Addressing Cybersecurity Vulnerabilities

Omar Y. Sharkasi, CBCP, CFE, CRP, is a retired lead IT bank examiner at the State of Illinois (USA) Department of Financial and Professional Regulation-Banking Division (IDFPR). His significant work experience includes regulatory compliance in the fields of information security, risk management, business continuity, Payment Card Industry Data Security Standard (PCI DSS), fraud prevention/detection strategies, data loss prevention system implementation, and policy enforcement. Prior to the IDFPR, he worked in diverse industries in the field of accounting and finance.

Today's IT leaders face many challenges and rapid changes with respect to Internet security. IT leaders must increase cybersecurity public awareness and coordination across the subset of federal governments, all while having to do more with less. They have to protect enterprise, customer, citizen, member and employee data, while thwarting attacks from cybercriminals. The problem is that much of the legislation worldwide addresses regulatory compliance and fails in advising organizations on the ins and outs of information security. That is to say, following regulatory guidelines may ensure compliance but not necessarily offer system security. This leaves many enterprises scrambling to understand their information security infrastructure and obligations. Conducting secure transactions across the Internet relies on a number of factors, not the least of which is government guidelines.

The Internet contains a virtual encyclopedia of information. It is also touted as the platform upon which the majority of business and consumer transactions takes place. This responsibility is being thrust upon a network on which reports of security violations (e.g., cyberhacking, exploitable holes) are on the rise at the same time that fortifying any system requires daily diligence on the part of network administrators. The Internet has provided terrorists and other criminals with a deadly, sophisticated new weapon in their arsenal. Yet the full potential of secure Internet connections has not been realized. Until recently, service providers, government organizations and private enterprises have been unable to benefit from the cost savings and flexibility of choosing the right security tools to mitigate the risk of deliberately intercepted, stolen or corrupted sensitive data.

> "Much of the legislation worldwide addresses regulatory compliance and fails in advising organizations on the ins and outs of information security."

The point is, with all of the weapons and adversaries present—threats, malicious intruders, thieves, disgruntled employees, industrial espionage and so on—security professionals should be able to detect, prevent and address security incidents and, if needed, provide information to help prosecute computer crimes.

Knowing who has access to critical data and making users take proper precautions to safeguard their files, workstations and mobile devices are basic steps all businesses should take. It is vitally important for financial, legal and health care operations to overhaul their information security processes and require IT positions to be filled by qualified staff who have undergone thorough background checks. Thus, organizations should consider the US Patriot Act and legislation such as the US Gramm-Leach-Bliley Act (GLBA), US Health Insurance Portability and Accountability Act (HIPAA), US Identity Theft Act, the new press releases from the Federal Financial Institutions Examination Council (FFIEC), Financial Crimes Enforcement Network's (FinCEN) Executive Alert, the US National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), and universally accepted standards and frameworks such as the ISO 27000 series, COBIT® and Industrial Automation Systems technologies.

This article examines the key areas in security programs that need attention now. This, in turn, helps create a framework to assist in meeting regulatory and security requirements, ensure corrective actionable recommendations for new processes and upgraded techniques, and enable security teams to face today's issues and prepare for tomorrow's. While much of this article is based on US legislation and US business, the analysis is applicable to many other nations.

Naturally, IT issues, whether intentional or unintentional, and unchecked cybersecurity risk

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

factors are the major cause of weak security of any business technology innovation. Not everyone is comfortable discussing them publicly, and many are still working on the fix. Quite often, unchecked IT cybersecurity risk factors that remain unmitigated for too long—something that happens in almost all businesses—are the cause for unexpected cyberattacks. The following are necessary areas for improvement.

AREA FOR IMPROVEMENT 1—INVENTORY OF ASSETS/DATA CLASSIFICATION

The data resource is as important as capital or personnel. Because of their value, data must be managed and controlled carefully. As noted in the preceding section, in addition to personally identifiable data, every business has other, highly proprietary information that it must protect (e.g., intellectual property, marketing plans, new product plans, investor information, financial information). These are all valuable assets of the business, deserving of protection. However, most enterprises' assets are not clearly and appropriately accounted for to an established inventory scheme. If information/physical assets are not clearly and appropriately labeled and documented, the efficacy of the asset inventory and data classification programs is greatly diminished. Without assigning ownership for specific assets, it becomes difficult to ensure that assets will be appropriately protected on a continuous basis. Asset inventory and associated data classification degrees of protection must be determined and applied to all information. Deciding which assets need protection is half the battle. Focusing on those critical and sensitive business processes is a crucial step in defending against cyberattacks.

A strongly established data function or active and consistently applied data management principles can help ensure data integrity and security. No matter how big or small the information security budget is, the key to security is prioritizing the effort to protect data.

Securing data must begin with data classification. To help ensure the integrity of data and the application of sound data administration practices, security managers must address issues that affect the credibility and security of the data being used. Security managers can ask the following questions to assess the credibility and security of their data:

1. Is there a centralized asset management team? If not, set one up as soon as possible.
2. Does the team complete regular or, at minimum, spot reviews of the various analyses? Does it regularly work with data owners to update and add new data resources?
3. What data do users need to access?
4. Where are the data located?
5. Do the team and the data owners have established or defined rules by which particular information classes of instances must be stored, transmitted, archived, transported and destroyed?
6. How much sensitive/critical information is available on the Internet?
7. Does the team know the cyberrisk protection their vendors and other relevant third parties have in place?

Ultimately, various business owners and the IT department must decide on what technologies and risk they are willing to live with, since most of them will have to maintain and administer the controls in some form. An understanding of user needs and existing systems is necessary to strike a balance between asset productivity and security.

AREA FOR IMPROVEMENT 2—EMERGING TECHNOLOGY RISK

Assessing and minimizing the risk of emerging technology security are the first things enterprises do before using Internet of Things (IoT) technologies to manage IT systems, building equipment, smartphones and other web-enabled intelligent systems. These first steps ensure that these technologies have adequate safeguards to fend off hackers. Many such technologies are vulnerable to attacks that could disrupt building operations and, worse, give hackers access to enterprise systems.

> “Auditors should play a significant role in IT projects and be part of the monitoring processes.”

IoT increases the security complexity by promoting the use of web services, multitiered applications, distrusted databases, security zones and getting into a virtualization rut. For instance, enterprises began server virtualization in 2009 and chose virtualization hastily without appropriate risk assessment and with total reliance on vendors, hoping to learn from them and thinking of private cloud services as a safe choice. Typically, new technology initiatives are deployed without a detailed risk assessment in place. In fact, innovation often happens only after putting new IT projects in employees' hands without proper risk assessment, security, accountability and proper IT audit.

To reduce risk, enterprises should pay more attention to newly proposed technology initiatives, ensure involvement of IT auditors in the early stages of any IT project, and extend the audit scope to include new technologies and management systems. Additionally, the performance of postimplementation review should be considered or viewed as a value-added audit project by the audit team. The audit team needs to have the right level of support and sponsorship to engage in the early stage of any IT projects. Auditors should play a significant role in IT projects and be part of the monitoring processes to ensure quality inputs and the merits of the project, rather than simply being involved with the outcome.

New technology brings more ways to access new types of devices and alternatives to the traditional personal computer (PC) or mainframe platforms. However, many new technology initiatives lack proper controls due to the issue of not assessing and addressing security problems on time and ignoring their warnings. It is always best for enterprises to do a security review before completing due diligence. When security is not represented during due diligence, problems can go undetected and may be costly to fix at later stages of project implementation. Security experts suggest that the following steps should be taken in order to best protect new technology initiatives:

"When security is not represented during due diligence, problems can go undetected and may be costly to fix at later stages of project implementation."

- Integrate security at the beginning of the software development life cycle. Risk and threat assessments should be built in up front rather than bolted on later.
- Integrate security into the maintenance process, such as ensuring that all applications are patched regularly. Mobile device applications and bring your own device (BYOD) policies need to be included in the maintenance process so that these devices do not become vulnerable.
- Develop best practices for protecting legacy applications that might require special handling, such as building segmented networks and deploying any additional defenses that might be required for protecting legacy software.
- Make sure that security devices (e.g., security default settings) are configured correctly and the engineering team understands what the alerts mean.

AREA FOR IMPROVEMENT 3—THE SHEER SIZE OF THE RISK ASSESSMENT MODULES

The conventional model for risk assessment is questionnaires and onsite audits, with results recorded in documents and updated annually. As a result, a large number of risk assessment modules and methodologies have been created. Organizations use numerous risk assessment matrices that vary from department to department, identifying variations in risk and mitigation strategies across different assets, business processes and applications. Point-in-time, piecemeal assessments are no longer sufficient. Discovering this insufficiency led to the belief that IT risk assessment processes may be practiced in an *ad hoc* manner, without following defined processes or policies. As a result, IT risk processes are today considered ineffective, inconsistent, fragmented and not robust enough to provide tools to secure the IT environment and the related enterprise functions. Furthermore, the responsibilities for continuous risk assessment processes are informal and have limited authority. Risk mitigation strategies are a top concern for the board, senior executives, the chief financial officer (CFO) and risk managers. And despite the need for rapid change and a robust risk assessment program, the challenge remains for implementing an integrated approach that can be ingrained in an organization and its management practices. Without a coordinated risk management strategy, organizations will continue to struggle with repeated policy iterations before risk-handling procedures and controls are efficiently aligned. Simply put, enterprises must get a handle on risk management. It is a key link to instilling more customer confidence, higher profitability and company longevity.

For example, many enterprises actively hedge their IT portfolio risk to immunize against asset/liability mismatches. Others focus on building a tangible asset portfolio, which does not include intangible assets, securitized and managed by specialists. Depending on its strategy, an enterprise can now more effectively decide what market risk it wishes to manage or assume. Risk that falls outside these parameters is avoided by transferring it to a third party. An enterprise risk dashboard brings together all of the key risk exposures—operational risk, reputational risk and more. With this dashboard, management can review changes in exposure and evaluate the potential impact on capital allocation throughout the operations. Drilling down into the risk management decision areas gives management additional insight into inherent Internet risk (e.g., loss events, loss of data or reputational risk assessments) and into the methods of responding to risk (e.g., avoidance, reduction, sharing, acceptance).

> “These valuable business benefits of cloud computing cannot be utilized without addressing the new data security challenges posed by it.”

AREA FOR IMPROVEMENT 4—DATA RESIDENCY/CLOUD COMPUTING RISK

Data residency violation is considered a major contributor to cyberattack risk, and it can cause massive data breaches and regulatory compliance issues. Corporate data are stored by utilizing cloud computing services. There are numerous cloud providers headquartered in every corner of the globe, with data centers equally distributed, and the typical end users may not think to question where the corporate data they upload will be stored. Unfortunately, in some cases, that *where* is critical to remaining in compliance with data privacy and data residency regulations. The revelation that employees have been storing data where they should not is one that can end up involving not only data breaches, but also legal risk. The major cloud application providers tend to offer robust security, but the same cannot always be said of smaller or more niche providers. In fact, some providers do not even offer basic transport layer security such as Secure Sockets Layer (SSL) to protect data while in transit to their servers. Employees uploading sensitive documents on unencrypted connections is an issue that must be addressed.

Enterprises increasingly recognize cloud computing’s compelling economic and operational benefits. Virtualizing and pooling IT resources in the cloud enables organizations to realize significant cost savings and accelerate the deployment of new applications. However, these valuable business benefits of cloud computing cannot be utilized without addressing the new data security challenges posed by it. Deploying confidential information and critical IT resources in the cloud raises concerns about vulnerability to attack, especially because of the anonymous, multitenant nature of cloud computing. Applications and storage volumes often reside next to potentially hostile virtual environments, leaving information at risk to theft, unauthorized exposure or malicious manipulation. Moreover, it is possible for data to remain present when consumers vacate cloud volumes, but vendors may not recycle storage devices securely. Governmental regulations on data privacy and location present the additional concern of significant legal and financial consequences if data confidentiality is breached or if cloud providers inadvertently move regulated data across national borders. As enterprises make plans to deploy applications in private and public cloud environments, new security challenges need to be addressed.

Optimal cloud security practices should include encryption of sensitive data used by cloud-based virtual machines, centralized key management that allows the user (and not the cloud provider) to control cloud data, and an assurance that cloud data are accessible according to established enterprise policies. A key component of an IT cloud development strategy is conditioning the IT vendor infrastructure for cloud delivery. This may include virtualizing and automating existing systems and adding the vendor service management capabilities requisite for cloud computing. It is advisable to get a security assessment from a neutral third party before committing to a cloud vendor.[1]

AREA FOR IMPROVEMENT 5—MIND THE INTERNAL THREAT

While the majority of enterprises use networks as the backbone for secure data exchange transactions, standard encryption and firewall technologies can provide some measure of protection from outside attacks and theft by competitors, hackers or mercenaries. But what about the internal threat committed by the enterprise's employees armed with computer access and passwords? The employee element is commonly overlooked. In fact, one of the most common bugs exploited by hackers to gain access to the inner workings of equipment is using default passwords. Default passwords are, from a manufacturing point of view, a convenient way of ensuring that its engineers can get into the company's own computers when carrying out maintenance. Too often, security administration is overwhelmed with the task of trying to do it all (e.g., managing operating systems, applications, network, mobile devices, physical security). Security administration must segregate duties and define and deploy a security policy for one area before moving on to another hot spot.

In conjunction with preventing internal irregularities, segregation of duties (SoD) should be applied so that the person responsible for assessing users' level of access authorization is not the same person who implements the access controls. Traditionally, SoD has been used to prevent any one individual from having sufficient power to perpetrate a fraud or as a check on the correct performance of one person's duties by other personnel. This principle of internal control is fairly easy to follow for simple systems, which have well-defined processes and few interfaces with other systems. However, as systems become more complex, the number of interfaces among subsystems increases, as does the risk of error in the communication process. In this case, the SoD can increase risk rather than prevent control problems.

Besides the control problems that can result from improper SoD, two other security aspects represent direct threats to data integrity. First, the existence of the privileged user role partially violates the traditional control principle of SoD. Second, the privileged user has available tools that, though necessary for the performance of various functions, can be used to override established controls. For example, tools exist to establish various levels of access and update authorization, crack and find user passwords, restructure the databases, and manipulate programs and files.

The privileged user can assign to a program a level of access, modify the web design and update authorization that can override all other controls. Furthermore, access paths can be eliminated to remove records from audit trails. For these reasons, database or security tools must be used only for their intended purposes.

The primary emphasis must be placed on administrative controls. Several remedial steps can be undertaken to increase controls and reduce the risk of internal threats. And the requirement to meet compliance demands, mitigate insider risk, and manage access and privileges of temporary workers, contractors and third parties is driving the requirement for least-privilege security across the Windows operating system (OS) environment and beyond to UNIX and Linux systems, regardless where these systems run (on the premises or in the cloud).

Poor password security and the "too much privilege" problem need to be addressed by delegating security administration and limiting what administrators can do to the tasks and resources required for their job roles, while enabling a fast, simple method of privilege elevation when required. A wide range of roles and rights are available in the Windows OS to implement least-privileged access for any user in the environment, while flexible and granular secure delegation using common sense allows for simplified management of roles and rights.

AREA FOR IMPROVEMENT 6—END-POINT SECURITY

Unfortunately, the issue of end-point security is being ignored by a significant number of enterprises. But the growing number and variety of threats to end points, in addition to the threats that use end points as a vector, have made end-point security a relevant topic to cybersecurity. Common end points are laptops, desktops, PCs and mobile devices. Most of these devices are not under the control of an organization, and one of the main concerns is management controls. As technologies continue to expand to meet the challenges of components' integration and data sharing, and as mobile workforces continue to grow and more people access corporate resources over structured public networks, the challenge becomes controlling what data should be allowed to reside on those end points or mobile devices and, when allowed, securing the data while at rest and in transit. Security administration should always weigh the security advantages of totally locking down an end point so no applications can be loaded, no port is active and no unauthorized communications can occur vs. the productivity gains of allowing people to use the technology being offered. To be effective, end-point security must balance the security risk with the productivity benefits. The right approach must also address the IT challenges faced by business today—mainly regulatory compliance and overburdened and understaffed IT departments. The solution sometimes requires compromise and relies heavily on solution tools that could manage, assess or control security at the end point. End-point protection should be focused on tools that deliver a centrally managed, web-based, easy-to-use, fully integrated management interface that delivers a full suite of protection to end points.

Clearly, no end point is truly secure without an integrated and embedded multilayered security approach throughout. End-point security tools should also be supported by a management dashboard that provides real-time security posture reporting over all managed end points.

A product of layering insecurity may take years to develop, deploy and implement once configurations have been created. Furthermore, as the number of connections to business partners increases, the amount of remote access grows, and the variety of services offered to customers rises. The originally reasonable set of security layers in network architecture can turn into a complex tangle of security mechanisms that may not be effective and may introduce more system vulnerabilities. The key to making the most of security layers remains in segregating sensitive data into separate zones. Also, the security designer must conduct a full analysis of the enterprise's layered security every year and repeat the assessment with every major addition to the enterprise's network environment. All of these factors—and many more—must be evaluated before selecting any sort of end-point security solution.

AREA FOR IMPROVEMENT 7—STRUGGLING TO DEAL WITH LEGACY SYSTEMS

Now that Microsoft has pulled the support plug for Windows XP, financial institutions (FIs) and companies that have not switched to Windows 7 need to explore their options. For FIs, this means upgrades to Windows 7 and Agilis 3 are required to keep up with the latest patches and maintain Payment Card Industry Data Security Standard (PCI DSS) compliance. Most FIs began a legacy system replacement early in 2014. But some FIs failed to truly understand the complexity of management reporting they had developed internally over the years, not to mention integrating multiple systems from different vendors. Specifically, neglecting the reliance on numerous system features or databases that tied to the old system required processing and culture changes to switch software and get off of those old functions. For these reasons, FIs felt that they needed a more comprehensive compliance plan before jumping in with upgrades. As a best practice, many FIs found it possible to get by with a special contract with Microsoft in which they could keep Windows XP and get the necessary security patches to remain compliant until they are ready to upgrade in conjunction with other planned changes.[2] Now that the Windows XP transition deadline has passed, continuing to ignore the upgrade puts FIs at risk. And because other requirements are coming, it makes sense to create a plan that addresses not only a Windows 7 upgrade, but future needs as well.

> “Data must be available anytime, on time and anywhere in the organization, whether IT approves of it or not.”

In addition to the Windows 7 requirement, FIs must address Europay/MasterCard/Visa (EMV) liability changes, which are a series of updates that will shift the liability for card counterfeiting losses from card issuers to transaction acquirers that do not enable EMV transactions.[3] These shifts began in 2015. In addition, PCI DSS 3.0 and 3.1 guidelines state that an updated version of the Encrypting PIN Pad (EPP7) will be required to maintain compliance on automated teller machines (ATMs) purchased, installed or moved after April 2014. ATM compliance and technology changes focus on EMV and EPP7.[4] Of these two, EMV requirements are more involved, with implications for ATM hardware, software and network systems.

Fraud-prevention advocates welcome EMV technology. The adoption of EMV technology, which replaces traditional magnetic stripe payment cards with more secure chip cards, could eliminate up to 30 percent of the US $8.6 billion in annual fraud losses by card issuers and merchants in the US.[5] Generally, card fraud drops in areas where EMV is in place, so the long-term gains are worth the short-term pain of transition. EMV cards are replacing current magnetic cards or non-EMV chip cards. Adoption of EMV depends on the region. Adoption was first seen in Europe, followed by Asia-Pacific, Latin America and Canada. While EMV adoption is not mandatory, it will be necessary in order to accept EMV chip cards. The US is one of the last countries to migrate to EMV. In 2011 and 2012, American Express, Discover, MasterCard and Visa all announced their plans for moving to an EMV-based payments infrastructure in the US.[6]

AREA FOR IMPROVEMENT 8—FILE-SHARING APPLICATIONS

Effective file sharing is a necessity in knowledge-intensive organizations. Today's knowledge workers want and demand access to their files whenever and wherever they need them. Data must be available anytime, on time and anywhere in the organization, whether IT approves of it or not. Employees are bridging the established enterprise infrastructure into their preferred work environment using solutions that corporate IT departments do not, cannot or are slow to approve. In short, knowledge workers are willing to look at tools outside of the paradigm offered by corporate IT to meet their needs.

As such, some organizations have users accessing hundreds of unsanctioned cloud applications, of which half or more are often file sharing. There are two problems with free or cheap consumer-facing file-sharing cloud applications: There are a lot of them, and not all of them are equally secure. As they have become more ubiquitous, file-sharing applications have become a significant concern for IT departments, especially in security-sensitive industries such as financial services. IT departments have to decide how strict the regulation of these applications will be and enforce compliance with these regulations. IT can outright prevent the installation of the application on workplace desktops and laptops through administrative lockdown (at the expense of the freedom of end users to customize their workstation). Access to web-based file-sharing services can also be restricted by blocking specific domains. But IT will have a harder time preventing information from leaking through mobile device sharing. As with most personal unmanaged applications (PUAs), file-sharing applications may be used with or without IT consent.

Documentcentric team collaboration is required for producing a variety of outputs, including internal-facing planning documents and external-facing deliverables. IT teams need adequate tools to collaborate around work-related documents. Collaboration platforms (e.g., Microsoft SharePoint) offer content repositories for working with documents, but many IT departments have set these tools up in a restrictive, cumbersome and unintuitive manner. It is important to establish strict, enforceable policies that are frequently communicated while still allowing users enough freedom to operate and manage their data comfortably.

AREA FOR IMPROVEMENT 9—SECURITY MATURITY AND REMOTE ACCESS

User systems are only as effective as the data they use. Data administration protects data from corruption and promotes the effective use of data. However, there are still a large number of enterprises that do not have a good grasp of control characteristics, classifications and requirements. Management needs to understand control requirements before assessing control strengths and weaknesses. In other words, there should be a basis or baselines in place (e.g., standards, guidelines, benchmarks) prior to control measurement and assessment.

> "No doubt, virtualized systems make it harder to manage risk, but sensible common sense security practices still apply."

Remote access is on the increase and telecommuting (working from home)/telepresence (video and audio communications for meetings) technology is becoming more prevalent as enterprises move to capitalize on its benefits, including gains in productivity and worker satisfaction. But administrators still have to master security best practices regarding these technologies.

Remote users can access corporate network services and resources with the same efficiency and functionality as if they were in the office. Business partners can connect to each other's networks, allowing for sharing proprietary information on joint projects.

The problem for many organizations is finding an efficient, affordable, scalable means of authenticating virtual private network (VPN) users. While there are many authentication solutions on the market, not all provide the best authentication and security solutions. Organizations want their VPN connections secure, but realize the security is only as strong as its ability to deploy a system, maintain it and have users consistently employ it.

No doubt virtualized systems make it harder to manage risk, but sensible security practices still apply. The key is deciding when to use tunnel vision technologies such as Internet Protocol Security (IPSec) VPNs and when to use SSL VPNs. Both IPSec and SSL VPNs can provide enterprise-level secure remote access, but they do so in fundamentally different ways. Before choosing to deploy either, or both, an enterprise should know how IPSec and SSL VPNs stack up in terms of security and what the cost is for that security administrative overhead. Security is built on standards and products that implement those standards, but it ultimately depends on appropriate deployment and sound policy definition. It is not always that simple, of course. Vendors promise to deliver secure access, but are SSL VPNs as secure and reliable as IPSec?

VPN vendors point out three essential security requirements:

1. **Authentication and access controls**—Each VPN type presents different options for user authentication with clear implications for security. The fundamental difference in how SSL and IPSec VPNs implement access control is an important consideration in where and how each technology is best applied.
2. **Defense against attack**—Strong data configuration and integrity and resistance to message replay and other attacks are essential to make a VPN secure.
3. **Client security**—The tunnel cannot be secure if the host client is compromised. VPN client computers need strong authentication and firewall protection, and administrators need a way to check on the health of those systems.

While most organizations acknowledge the need for some sort of security, it is quite another matter to implement it. Yet it seems too many of these policies fail to create an effective IT security platform to handle the scale and complexity of managing cybersecurity risk for an enterprise today. However, the purpose of developing policies is to ensure prevention rather than detection. Prevention is deemed to be proactive. Detection is reactive. When dealing with flaws, detective controls are considered inefficient when compared to preventive techniques. Preventive measures stop flaws up front rather than finding and fixing them once found, which may be too late and costly to address. Knowing security controls up front allows development teams to build cost estimates and prioritize security issues alongside other priorities at project or iteration inception. Implementing upfront controls is most effective, and only then can application owners decide to accept the risk or mitigate the risk at the planning stage rather than at a later stage.

Clearly, at the very least, companies should adhere to a recognized standard (e.g., ISO 17799) and place a high priority on educating and communicating with employees about the risk of Internet communication and the threat of cyberspace landscaping. Security threats are growing more complex and more sophisticated, so businesses' weapons against them need to be more sophisticated as well.

AREA FOR IMPROVEMENT 10—CYBERSECURITY TEST TOOLS

Cyberattacks on enterprises and banks worldwide reflect a frightening new era in cyberwarfare. As many security experts say, "You cannot hack or protect what you cannot see." Traditional network security strategies have become increasingly complex and costly, yet they do not deliver the level of reliability that modern mission-critical computing environments require. The solution is moving to a deeper, inside-out software-based approach that greatly reduces the number of vulnerabilities that hackers and cybercriminals can exploit. Cybersecurity stealth tools do exactly this and are an innovative, software-based approach to security that saves money, increases security, and is an agile component that adapts to changes in critical business networks and rapidly evolving regulatory requirements. Enterprises need to understand the threat landscape and engage in basic cyberhygiene to be able to mitigate a broad range of cyberrisk. This includes knowing all the devices connected to the network, what software tools are being used, how to hide data, and who has administrative permission to change or bypass/override system configurations and reducing that number to only those who need those privileges. To that end, it is good to see developers starting to introduce security tools that bring together maintenance and help-desk products with the security system. Security professionals should become familiar with the tools, techniques and weapons used in attacking their security infrastructure. Then they will be prepared to make a number of wise acquisitions, bringing in the best-of-breed products.

> "The solution is moving to a deeper, inside-out software-based approach that greatly reduces the number of vulnerabilities that hackers and cybercriminals can exploit."

Often, cyberattacks such as identity theft, account takeovers and mass disruption might have been prevented if the enterprise had been aware that their network was being accessed via cybersecurity tools. Security experts agree that nothing can be done to prevent cybersecurity criminals from using The Onion Router (Tor) without raising the risk to legitimate users.

Tor is software designed to allow someone to remain anonymous when accessing the Internet. It has been around for some time, but for many years it was used mainly by experts and enthusiasts. Tor's hidden services and anonymous browsing enables cybercriminals to cover their operations and provides a hosting platform to sell stolen information using bitcoins as currency. Tor is also dual-use software. For instance, it can be used by security professionals to hide data from cybercriminals and intruders, but it can also be used by criminals to hack into an Internet network and compromise its security. The key is to target those who would misuse the technology, and not the technology itself.

In addition to Tor, tools called botnets are emerging and are being installed on the compromised systems to attack the victims by controlling them from a remote location. The word "bot" (from robot) refers to automated software programs that perform specific tasks on a network of computers with some degree of autonomy. Typically, computers become bots when attackers illicitly install malware that secretly connects the computer to a botnet. These tools, among others, are readily identifiable through open-source research.

Another way of looking at security products is to look at the risk of free and open-source software (FOSS). FOSS refers to software tools that users are allowed to run, study, modify and redistribute without paying a license fee.[7]

There are benefits to using FOSS. FOSS offers the ability to create new applications quickly, reliably and economically. The desire to save money, develop quality and solid pieces of code, and reduce dependence on one or more vendors are the key reasons why enterprises of all sizes are taking FOSS seriously. Thus, FOSS products are gaining broad acceptance in organizations around the world and are moving into the cloud.

Drawn by similar competitive advantages, enterprises are beginning to merge open-source applications with the cloud. Increasingly, the building blocks of Software as a Service (SaaS) applications, cloud platforms (Platform as a Service [PaaS]) and cloud infrastructure (Infrastructure as a Service [IaaS]) are composed of open-source components. These versatile technologies provide vital competitive advantages, but they can also introduce risk when employed without adequate precautions. Recent evidence suggests that the presence of application vulnerabilities in open-source software is a far more pervasive problem than most people realize. Nevertheless, the use of FOSS does pose a risk, and generally FOSS tools are permitted to access the source code or allowed to redistribute programs. The risk comes from integration tools and a lack of technical skills or support to manage open-source efforts. FOSS redistribution access may be permitted due to concerns about security and licensing. FOSS adoption and usage necessitates the ability to enforce security policies, ensure SoD and protect an enterprise's intellectual property and programming integrity. When it comes to applications, security must be as pervasive as software codes themselves and the continuously evolving threats against applications.

Firms may benefit immediately from a heightened awareness of security tools and incorporating their knowledge into their transaction monitoring efforts to prevent unauthorized intrusion and/or hide sensitive data from possible intruders. What can security tools do for a company?

- Keep Internet users from becoming Internet abusers.
- Guard against network-draining viruses, spam and chain email.
- Crack weak passwords for policy enforcement and controls.
- Mitigate legal, compliance and reputational risk.
- Protect and prevent intellectual property or confidential information leaks.
- Improve logging management capabilities, facilitate incident investigation and provide an accurate audit trail.

WHAT CAN BE DONE?

It is evident that there is no simple solution to securing an enterprise's critical infrastructure. The process takes a lot of time and effort and some careful planning. A combination of three strategies—policy and technologies designed for cybersecurity, best practices, and a focused effort—are effective in mitigating the risk of attacks on enterprise systems.

In 2014, NIST[8] and FFIEC[9, 10] announced that they would build strategic security safeguards to help cyberspace users escape an emergency and devise and implement effective cyberrisk management and security policies to reduce cybersecurity threats and keep business and other organizations safe. At this point, sharing knowledge of vulnerability, threats, incidents and security safeguards used by others is highly encouraged to mitigate cybersecurity risk.

To get started on this track, enterprises of all kinds are trying to protect themselves against advanced persistent threats (APTs) by relying on firewalls and other traditional signature-based antivirus defenses. In addition to antivirus and firewall technologies, IT security practitioners need a mix of tools as cited in frameworks such as the Cybersecurity Framework or the FFIEC announcements and guidelines.

They should begin by implementing well-understood best practices, starting with end-point hardening to remove existing malware and to close and manage vulnerabilities. Even then, they ought to have a plan for detection and a response strategy if a breach should occur. Here are three key tools to maintain and consider when mitigating cybersecurity risk:

1. The NIST Cybersecurity Framework encourages network equipment manufacturers, enterprises, service providers, government agencies and federal integrators to take an active role in risk management, with the goal of improving the security posture and defending the IT critical infrastructures from cyberattackers and intruders. The NIST framework's approach to risk assessment is best described as a life cycle of activities based on five core functions that organize cybersecurity activities at their highest level. The framework consists of three parts: the framework core, the framework profile and the framework implementation tiers. The most important thing to remember is that risk is evolutionary, which means these activities must be continuously repeated and refined. This is NIST's first attempt at improving cybersecurity infrastructure, so this framework only scratches the surface of the activities involved in the risk life cycle. Each of these steps seems intuitive, but few organizations effectively execute all of these steps at any given time. The security chain is only as strong as the weakest link.[11]
2. FFIEC announced and introduced a cybersecurity assessment summary on its web site.[12, 13, 14] This initial round of assessments focuses on five key components of cybersecurity preparedness: risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyberincident management and resilience. Per FFIEC guidance, FIs should think like hackers and develop a risk-based approach to security activities to mitigate increasing cyberthreats. To implement this type of holistic approach, security professionals must practice a variety of defense techniques (e.g., configuring access controls, addressing distributed denial-of-service [DDoS] readiness, assessing the capabilities of universal serial bus [USB] ports, enhancing BYOD security, and focusing on procedures such as penetration testing and ethical hacking). More specifically, each FI is expected to monitor incoming traffic to its public web site, activate incident response plans if it suspects that a DDoS attack is occurring, and ensure sufficient staffing for the duration of the attack, including leveraging next-generation test tools to assess and manage cybersecurity risk. Implementing NIST and/or FFIEC holistic approaches requires intensive training while developing a risk-based approach to security. Just as vital, though, is the need for cybersecurity education for all security experts. They must also learn how to properly use cybersecurity tools and conduct an organizational security audit to identify security breaches and other problems.
3. It is advantageous to strengthen IT relationships and categorize best business practices. Proactively managing cybersecurity risk is a must. From this perspective it is possible to broaden the sphere of knowledge to the risk landscape, beyond what has traditionally been an IT-based discipline. Being prepared to detect and respond to attacks and attempted attacks starts with knowing the computer environment. This should include having a cyberattack contingency plan. Having a business resilience plan that includes cyberattacks will not only save money on impacting events, it will also allow business to resume much sooner than if data are lost or compromised.

CONCLUSION

Attackers need to find only one weakness to get into an enterprise system and spread their reach. Defenders need to plan for the inevitable breach and have a plan in place. If enterprises run out of options to deal with a cyberattack, they are done. Enterprises need to make sure that they are managing cybersecurity as they go.

Security professionals are going to have to make the correct investment in security infrastructure based on a sound cybersecurity plan that leverages industry standards and extends beyond traditional security standards to ensure strong preventive measures, more rapid detection, response and recovery (should a breach occur). For now, decision makers within the government and private sectors need to exert more efforts to that end, invent new and creative ways to protect IT infrastructures, adopt the best security practices, and educate the end user with a formally defined security policy to minimize data leaks.

ENDNOTES

[1] Gartner Group, "Assessing the Security Risks of Cloud Computing," June 2014, *www.gartner.com/doc/685308*

[2] Stewart, D.; "Outlook for ATMs After Windows XP," *BAI Banking Strategies*, 16 April 2014, *www.bai.org/bankingstrategies/Distribution-Channels/ATM/Outlook-for-ATMs-after-Windows-XP?utm_source=BSO_Daily_041714&utm_medium=email&utm_campaign=BSO_Daily_Enewsletter&utm_content=thoughtleadership&ca=901590949I*

[3] *Ibid.*

[4] PCI Security Standards Council, *Requirements and Security Assessment Procedures, Version 3.0*, November 2013, *www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf*

[5] Controy, J.; J. Fishman; *From Mag Stripe to Malware: Card Security Risks in 2011*, 13 July 2011, *www.aitegroup.com/report/mag-stripe-malware-card-security-risks-2011*

[6] *Ibid.*

[7] Federal Financial Institutions Examination Council (FFIEC), FIL 114-2004, "Risk Management of Free and Open Source Software," 24 June 2014

[8] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 2014, *www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*

[9] Federal Financial Institutions Examination Council (FFIEC), Advisory Letter, 24 June 2014

[10] Federal Financial Institutions Examination Council (FFIEC), Advisory Letter, 2 April 2014

[11] *Op cit* NIST

[12] *Op cit* FFIEC letter 24 June 2014

[13] *Op cit* FFIEC 2 April 2014

[14] FinCent Resource Center, Intelligence Division, Cybercrime Against Financial Institutions, *www.fincen.gov*