THOMSON REUTERS
CHECKPOINT™

How Small and Mid-Sized Entities Can Protect Themselves from a Cybersecurity Breach

The Financial Management and Controllership Editorial Team at Thomson Reuters

WHITE PAPER

the answer company™
THOMSON REUTERS®

A cybersecurity breach at a major corporation has taken place. How many times have we read about this in recent years? Just last year, we learned that the private information of around 143 million consumers was compromised when Equifax was hacked.[1] And if a major corporation cannot protect its information, how can a smaller or mid-sized corporation hope to protect its assets from a breach? The first step is to implement strong information technology controls. Author A. Wayne Avellanet[2] provides a roadmap for this situation in Chapter 1109, Information Technology Controls, in the Thomson Reuters landmark product, **Financial Management and Controllership**.

The key concern for an organization is that 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.

The Greatest Challenge

There was a time when the threat of an IT security breach was not a constant concern for business entities. That time ended years ago. IT security concerns permeate internal control at even the smallest corporations.

Indeed, the most challenging topic in internal control today, and for the foreseeable future, is information security. Modern organizations rely on their information systems to conduct nearly all their business; any weakness in information security places the entire organization in peril. Organizations suffering a security breach not only encounter internal disruption, but may also be subject to government penalties, industry fines, consumer lawsuits, and, most of all, reputation damage. It is imperative that all employees involved with internal control understand the key terms and control points related to information security.

The Key Concern

Mr. Avellanet explains that the key concern for an organization is that 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. In fact, many systems and organizations still get infected by users clicking on an attachment to an email, or by users sharing passwords. A recent study by Willis Towers Watson found that nearly 90% of all cybersecurity breaches were caused by some type of human error or behavior.[3] Companies of every size constantly struggle to defend themselves against hackers around the world intent on stealing identities, payment card information, and intellectual property, and manipulating the firm's systems to generate fraudulent payments. These malefactors can also penetrate the firm's IT environment to set up fake vendors in the payment system, email invoices (from employees' email accounts as attachments), and then email invoice approvals — using account coding from yet other employee email accounts. Cybercriminals may also duplicate the firm's processes in order to trick the firm into transferring large cash payments directly to the criminals. In this evolving, sophisticated hacking environment, every system exposed to the internet or other external interfaces must be protected against digital intrusion. Proper security must include user education and the application of preventive, detective, and reactive controls.

Who Are Hackers?

Many types of hackers exist, but they can generally be categorized by the following labels: "black hats" (those out to steal information or otherwise compromise entities' information security), "white hats" (those out to protect entities' information security), "gray hats" (those whose hacking may violate the law but who do not act with malicious intent), and "hacktivists" (social activists, such as Anonymous, who hack websites to advance a social, political, or religious agenda). White hats, often IT security experts, work for a company to find security weaknesses. Black hats are often in the news, as they spread malware or steal financial information, personal information, and login credentials.

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 A. Wayne Avellanet possesses decades of business experience working with corporations of all sizes in a variety of industries. His functional background includes internal, IT, and operational audit; information security; fraud investigations; and accounting, finance, financial analysis, and SEC reporting. Mr. Avellanet is a Certified Internal Auditor, Certified Information Systems Auditor, Certified Information Systems Security Professional, Certified Fraud Examiner, and Certified Management Accountant.

3 Adeola Adele, "Cyber risk: it's a people problem, too," Willis Towers Watson, willistowerswatson.com, September 25, 2017, accessed May 2, 2018, https://www.willistowerswatson.com/en/insights/2017/09/Cyber-risk-its-a-people-problem-too.

How Hackers Do It

Black-hat hackers obtain data through the illegal compromise of neglected, poorly designed, or under-protected systems. Hackers have proven to be quite adept at bypassing company systems; they can penetrate a company's systems by any number of methods. As mentioned above, in many cases, penetration into an organization can be accomplished simply via email. "Ransomware" is a relatively new threat; it is hostile code that encrypts victim machines and displays a splash screen demanding payment for decryption of the target. Unfortunately, in many cases, even if the organization pays the ransom, no actual solution is provided.

The typical modus operandi of a hacker today is to methodically penetrate a company's information security defenses and achieve the following objectives:

People are their own worst enemies, and many use similar passwords.

- Gain initial access. This is accomplished by guessing a password or the answers to security questions. It can also be done by exploiting numerous other weaknesses.
- Gain ever-higher levels of access. Once access to a system or user account is gained, the hackers will typically try to expand their access before exploiting it.
- Reconnoiter the system and identify valuable information. Once further access is gained, the hackers will reconnoiter the company's information assets and identify anything worth stealing such as intellectual property, money, and credit card information.
- Determine who has access to that information. The hackers will then identify which users have access to that information to expand their access. This process is repeated as needed until the hackers gain access to the targeted information.
- Exfiltrate, remove, or otherwise steal the information. Finally, when sufficient access is obtained, the hackers will remove the desired information, money, etc. In some cases, they will not remove the data but instead exploit their knowledge of the company's processes to extort funds from the company.

One method of penetrating a company's systems is by identifying the typical username configuration used by the organization and then running a program or script that guesses passwords. Hackers will use a known set of common passwords for this task. People are their own worst enemies, and many use similar passwords; according to Fortune.com, even as late as 2017, the top two passwords of all time were "password" and "123456."[4] Hackers will then identify the number of failed login user attempts that lock the account and the time period for attempts-to-lockout. They will set their program to stop at one try less than the lockout, wait the allotted time, then try again. A single computer will simultaneously attempt this on many accounts and many computers at the same time. For example, many firms use the first letter of employees' first names and the first seven to ten characters of their last names followed by the firm's domain name. Picture thousands of computers simultaneously attempting to log in to thousands of user accounts using usernames either easily found or deduced, for example, by searching a social media site like LinkedIn®, which provides the names of real individuals and their associated companies. Such attacks are known as advanced persistent threats (APTs).

The best way to bring order to the information-security strategy is for the organization to establish a set of policies that can be amended as new topics and risks arise.

Small and mid-sized corporations must understand that APTs are playing the long game. The goal is usually not merely to hack a company's system once and steal a list of credit card numbers or intellectual property, but to achieve that same objective systematically and, conceivably, forever. For example, if a foreign government wants access to the design of US military equipment, it might hack a defense contractor and steal this specific information. However, if the foreign power gains permanent access to the defense contractor's systems by obtaining sufficient user credentials, it can steal that data secretly in perpetuity. Even more disturbing, it could monitor the ongoing development of future systems and steal the technology as it is being developed.

How to Strengthen Information Security: Pinpoint Potential Weaknesses

Mr. Avellanet acknowledges that the topic of information security is broad and complex, and the level of detail can seem overwhelming. The best way to bring order to the information-security strategy is for the organization to establish a set of policies that can be amended as new topics and risks arise. Below are a few of the crucial controls necessary for strong information security.

4 Kirsten Korosec, "The 25 Most Common Passwords of 2017 Include 'Star Wars,'" Fortune.com, December 19, 2017, accessed May 2, 2018, http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/.

Data inventory. Every firm should know, and have properly documented, what information they have, where it is stored, and precisely how it is protected. Examples of proprietary, confidential, or otherwise protected information include the following:

- Email addresses
- Names of employees and their personal information such as phone numbers and addresses
- Any personally identifiable information (PII), which includes customer lists and customer purchase history
- Personal health information (PHI), which is also subject to state and federal laws
- Credit card, bank account, and other payment information
- Intellectual property of all types related to the firm's business
- Financial, sales, and any other business information subject to SEC disclosure rules
- Any other data that is unique to the firm, the disclosure of which could impair the firm's competitive advantage or grant any other firm or country unique knowledge not otherwise obtainable

Security patch update practices and "zero-day" threats. 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 the widespread ransomware attacks mentioned above. 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. The practitioner 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.

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.[5] Given the need for up-to-date anti-virus and anti-malware software, the organization should verify not only that the software is constantly updated, but also that it is properly updated and deployed on all the organization's devices. For various reasons, the 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.

An SLA signed by the organization should provide for location security, transmission security, encryption, and all other information security concerns related to cloud computing.

Data encryption. Secret, confidential, proprietary, and other types of secured data should be encrypted, at a very minimum, when in transit outside the firm's firewall and while stored in any cloud environment. Even when black-hat hackers cannot gain access to the organization's internal network, they can intercept internet traffic, so it is important that the firm's information is encrypted while in transit as well as when it is stored in a location the organization does not control.

Cloud computing and multi-location cloud configurations. 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. The practitioner should review SLAs for all of the organization's cloud computing solutions. All key information security concerns should be addressed in the SLA.

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

A popular axiom holds that there are only two types of organizations in the US, those that have been hacked and those that don't know they've been hacked.

Data loss prevention. In the event that a hacker gains access to an organization's system, the hacker 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 techniques as well, such as prohibiting the use of removable media and encrypting and filtering outbound email. The organization should have proven data loss prevention techniques, and alert logs should be prepared, tracked, analyzed, and acted upon.

Change management. Technology has evolved enormously over the last thirty years. Each successive change to any of the software, hardware (including internet-based cloud computing), or internal processes used to produce, store, or process the 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.

Previous hacking events. A popular axiom holds that there are only two types of organizations in the US, 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. The circumstances regarding the nature of previous hacking events must be explored and documented.

The sheer magnitude and complexity involved in information security virtually ensures that some potential vulnerability will go undetected by the firm.

Security training (at least annually). Information security is obviously very detailed and complex. It requires that all participants — employees, customers, vendors, etc. — have knowledge of their part in the organization's overall information security program. For these reasons, virtually all firms should require their employees — and perhaps vendors and other stakeholders — to complete an information security awareness training course at least annually. A variety of in-house personnel can be used to provide training in their area of expertise, or alternatively, there are numerous firms and organizations that provide this training.

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 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 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.

Information Security Controls Risk Assessment: Questions to Ask

Mr. Avellanet presents the following risk assessment questions:

- Is the information technology (IT) department, or a subset thereof, responsible for the firm's information security? If not, why not?
- Are password complexity standards enforced by the network security configuration?
- Are failed login attempts logged and investigated?
- Do the firm's password reset requirements involve validation of the user's identity?
- Does the firm have a current data inventory by type, system, geography, etc.?

- Are the organization's information security policies complete and current?
- Does the company use intrusion detection and prevention systems (IDS/IPS)? How are they configured? How are the configurations kept current?
- Are IDS/IPS event logs and alerts monitored, reviewed, and investigated?
- How are security patch updates tracked, implemented, and verified by the company?
- Are anti-virus and anti-malware solutions installed on all company devices? How are the threat libraries updated, and how frequently?
- Does remote access require multi-factor authorization? Which factors are used?
- Is the organization's critical data encrypted both at rest and in transit?
- How are the firm's encryption key libraries maintained and managed?
- Does the firm use cloud-based computing? Has the firm identified all locations in which its critical data is processed, transmitted, and stored? Are all locations covered and addressed by the security policies?
- How does the organization prevent data loss? Is a robust data-loss-prevention strategy employed? Are outbound transmissions (email, etc.) monitored for company data transmitted in clear text (that is, in an easily readable, unencrypted form)?
- Does the organization allow removable media? Are USB ports on laptops and other devices enabled? If so, how does the organization address the issue of data loss prevention?
- Is all critical data monitored by the firm? Is access to critical data at rest monitored to ensure that it is only accessed by valid programs and personnel?
- Does the firm allow ad hoc routers to be created by the connection of cell phones, tablets, or other devices to laptops and other computers that are connected to the firm's network? What precautions are taken to prevent the creation of ad hoc routers?
- What technologies are restricted by the firm? Is there a listing of nonpermitted technology? How does the organization validate that no restricted technologies, which might pose an information security threat, are attached to the company's networks?
- How is technology change managed? Is there a formal process for changing software applications? Servers and other hardware? Cloud-based configurations? Routers and other connectivity devices?
- Does the firm receive data from, or transfer data to, vendors, customers, or others? If so, how does the organization assess the information security of its vendors and others with whom it exchanges data or who may have possession of the company's data? Are information security considerations addressed in the service level agreements (SLAs) with these other parties?

- For internal data access, does the company employ the principle of least privilege — assigning users only the minimum rights necessary to complete the job? Do job descriptions reference the systems, data requirements, and segregation of duties for each position? How often are employees' data access privileges reviewed? Are privileges removed for terminated employees in a timely manner?
- Are information security weaknesses tracked? Is remediation progress tracked and reviewed on a regular basis? Is there regular reporting to management on remediation efforts?
- What is the firm's process for identifying new threats and known technical vulnerabilities? How are these emerging threats communicated throughout the organization? What department is responsible for assessing the threat to the organization and initiating the response?
- Has the organization experienced previous information security events such as successful hacking attempts and/or data breaches? If so, how many?
- Does the firm have a listing of state and federal regulations and reporting requirements with which it must comply in the event of a data breach?
- Does the organization have a data breach response plan?
- Following a possible breach, does the firm have a data recovery/business response plan?

- Is annual (or more frequent) information security awareness training required of all employees? How is compliance with the training tracked?
- Does the firm conduct regular penetration testing (pentesting)?
- Does the firm use reputable white-hat hacking firm(s) to emulate an advanced persistent threat (APT) and identify potential attack vectors so that the firm can take proactive steps to harden its information technology environment?

Additional Guidance and Resources on Meeting IT Security-Related Challenges

In addition to **Financial Management and Controllership's** Chapter 1109, Chapter 1618, Information Security, provides practice aids that can be modified to meet an organization's specific needs. The chapter includes a sample information security policy; sample procedures for overall security administration as well as conducting a risk management analysis and establishing an employee security awareness training and compliance program; and sample checklists and forms.

Access Your Cloud Accounting Software Without IT Burdens
Virtual Office CS® offers anytime, anywhere remote accounting software access, relieving you of the IT burden and ensuring business continuance in any situation. Our full line of CS Professional Suite® tax and accounting software and select Microsoft® products are available in the Virtual Office CS environment. With our cloud accounting software, your tax and accounting programs operate and integrate exactly as if the programs were loaded on your hard drive. But since the software is loaded onto our hardware, we take care of maintenance and updates — you simply log on, go to work, and enjoy peace of mind. Even in the event of a fire, theft, or natural disaster, your software and client data remain safe on our powerful servers. We perform routine data back-ups to ensure that your data is always secure. **Learn more**

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 professional publishing. His current responsibility is managing products in the areas of GAAP practice and financial management.

Nancy Ford is a senior editor, focusing primarily on controllership, bank accounting, and internal auditing.

Scott Gates is a senior editor, focusing particularly on corporate governance and GAAP.

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

Thomson Reuters®

Thomson Reuters is the world's leading source of news and information for professional markets. Our customers rely on us to deliver the intelligence, technology, and expertise they need to find trusted answers. The business has operated in more than 100 countries for more than 100 years. Thomson Reuters shares are listed on the Toronto and New York Stock Exchanges (symbol: TRI). For more information, **visit tr.com**.

About Financial Management and Controllership

Financial Management and Controllership from Thomson Reuters brings together the expert analysis and practical guidance today's financial managers and controllers need to succeed in all aspects of their roles. It is a powerful resource that addresses accounting and financial reporting, budgeting and forecasting, cost and cash management, human resources, controllership issues for smaller companies, and internal controls and risk management. It provides a repository of practice aids in the form of sample policies and procedures that cover more than 80 topics and include hundreds of customizable checklists, worksheets, forms, agreements, and schedules. The focus throughout is on practical guidance for the day-to-day operations of financial management and controllership.

For more information, visit **store.tax.thomsonreuters.com/accounting/Finance/Financial-Management-and-Controllership/p/100200682**

Contact us today: +800 950 1216

Visit tax.tr.com

The intelligence, technology and human expertise you need to find trusted answers.

the answer company™
THOMSON REUTERS®

TA568838_JUNE 2018_DGM