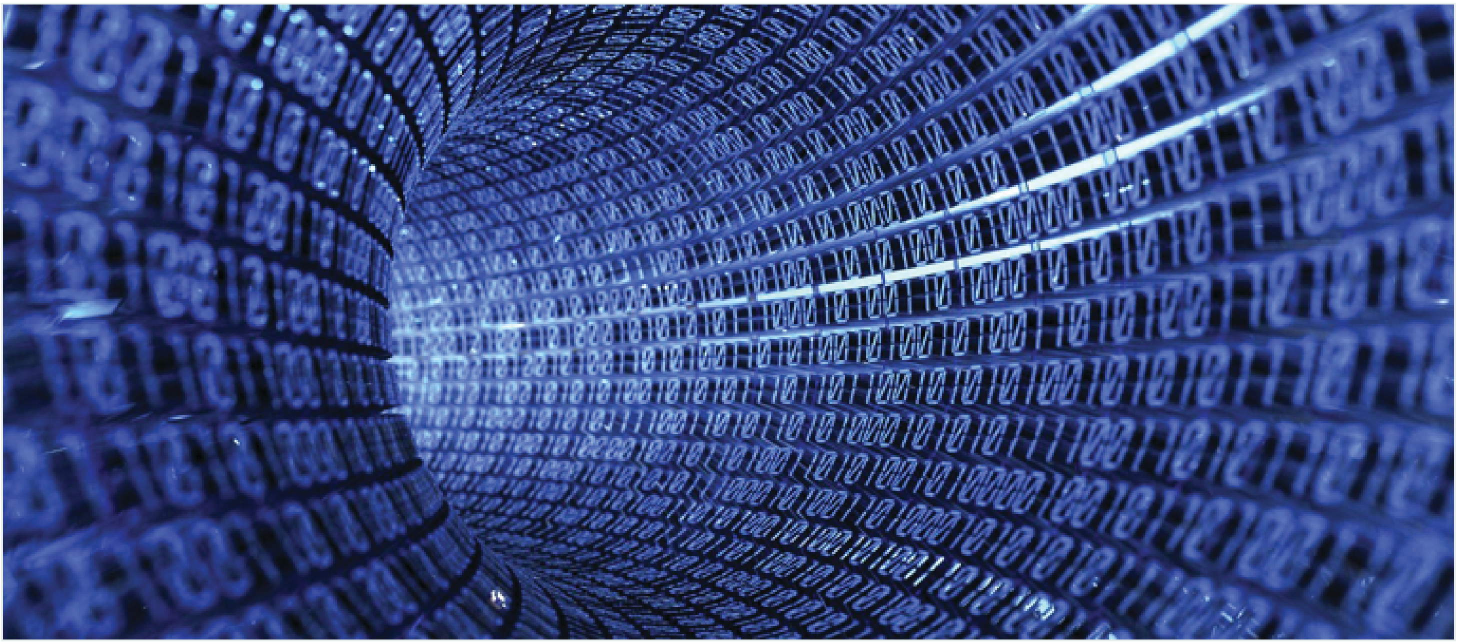
CPA
Practice Advisor

Security

Oct. 01, 2018



As cybercrime becomes increasingly sophisticated, security breaches at major corporations around the world are becoming quite commonplace. Just last year, the private information of 143 million Equifax consumers was compromised.[1] And if a major corporation cannot protect its information, how does a small or mid-sized corporation stand a chance?

Most modern organizations, whether large or small, heavily rely on information systems to conduct business, so any weakness in information security puts the entire organization at risk. Organizations suffering a security breach not only encounter internal disruption, but may also be subject to government penalties, industry fines, consumer lawsuits, and worst of all, reputation damage. For small to mid-sized organizations, these consequences can be particularly damaging.

While there is no silver bullet to protect your organization against all cyberthreats,

have, where it is stored, and precisely how it is protected. Examples of proprietary, confidential, or otherwise protected information include any personally identifiable information (PII) or personal health information (PHI), as well as intellectual property and any unique data that could impair the firm's competitive advantage if disclosed.

2. **Identify zero-day threats and update security patches.**

An epitome of the constantly changing nature of cybersecurity threats is the phenomenon of the zero-day threat. Any previously unknown threat would fall under this classification. An example of this is ransomware attacks. Often in such an attack, an unsuspecting user clicks on a link, typically in a spam email, that launches malicious software (malware) that encrypts the user's files, rendering them inaccessible. The malware creator then offers to decrypt the user's files for a fee. Many large firms have been victimized by this type of attack. Practitioners should validate that the organization has a practice in place to identify zero-day threats and that it has a policy in place to update its anti-virus and anti-malware libraries on a constant basis.

3. **Utilize anti-virus and anti-malware software.**

In 2015, research by Internet security teams at Symantec and Verizon revealed that one million new malware threats were released every day the previous year.[2] Given the need for up-to-date anti-virus and anti-malware software, organizations should verify not only that software is constantly updated, but also that it is properly updated and deployed on all the organization's devices. For various reasons, a firm's devices may not have the current version of the software installed or that software may not have been properly updated. Internal auditing should check a sample of individual devices in a variety of locations to ensure that all devices have the anti-virus software properly installed and constantly updated.

4. Encrypt your data.

Agreement (SLA).

The cloud refers to a massive combination of data-centers, servers, routers, connections, and switches located all over the world, to house and operate software applications of all types. Currently, innumerable cloud-based data centers and software applications are in use by many organizations. Many software applications are offered exclusively as software as a service (SaaS), which allows for massive economies of scale, much like an electric grid.

The management of cloud computing operations is normally automated, and the current scale of cloud computing is unfathomable. This poses a unique set of risks for the organization using cloud computing and the internal auditor’s ability to ensure information security. To begin with, there is the physical security risk. Given that most firms do not even know where their company’s data is stored, it is difficult to ensure that the data centers are physically inaccessible to someone who might simply steal the physical data servers.

Fortunately, a framework has been developed for the procurement of SaaS that ensures physical, virtual, and data security. These security specifications are outlined in a service level agreement (SLA). An SLA signed by the organization should provide for location security, transmission security, encryption, and all other information security concerns related to cloud computing. Practitioners should review SLAs for all the organization’s cloud computing solutions. All key information security concerns should be addressed in the SLA.

6. Implement controls for data loss.

If a hacker gains access to your organization’s system, they will then attempt to exfiltrate (i.e., remove) data assets. The intrusion detection system (IDS), intrusion prevention system (IPS), firewall, and other tools used by the firm should be configured to monitor all outbound Internet traffic. Data loss controls include other

computing), or internal processes used to produce, store, or process a firm's financial information should be subject to documented change-control procedures. Correct change-control procedures involve the following:

- Specification/request (typically called a change request);
- Approval by proper levels of management;
- Planning;
- Testing, including user acceptance testing;
- Scheduling;
- Communication;
- Training;
- Implementation;
- Documentation; and
- Implementation verification of effectiveness.

8. **Explore and document previous hacking events.**

A popular axiom holds that there are only two types of organizations in the U.S., those that have been hacked and those that don't know they've been hacked. One of the best indicators of information security weakness is that the firm has had information security, or hacking, events in the past. The fact that there are many thousands, perhaps even millions, of bad actors attempting on a constant basis to hack into companies and steal information and money should provide a sense of urgency to all companies' information security activities. As such, the circumstances regarding the nature of previous hacking events must be explored and documented.

9. **Conduct security training (at least annually).**

Information security is obviously very detailed and complex. It requires that all

10. Engage a third party for white-hat external and internal vulnerability scanning tests.

The sheer magnitude and complexity involved in information security virtually ensures that some potential vulnerability will go undetected by the firm. It is therefore a solid practice for the firm, at least annually, to engage a third-party "white-hat" (i.e., good guy) hacking firm to conduct a vulnerability scan. Ideally, the white-hat hacker will use all the techniques that might be employed by a "black-hat" (i.e., bad guy) hacker to identify potential information security weaknesses. This is the best way to find any weaknesses, remediate those potential weaknesses, and harden the firm's information processing environment.

Remember: No matter the size of your organization, a failure in any area of the IT structure, no matter how small, can compromise the entire system and enable a hacker to access the application software and source data. Proper security must include user education and the application of preventive, detective, and reactive controls.

For more information on how to strengthen your organization's information security, including a risk assessment, download our white paper, *How Small and Mid-Sized Entities Can Protect Themselves from a Cybersecurity Breach*.

============

The Financial Management and Controllership Editorial Team at Thomson Reuters:

Lon E. Dobbs, J.D., is a Senior Editor with over two decades of experience in

Susan B. Weisenfeld, J.D., is a Managing Editor, with responsibility for products covering financial management and controllership, corporate governance, internal auditing, and GAAP.

========

[1] Taylor Armeding, “The 17 biggest data breaches of the 21st century,” CSOnline.com, January 26, 2018, accessed May 2, 2018, https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

[2] Virginia Harrison and Jose Pagliery, “Nearly 1 million new malware threats released every day,” Money.ccn.com, April 14, 2015, accessed May 2, 2018, http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html.

Hardware • Small Business

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.