Integrating Real Life Cases Into A Security System: Seven Checklists For Managers

Hossein Bidgoli
California State University-Bakersfield

This paper examines seven recent real life cases related to computer and network security breaches, vulnerabilities, and successful security enforcements and then propose seven checklists for managers to consider when designing a security system. The checklists include (1) understanding the landscape of computer and network security, (2) putting together the basic safeguards, (3) identifying security threats, (4) identifying security measures and enforcement, (5) understanding the services of computer emergency response team, (6) preparing a comprehensive security system, and (7) the business continuity planning. If these checklists are followed they should increase the chances of success for designing and implementing a security system.

INTRODUCTION AND BACKGROUND

In recent months, several major private-sector and public-sector organizations have been hacked, including, Yahoo!, Anthem Blue Cross, the Home Depot, Target , Neiman Marcus, Adobe, RSA, Lockheed Martin, Oak Ridge National Laboratories, and the International Monetary Fund. Ponemon Research conducted a survey of 583 U.S companies, ranging from small organizations with less than 500 employees to enterprises with workforces of more than 75,000. Ninety percent of the respondents indicated their organizations' computers and network systems had been compromised by hackers at least once in the previous 12 months; nearly 60 percent reported two or more breaches in the past year. Over half the respondents indicated they had little confidence in their organization's ability to avoid further attacks. Roughly half blamed a lack of resources for their security problems, and about the same number said network complexity was their main challenge to implementing security protections (Vijayan, 2011). The following seven cases put our discussion into perspective and provide insight for the proposed seven checklists for designing a security system (Bidgoli, 2017).

Case #1: Data Breach at Home Depot

In September 2014, the Home Depot payment systems was breached, which may have impacted more than 56 million credit/debit cards. In addition hackers stole more than 50 million of its customer's e-mail addresses (Unknown, 2014). Target, Michaels, and Neiman Marcus are other retailers that have faced security breaches in recent months. The hackers used custom-made software to hack the system that is difficult to detect. According to the report, prior to the attack, Home Depot has tried to keep the cost dawn and reduce the system downtime at the expense of improving security. It did not encrypt the customer card data on its registers and computers inside its stores and did not activate intrusion prevention feature in its software suite (Elgin, Riley, & Dune, 2014).

The security breach has been going on for about five months, from April through September 2014. Home Depot data breach is significantly larger than Target Corporation breach, which impacted nearly 40 million cards. So far the data breach has cost Home Depot $62 million but it received 27 million from the insurance. The total cost to date is not known including the upgrade cost and possible cost of losing customers. Banks reissued customer cards that were breached, costing about $8 per card. Home Depot tried to win the customers back by offering a year of free identity protection services, including credit monitoring for those who have used the system in the five month period. After the attack Home Depot has encrypted customer card data and has enhanced its security system (Team, 2014).

Case #2: Identity Theft at Internal Revenue Service

In 2011 alone, the Internal Revenue Service (IRS) sent more than $5 billion in refund checks to identity thieves who had filed fraudulent claims. It was estimated at the time that another $21 billion would be lost to identity theft in the succeeding 5 years. Tampa and Miami were the two top cities from where fraudulent tax returns originated, the perpetrators usually stealing the identities of dead people, children, or someone else who normally does not file a tax return. In 2011, the IRS detected about 940,000 fraudulent returns; however, it was estimated that another 1.5 million cases went undetected. In one case, a single address in Lansing, Michigan, was used to file 2,137 separate tax returns totaling $3.3 million. To combat this problem, the IRS needs access to third-party information in order to verify returns. Also, the timing of when employees can file their returns and when employers submit their withholding and income information needs to be synchronized. The IRS currently uses new ID theft-screening filters that will not issue refunds until the IRS can verify a taxpayer's identity. There is another system in place that flags returns filed with Social Security numbers of individuals who have died. As of April 2012, the new ID theft-screening filters system had stopped approximately $1.3 billion in potentially fraudulent refunds (Bidgoli, 2017).

Case #3: Security Breach at Sony's Playstation Network

Some call it the largest breach of confidential user information in history. The attack occurred on April 20, 2011. It resulted in the loss of more than 75 million customers' crucial information from Sony's PlayStation Network (PSN) and Qriocity music and video service. The stolen information included name, address (city, state, and zip), country, e-mail address, birthday, PSN password, login name, and possibly credit card information. It is believed that hackers exploited a weakness in the PlayStation 3's encryption system and accessed the public key required to run any software on the machine (Stuart, 2011). This would cost Sony over $170 million, not including the loss of reputation and trust that the company had enjoyed for many years. Sony has been unable to determine who attacked its networks. The company did not even know that so much of its customer information had been stolen until an external security consultant discovered the theft a week after the incident took place. According to Sony, credit card information was encrypted. To conduct a thorough investigation and improve and rebuild the security of the network services for the future, Sony disconnected PlayStation Network and Qriocity services for several days. This situation underscores that, given the growth of cybersecurity threats, console makers must beef up their security systems. Furthermore, console users must be aware of these threats when they are online (Kuchera, 2011 & Schiesel, 2011).

Case #4: Lost and Stolen Laptops

With wireless connections now available in many public places, laptops are more popular than ever. However, they can easily be lost or stolen. And replacing the laptop is not the only problem. You also have to replace the data stored on it, which can be a quite serious loss. In 2006, an employee of the U.S. Department of Veteran Affairs lost a laptop that contained personal information regarding 26 million veterans. The same year, an employee of the American Institute of Certified Public Accountants (AICPA) lost a laptop that stored the Social Security numbers of AICPA's members. If unauthorized users gain access to this kind of confidential information, identity theft and other crimes can result. To make laptops more secure, consider the following recommendations (Bueb & Fife, 2010):

- Install cable locks on laptops, and use biometric security measures.
- Make sure confidential data is stored on laptops only when absolutely necessary.
- Use logon passwords, screensaver passwords, and passwords for confidential files.
- Encrypt data stored on the laptop.
- Install security chips that disable a laptop if unauthorized users try to access it. Some chips send out an audio distress signal and a GPS alert showing the laptop's location.

Case #5: Computer Viruses Target Medical Devices

Medical devices that are controlled by computer software—from heart monitors and pacemakers to mammogram and X-ray machines—are new targets for computer viruses and malware. This could put patients at risk, although no injuries or deaths have been reported so far. The Food and Drug Administration is warning the manufacturers of medical devices about the problem and is requesting them to review the parts of their security plans that are related to these devices when they seek approval from the government agency.

A Department of Veterans Affairs report has shown that 327 devices at VA hospitals have been infected by malware since 2009. In January 2010, a VA catheterization laboratory was temporarily closed due to infected computer equipment that is used to open blocked arteries. And in a case at a private Boston hospital, computer viruses exposed sensitive patient data by sending it to outside servers. The increased applications of electronic record systems as a part of the 2009 stimulus package is adding to this risk.

Manufacturers must improve the security features of these devices, making them more difficult for hackers to break into. And there needs to be close coordination between the manufacturers and healthcare providers to further enhance security. Also, hospitals and medical facilities must make sure that all the software running these devices is up to date and any updates have been installed. Finally, these devices must be blocked from Internet access (Weaver, 2014).

Case #6: Data Theft and Data Loss

Memory sticks, PDAs, CDs, USB flash drives, smartphones, and other portable storage media pose a serious security threat to organizations' data resources. Theft or loss of these devices is a risk, of course, but disgruntled employees can also use these devices to steal company data. The following guidelines are recommended to protect against these potential risks (Unknown, 2010):

- Do a risk analysis to determine the effects of confidential data being lost or stolen.
- Ban portable media devices and remove or block USB ports, floppy drives, and CD/DVD-ROM drives, particularly in organizations that require tight security. This measure might not be practical in some companies, however.
- Make sure employees have access only to data they need for performing their jobs, and set up rigorous access controls.
- Store data in databases instead of in spreadsheet files, for better access control.
- Have clear, detailed policies about what employees can do with confidential data, including whether data can be removed from the organization.
- Encrypt data downloaded from the corporate network.

Case #7: Biometrics at Phoebe Putney Memorial Hospital

Phoebe Putney Memorial Hospital, a 443-bed community hospital in Albany, Georgia, needed to improve its electronic health record (EHR) system. Doctors and nurses were complaining about the number of passwords required to access clinical records, so the hospital switched to fingerprint scanners, which, along with a single sign-on application, made the EHR system both easier to use and more secure. With the scanners, it is possible to audit usage, thereby ensuring that only authorized users have access to sensitive information. Another advantage of fingerprint scanners: Fingerprints do not get lost like smart cards (Anderson, 2010).

In the following pages we describe the proposed seven checklists for designing a security system which integrates the experiences gained from the analysis of the above seven cases.

CHECKLIST 1: UNDERSTANDING THE LANDSCAPE OF COMPUTER AND NETWORK SECURITY

Hackers, computer criminals, and cyber criminals, both domestic and international, could cost the U.S. economy over $100 billion and 500,000 jobs per year, according to a 2013 report by the Center for Strategic and International Studies (CSIS), a Washington D.C. think tank. The costs will include stolen identities, intellectual property, and trade secrets as well as the damage done to companies' and individuals' reputations. The total cost will also include the expense of enhancing and upgrading a company's network security after an attack. The CSIS report went further and included the opportunity costs associated with downtime and lost trust as well as the loss of sensitive business information. Job losses would include manufacturing jobs as well as jobs where stolen trade secrets and other intellectual properties resulted in jobs being moved overseas. Actually, the total cost may even be higher than the CSIS report projects, given that businesses often do not reveal or admit certain cybercrimes or do not even realize the amount of damage that has been caused by computer criminals and cyber criminals (Corbin, 2013). Table 1 lists basic security risks.

TABLE 1
BASIC SECURITY RISKS

Spyware and Adware
Phishing and Pharming
Keystroke Loggers
Sniffing and Spoofing
Computer Crime and Fraud (ID theft, industrial espionage, and sabotage)

Spyware is software that secretly gathers information about users while they browse the Web. This information could be used for malicious purposes. Spyware can also interfere with users' control of their computers, through such methods as installing additional software and redirecting Web browsers. Some spyware changes computer settings, resulting in slow Internet connections, changes to users' default home pages, and loss of functions in other programs. To protect against spyware, you should install antivirus software that also checks for spyware or you should install antispyware software, such as Spy Sweeper, CounterSpy, STOPzilla, and Spyware Doctor.

Adware is a form of spyware that collects information about the user (without the user's consent) to determine which advertisements to display in the user's Web browser. In addition to antivirus software, an ad-blocking feature should be installed in your Web browser to protect against adware.

Phishing is sending fraudulent e-mails that seem to come from legitimate sources, such as a bank or university. The e-mails usually direct recipients to false Web sites that look like the real thing for the purpose of capturing personal information, such as Social Security numbers, passwords, bank account numbers, and credit card numbers.

Pharming is similar to phishing in that Internet users are directed to fraudulent Web sites with the intention of stealing their personal information, such as Social Security numbers, passwords, bank account numbers, and credit card numbers. The difference is that pharmers usually hijack an official Web site address by hacking a Domain Name System server, then alter the legitimate Web site IP address so that users who enter the correct Web address are directed to the pharmers's fraudulent Web site.

Keystroke loggers monitor and record keystrokes and can be software or hardware devices. Sometimes, companies use these devices to track employees' use of e-mail and the Internet, and this use is legal. However, keystroke loggers can be used for malicious purposes, too, such as collecting the credit card numbers that users enter while shopping online. Some antivirus and antispyware programs guard against software keystroke loggers, and utilities are available to install as additional protection.

Sniffing is capturing and recording network traffic. Although it can be done for legitimate reasons, such as monitoring network performance, hackers often use it to intercept information.

Spoofing is an attempt to gain access to a network by posing as an authorized user in order to find sensitive information, such as passwords and credit card information. Spoofing is also when an illegitimate program poses as a legitimate one.

Computer fraud is the unauthorized use of computer data for personal gain, such as transferring money from another's account or charging purchases to someone else's account. Many of the technologies discussed previously can be used for committing computer crimes. In addition, social networking sites, such as Facebook and Snapchat, have been used for committing computer crimes.

Another computer crime is sabotage, which involves destroying or disrupting computer services. Computer criminals change, delete, hide, or use computer files for personal gain. Usually called hackers, many of them break into computer systems for personal satisfaction, but others seek financial gain. Surprisingly, most computer crimes are committed by company insiders, which makes protecting information resources even more difficult.

CHECKLIST 2: PUTTING TOGETHER THE BASIC SAFEGUARDS

Computer and network security has become critical for most organizations, especially in recent years, with hackers becoming more numerous and more adept at stealing and altering private information. To break into computers and networks, hackers use a variety of tools, such as sniffers, password crackers, rootkits, and many others; all can be found free on the Web. Also, journals such as *Phrack* and *2600: The Hacker Quarterly* offer hackers informative tips. A rootkit is a software application that hides its presence on the computer, which makes it nearly undetectable by common anti-malware software.

A comprehensive security system protects an organization's resources, including information, computer, and network equipment. The information an organization needs to protect can take many forms: e-mails, invoices transferred via electronic data interchange (EDI), new product designs, marketing campaigns, and financial statements. Security threats involve more than stealing data; they include such actions as sharing passwords with coworkers, leaving a computer unattended while logged on to the network, or even spilling coffee on a keyboard. A comprehensive security system includes hardware, software, procedures, and personnel that collectively protect information resources and keep intruders and hackers at bay. There are three important aspects of computer and network security: confidentiality, integrity, and availability, collectively referred to as the CIA triangle (Saunders, 1996).

Confidentiality means that a system must not allow the disclosing of information by anyone who is not authorized to access it. In highly secure government agencies, such as the Department of Defense, the CIA, and the IRS, confidentiality ensures that the public cannot access private information. In businesses, confidentiality ensures that private information, such as payroll and personnel data, is protected from competitors and other organizations. In the e-commerce world, confidentiality ensures that customers' data cannot be used for malicious or illegal purposes.

Integrity refers to the accuracy of information resources within an organization. In other words, the security system must not allow data to be corrupted or allow unauthorized changes to a corporate database. In financial transactions, integrity is probably the most important aspect of a security system, because incorrect or corrupted data can have a huge impact. For example, imagine a hacker breaking into a financial network and changing a customer's balance from $10,000 to $1,000—a small change, but one with a serious consequence. Database administrators and Webmasters are essential in this aspect of security. In addition, part of ensuring integrity is identifying authorized users and granting them access privileges.

Availability means that computers and networks are operating and authorized users can access the information they need. It also means a quick recovery in the event of a system failure or disaster. In many cases, availability is the most important aspect for authorized users. If a system is not accessible to users, the confidentiality and integrity aspects cannot be assessed.

The Committee on National Security Systems (CNSS) has proposed another model, called the McCumber cube. John McCumber created this framework for evaluating information security. Represented as a three-dimensional cube, it defines nine characteristics of information security (McCumber, 2004). The McCumber cube is more specific than the CIA triangle and helps designers of security systems consider many crucial issues for improving the effectiveness of security measures. Note that this model includes the different states in which information can exist in a system: transaction, storage, and processing.

In addition, a comprehensive security system must provide three levels of security:

- *Level 1*—Front-end servers, those available to both internal and external users, must be protected against unauthorized access. Typically, these systems are e-mail and Web servers.
- *Level 2*—Back-end systems (such as users' workstations and internal database servers) must be protected to ensure confidentiality, accuracy, and integrity of data.
- *Level 3*—The corporate network must be protected against intrusion, denial-of-service attacks, and unauthorized access.

When planning a comprehensive security system, the first step is designing fault-tolerant systems, which use a combination of hardware and software for improving reliability—a way of ensuring availability in case of a system failure. Commonly used methods include the following:

- Uninterruptible power supply (UPS)—This backup power unit continues to provide electrical power in the event of blackouts and other power interruptions and is most often used to protect servers. It performs two crucial tasks: It serves as a power source to continue running the server (usually for a short period), and it safely shuts down the server. More sophisticated UPS units can prevent users from accessing the server and send an alert to the network administrator.
- Redundant array of independent disks (RAID)—A RAID system is a collection of disk drives used to store data in multiple places. RAID systems also store a value called a *checksum*, used to verify that data has been stored or transmitted without error. If a drive in the RAID system fails, data stored on it can be reconstructed from data stored on the remaining drives. RAID systems vary in cost, performance, and reliability.
- Mirror disks—This method uses two disks containing the same data; if one fails, the other is available, allowing operations to continue. Mirror disks are usually a less expensive, level-1 RAID system and can be a suitable solution for small organizations.

CHECKLIST 3: IDENTIFYING SECURITY THREATS

Computer and network security are important to prevent loss of, or unauthorized access to, important information resources. Some threats can be controlled completely or partially, but some cannot be controlled. For example, you can control power fluctuations and blackouts to some degree by using surge suppressors and UPSs, but you cannot control whether natural disasters strike. You can, however, minimize the effects of a natural disaster by making sure fire suppression systems are up to code or by making structural changes to your organization's facility for earthquake protection—such as bolting the foundation.

Threats can also be categorized by whether they are unintentional (such as natural disasters, a user's accidental deletion of data, and structural failures) or intentional. Intentional threats include hacker attacks and attacks by disgruntled employees—such as spreading a virus on the company network. The following sections describe the most common intentional threats.

Intentional Threats

Intentional computer and network threats include:

- Viruses
- Worms
- Trojan programs
- Logic bombs
- Backdoors
- Blended threats (e.g., a worm launched by Trojan)
- Rootkits
- Denial-of-service attacks
- Social engineering

Viruses are the most well-known computer and network threats. (You have probably heard of the I Love You and Michelangelo viruses, for example.) They are a type of malware (short for *malicious software*), which is any program or file that is harmful to computers or networks.

A recent study estimates the annual cost of cybercrime to the global economy is $1 trillion and that malware is being introduced at a rate of 55,000 pieces per day (Cooney, 2011). However, estimating the dollar cost of viruses can be difficult. Many organizations are reluctant to report their losses because they do not want to publicize how vulnerable they are.

A virus consists of self-propagating program code that is triggered by a specified time or event. When the program or operating system containing the virus is used, the virus attaches itself to other files, and the cycle continues. The seriousness of viruses varies, ranging from playing a prank, such as displaying a funny (but usually annoying) image on the user's screen, to destroying programs and data.

Viruses can be transmitted through a network or through e-mail attachments. Some of the most dangerous ones come through bulletin boards or message boards because they can infect any system using the board. Experts believe that viruses infecting large servers, such as those used by air traffic control systems, pose the most risk to national security.

There are times that virus hoaxes are spread as well. These reports about viruses that turn out not to exist can cause panic and even prompt organizations to shut down their networks. In some ways, virus hoaxes can cause as much damage as real viruses.

The following list describes some of the indications that a computer might be infected by a virus:

- Some programs have suddenly increased in size.
- Files have been corrupted, or the user is unable to open some files.
- Hard disk free space is reduced drastically.
- The keyboard locks up, or the screen freezes.
- Available memory dips down more than usual.
- Disk access is slow.
- The computer takes longer than normal to start.
- There is unexpected disk activity, such as the disk drive light flashing even though the user is not trying to save or open a file.
- There are unfamiliar messages on the screen.

Installing and updating an antivirus program is the best measure against viruses. Widely used antivirus programs include McAfee Virus Scan (*www.mcafee.com/us*), Norton Antivirus (*www.norton.com*), and Trend Micro (*www.trendmicro.com*). You can even download free or low-cost programs on the Internet. Most computers now have antivirus software already installed, but you should check for the most current version of the antivirus software. New viruses are released constantly, so use automatic updating to make sure your computer's protection is current.

A worm travels from computer to computer in a network, but it does not usually erase data. Unlike a virus, it is an independent program that can spread itself without having to be attached to a host program. It might corrupt data, but it usually replicates itself into a full-blown version that eats up computing resources, eventually bringing a computer or network to a halt. Well-known worms include Code Red, Melissa, and Sasser. Conficker, a recent worm, has infected millions of Windows computers.

A Trojan program (named after the Trojan horse that the Greeks used to enter Troy during the Trojan War) contains code intended to disrupt a computer, network, or Web site, and it is usually hidden inside a popular program. Users run the popular program, unaware that the malicious program is also running in the background. Disgruntled programmers possibly seeking revenge with an organization have created many Trojan programs. These programs can erase data and wreak havoc on computers and networks, but they do not replicate themselves, as viruses and worms do.

A logic bomb is a type of Trojan program used to release a virus, worm, or other destructive code. Logic bombs are triggered at a certain time (sometimes the birthday of a famous person) or by a specific event, such as a user pressing the Enter key or running a certain program.

A backdoor (also called a *trapdoor*) is a programming routine built into a system by its designer or programmer. This routine enables the designer or programmer to bypass system security and sneak back into the system later to access programs or files. Usually, system users are not aware that a backdoor has been activated; a user logon or combination of keystrokes can be used to activate backdoors.

A blended threat is a security threat that combines the characteristics of computer viruses, worms, and other malicious codes with vulnerabilities found on public and private networks. Blended threats search for vulnerabilities in computer networks and then take advantage of these vulnerabilities by embedding malicious codes in the server's HTML files or by sending unauthorized e-mails from compromised servers with a worm attachment. They may launch a worm through a Trojan horse or launch a denial-of-service (DoS) attack at a targeted IP address. Their goal is not just to start and transmit an attack but to spread it. A multilayer security system, as discussed in this paper, can guard against blended threats.

A denial-of-service (DoS) attack floods a network or server with service requests to prevent legitimate users' access to the system. Think of it as 5,000 people surrounding a store and blocking customers who want to enter; the store is open, but it cannot provide service to legitimate customers. Typically, DoS attackers target Internet servers (usually Web, FTP, or mail servers), although any system connected to the Internet running TCP services is subject to attack.

In 2013, a DoS attack hit the online banking sites of dozens of U.S. and Canadian banks, including Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T, and HSBC (Kitten, 2013, Perlroth & Hardy, 2013). This particular assault was a distributed denial-of-service (DDoS) attack, which is when hundreds or thousands of computers work together to bombard a Web site with thousands of requests for information in a short period, causing it to grind to a halt. Because DDoS attacks come from multiple computers, they are difficult to trace.

Recently, emergency-service providers and many other organizations have been targeted by a new type of DOS attack, called a TDoS (telephony denial of service) attacks. These attacks use high volumes of automated calls to tie up a target phone system, halting incoming and outgoing calls. In some cases, the attacker demands a ransom. If the ransom is not paid, the TDoS begins, perhaps lasting for several hours (Samson, 2013).

In the context of security, social engineering means using "people skills"—such as being a good listener and assuming a friendly, unthreatening air—to trick others into revealing private information. This is an attack that takes advantage of the human element of security systems. Social engineers use the private information they have gathered to break into servers and networks and steal data, thus compromising the integrity of information resources. Social engineers use a variety of tools and techniques to gather private information, including publicly available sources of information—Google Maps, company Web sites, newsgroups, and blogs, for example.

In addition, two commonly used social-engineering techniques are called *dumpster diving* and *shoulder surfing*. Social engineers often search through dumpsters or trash cans looking for discarded material (such as phone lists and bank statements) that they can use to help break into a network. For example, a social engineer might look up the phone number of a receptionist he or she can call and pretend to be someone else in the organization. Shoulder surfing—that is, looking over someone's shoulder—is the easiest form of collecting information. Social engineers use this technique to observe an employee entering a password or a person entering a PIN at an ATM, for example.

In addition to these intentional threats, loss or theft of equipment and computer media is a serious problem, particularly when a computer or flash drive contains confidential data.

CHECKLIST 4: IDENTIFYING SECURITY MEASURES AND ENFORCEMENT

In addition to backing up data and storing it securely, organizations can take many other steps to guard against threats. Table 2 lists major security measures and enforcement.

TABLE 2
MAJOR SECURITY MEASURES AND ENFORCEMENT

Biometric security measures
Nonbiometric security measures (callback modems, firewalls, and intrusion detection systems)
Physical security measures (Cable shielding, Corner bolts, Electronic trackers, ID badges)
Access controls (terminal resource security and passwords)
Virtual private networks
Data encryption

Biometric security measures use a physiological element that is unique to a person and cannot be stolen, lost, copied, or passed on to others. The following list describes some biometric devices and measures:

- *Facial recognition*—Identify users by analyzing the unique shape, pattern, and positioning of facial features.
- *Fingerprints*—Scan users' fingerprints and verify them against prints stored in a database.
- *Hand geometry*—Compare the length of each finger, the translucence of fingertips, and the webbing between fingers against stored data to verify users' identities.
- *Iris analysis*—Use a video camera to capture an image of the user's iris, then use software to compare the data against stored templates.
- *Palm prints*—Use the palm's unique characteristics to identify users. A palm reader uses near-infrared light to capture a user's vein pattern, which is unique to each individual. This is compared to a database that contains existing patterns. This method is often used by law enforcement agencies.
- *Retinal scanning*—Scan the retina using a binocular eye camera, then check against data stored in a database.
- *Signature analysis*—Check the user's signature as well as deviations in pen pressure, speed, and length of time used to sign the name.
- *Vein analysis*—Analyze the pattern of veins in the wrist and back of the hand without making any direct contact with the veins.
- *Voice recognition*—Translate words into digital patterns, which are recorded and examined for tone and pitch. Using voice to verify user identity has one advantage over most other biometric measures: It can work over long distances via ordinary telephones. A well-designed voice-recognition security system can improve the security of financial transactions conducted over the phone.

Although biometric techniques are effective security measures, they might not be right for all organizations. Some drawbacks of biometrics are high cost, users' reluctance, and complex installation.

However, with improvements being made to address these drawbacks, biometrics can be a viable alternative to traditional security measures.

The three main nonbiometric security measures are callback modems, firewalls, and intrusion detection systems.

A callback modem verifies whether a user's access is valid by logging the user off (after he or she attempts to connect to the network) and then calling the user back at a predetermined number. This method is useful in organizations with many employees who work off-site and who need to connect to the network from remote locations.

A firewall is a combination of hardware and software that acts as a filter or barrier between a private network and external computers or networks, including the Internet. A network administrator defines rules for access, and all other data transmissions are blocked. An effective firewall should protect data going from the network as well as data coming into the network.

A firewall can examine data passing into or out of a private network and decide whether to allow the transmission based on users' IDs, the transmission's origin and destination, and the transmission's contents. Information being transmitted is stored in what's called a *packet*, and after examining a packet, a firewall can take one of the following actions:

- Reject the incoming packet.
- Send a warning to the network administrator.
- Send a message to the packet's sender that the attempt failed.
- Allow the packet to enter (or leave) the private network.

Although firewalls can do a lot to protect networks and computers, they do not offer complete security. Sophisticated hackers and computer criminals can circumvent almost any security measure. For example, some hackers use a technique called IP spoofing to trick firewalls into treating packets as coming from legitimate IP addresses. This technique is the equivalent of forgery. To provide comprehensive security for data resources, firewalls should be used along with other security measures. Other guidelines for improving a firewall's capabilities include the following:

- Identify what data must be secured, and conduct a risk analysis to assess the costs and benefits of a firewall.
- Compare a firewall's features with the organization's security needs. For example, if your organization uses e-mail and FTP frequently, make sure the application-filtering firewall you are considering can handle these network applications.
- Compare features of packet-filtering firewalls, application-filtering firewalls, and proxy servers to determine which of these types addresses your network's security needs the best.
- Examine the costs of firewalls, and remember that the most expensive firewall is not necessarily the best. Some inexpensive firewalls might be capable of handling everything your organization needs.
- Compare the firewall's security with its ease of use. Some firewalls emphasize accuracy and security rather than ease of use and functionality. Determine what is most important to your organization when considering the trade-offs.
- Check the vendor's reputation, technical support, and update policies before making a final decision.

As the demand for firewalls has increased, so has the number of vendors, and not all vendors are equal. Keep in mind that you might have to pay more for a product from a vendor with a good reputation that offers comprehensive technical support.

Firewalls protect against external access, but they leave networks unprotected from internal intrusions. An intrusion detection system (IDS) can protect against both external and internal access. It is usually placed in front of a firewall and can identify attack signatures, trace patterns, generate alarms for the network administrator, and cause routers to terminate connections with suspicious sources. These systems can also prevent DoS attacks. An IDS monitors network traffic and uses the "prevent, detect, and react" approach to security. Although it improves security, it requires a great deal of processing power and can affect network performance. It might also need additional configuration to prevent it from generating false positive alarms. The vendors listed in Table 3 offer comprehensive IDS products and services.

TABLE 3
IDS VENDORS

Vendor	**URL**
Enterasys Networks	*www.enterasys.com*
Cisco Systems	*www.cisco.com*
IBM Internet Security Systems	*www.iss.net*
Juniper Networks	*www.juniper.net/us/en*
Check Point Software Technologies	*www.checkpoint.com*

Physical security measures primarily control access to computers and networks, and they include devices for securing computers and peripherals from theft. Common physical security measures can include the following:

- *Cable shielding*—Braided layers around the conductor cable protect it from electromagnetic interference (EMI), which could corrupt data or data transmissions.
- *Corner bolts*—An inexpensive way to secure a computer to a desktop or counter, these often have locks as an additional protection against theft.
- *Electronic trackers*—These devices are secured to a computer at the power outlet. If the power cord is disconnected, a transmitter sends a message to an alarm that goes off or to a camera that records what happens.
- *Identification (ID) badges*—These are checked against a list of authorized personnel, which must be updated regularly to reflect changes in personnel.
- *Proximity-release door openers*—These are an effective way to control access to the computer room. A small radio transmitter is placed in authorized employees' ID badges, and when they come within a predetermined distance of the computer room's door, a radio signal sends a key number to the receiver, which unlocks the door.
- R*oom shielding*—A nonconductive material is sprayed in the computer room, which reduces the number of signals transmitted or confines the signals to the computer room.
- *Steel encasements*—These fit over the entire computer and can be locked.

With the increasing popularity of laptops, theft has become a major security risk. Laptops can store confidential data, so a variety of security measures should be used. For example, a cable lock on the laptop could be combined with a fingerprint scan to make sure only the laptop's owner can access files.

Access controls are designed to protect systems from unauthorized access in order to preserve data integrity. The following sections describe two widely used access controls: terminal resource security and passwords.

Terminal resource security is a software feature that erases the screen and signs the user off automatically after a specified length of inactivity. This method of access control prevents unauthorized users from using an unattended computer to access the network and data. Some programs also allow users to access data only during certain times, which reduces break-in attempts during off hours.

A password is a combination of numbers, characters, and symbols that is entered to allow access to a system. A password's length and complexity determines its vulnerability to discovery by unauthorized users. For example, *p@s$w0rD* is much harder to guess than *password*. The human element is one of the most notable weaknesses of password security, because users can forget passwords or give them to an unauthorized user (intentionally or unintentionally). To increase the effectiveness of passwords, follow these guidelines:

- Change passwords frequently.
- Passwords should be eight characters or longer.
- Passwords should be a combination of uppercase and lowercase letters, numbers, and special symbols, such as @ or $.
- Passwords should not be written down.
- Passwords should not be common names, such as the user's first or last name, obvious dates (such as birthdays or anniversaries), or words that can be found in a dictionary.
- Passwords should not be increased or decreased sequentially or follow a pattern (for example, 222ABC, 224ABC, 226ABC).
- Before employees are terminated, make sure their passwords have been deleted.

A virtual private network (VPN) provides a secure "tunnel" through the Internet for transmitting messages and data via a private network. It is often used so remote users have a secure connection to the organization's network. VPNs can also be used to provide security for extranets, which are networks set up between an organization and an external entity, such as a supplier. Data is encrypted before it is sent through the tunnel with a protocol, such as Layer Two Tunneling Protocol (L2TP) or Internet Protocol Security (IPSec). The cost of setting up a VPN is usually low, but transmission speeds can be slow, and lack of standardization can be a problem.

Typically, an organization leases the media used for a VPN on an as-needed basis, and network traffic can be sent over the combination of a public network (usually the Internet) and a private network. VPNs are an alternative to private leased lines or dedicated Integrated Services Digital Network (ISDN) lines and T1 lines.

Data encryption transforms data, called *plaintext* or *cleartext*, into a scrambled form called *ciphertext* that cannot be read by others. The rules for encryption, known as the encryption algorithm, determine how simple or complex the transformation process should be. The receiver then unscrambles the data by using a decryption key.

There are many different encryption algorithms used. One of the oldest encryption algorithms, used by Julius Caesar, is a simple substitution algorithm in which each letter in the original message is replaced by the letter three positions farther in the alphabet. For example, the word *top* is transmitted as *wrs*.

A commonly used encryption protocol is Secure Sockets layer (SSL)**,** which manages transmission security on the Internet. Next time you purchase an item online, notice that the *http* in the browser address bar changes to *https*. The *https* indicates a Secure HTTP connection over SSL. You might also see a padlock icon in the status bar at the bottom to indicate that your information has been encrypted and hackers cannot intercept it. A more recent cryptographic protocol is Transport Layer Security (TLS)**,** which ensures data security and integrity over public networks, such as the Internet. Similar to SSL, TLS encrypts the network segment used for performing transactions. In addition to being encryption protocols, SSL and TLS have authentication functions.

As mentioned, encryption algorithms use a key to encrypt and decrypt data. The key's size varies from 32 bits to 168 bits; the longer the key, the harder the encryption is to break. There are two main types of encryption: asymmetric (also called *public key encryption*) and symmetric, which will be explained next, but first you need to understand PKI. A PKI (public key infrastructure) enables users of a public network such as the Internet to securely and privately exchange data through the use of a pair of keys—a public one and a private one—that is obtained from a trusted authority and shared through that authority.

Asymmetric encryption uses two keys: a public key known to everyone and a private or secret key known only to the recipient. A message encrypted with a public key can be decrypted only with the same algorithm used by the public key and requires the recipient's private key, too. Anyone intercepting the message cannot decrypt it, because he or she does not have the private key.

This encryption usually works better for public networks, such as the Internet. Each company conducting transactions or sending messages gets a private key and a public key; a company keeps its private key and publishes its public key for others to use. One of the first public key algorithms, RSA (named after its creators—Rivest, Shamir, and Adleman), is still widely used today. The main drawback of asymmetric encryption is that it is slower and requires a large amount of processing power.

In symmetric encryption (also called *secret key encryption*), the same key is used to encrypt and decrypt the message. The sender and receiver must agree on the key and keep it secret. Advanced Encryption Standard (AES), a symmetric encryption algorithm with a 56-bit key, is the one used by the U.S. government. The problem with symmetric encryption is that sharing the key over the Internet is difficult.

Encryption can also be used to create digital signatures that authenticate senders' identities and verify that the message or data has not been altered. Digital signatures are particularly important in online financial transactions. They also provide nonrepudiation, discussed in the next section. Here is how they work: You encrypt a message with your private key and use an algorithm that hashes the message and creates a message digest. The message digest cannot be converted back to the original message, so anyone intercepting the message cannot read it. Then you use your private key to encrypt the message digest, and this encrypted piece is called the *digital signature*. You then send the encrypted message and digital signature. The recipient has your public key and uses it to decrypt the message, and then uses the same algorithm that you did to hash the message and create another version of the message digest. Next, the recipient uses your public key to decrypt your digital signature and get the message digest you sent. The recipient then compares the two message digests. If they match, the message was not tampered with and is the same as the one you sent.

CHECKLIST 5: UNDERSTANDING THE SERVICES OF COMPUTER EMERGENCY RESPONSE TEAM

The Computer Emergency Response Team (CERT) was developed by the Defense Advanced Research Projects Agency (part of the Department of Defense) in response to the 1988 Morris worm attack, which disabled 10 percent of the computers connected to the Internet. Many organizations now follow the CERT model to form teams that can handle network intrusions and attacks quickly and effectively. Currently, CERT focuses on security breaches and DoS attacks and offers guidelines on handling and preventing these incidents. CERT also conducts a public awareness campaign and researches Internet security vulnerabilities and ways to improve security systems. Network administrators and e-commerce site managers should check the CERT Coordination Center for updates on protecting network and information resources.

In addition, the Office of Cyber Security at the Department of Energy offers a security service: Cyber Incident Response Capability (CIRC), which you can learn more about at *http://energy.gov/cio/office-chief-information-officer/services/incident-management*. CIRC's main function is to provide information on security incidents, including information systems' vulnerabilities, viruses, and malicious programs. CIRC also provides awareness training, analysis of threats and vulnerabilities, and other services.

CHECKLIST 6: PREPARING A COMPREHENSIVE SECURITY SYSTEM

An organization's employees are an essential part of the success of any security system, so training employees about security awareness and security measures is important. Some organizations use a classroom setting for training, and others conduct it over the organization's intranet. Tests and certificates should be given to participants at the end of training sessions. In addition, making sure management supports security training is important to help promote security awareness throughout the organization.

Organizations should understand the principles of the Sarbanes-Oxley Act of 2002 and conduct a basic risk analysis before establishing a security program (Unknown, 2002). This analysis often makes use of financial and budgeting techniques, such as return on investment (ROI), to determine which resources are most important and should have the strongest protection. This information can also help organizations weigh the cost of a security system.

The following steps should be considered when developing a comprehensive security plan (Bidgoli, 2008 & Bidgoli, 2017):

1. Set up a security committee with representatives from all departments as well as upper management. The committee's responsibilities include the following:
    - Developing clear, detailed security policy and procedures
    - Providing security training and security awareness for key decision makers and computer users
    - Periodically assessing the security policy's effectiveness
    - Developing an audit procedure for system access and use
    - Overseeing enforcement of the security policy
    - Designing an audit trail procedure for incoming and outgoing data
2. Post the security policy in a visible place, or post copies next to all workstations.
3. Raise employees' awareness of security problems.
4. Revoke terminated employees' passwords and ID badges immediately to prevent attempts at retaliation.
5. Keep sensitive data, software, and printouts locked in secure locations.
6. Exit programs and systems promptly, and never leave logged-on workstations unattended.
7. Limit computer access to authorized personnel only.
8. Compare communication logs with communication billing periodically. The log should list all outgoing calls with users' name, call destination, and time of call. Investigate any billing discrepancies.
9. Install antivirus programs, and make sure they are updated automatically.
10. Install only licensed software purchased from reputable vendors.
11. Make sure fire protection systems and alarms are up to date, and test them regularly.
12. Check environmental factors, such as temperature and humidity levels.
13. Use physical security measures, such as corner bolts on workstations, ID badges, and door locks.
14. Install firewalls and intrusion detection systems. If necessary, consider biometric security measures.

These steps should be used as a guideline. Not every organization needs to follow every step; however, some might need to include even more to fit their needs.

CHECKLIST 7: THE BUSINESS CONTINUITY PLANNING

To lessen the effects of a natural disaster or a network attack or intrusion, planning the recovery is important. This should include business continuity planning**,** which outlines procedures for keeping an organization operational. A disaster recovery plan lists the tasks that must be performed to restore damaged data and equipment as well as steps to prepare for disaster, such as the following:

- Back up all files.
- Periodically review security and fire standards for computer facilities.
- Periodically review information from CERT and other security agencies.
- Make sure staff members have been trained and are aware of the consequences of possible disasters and steps to reduce the effects of disasters.
- Test the disaster recovery plan with trial data.
- Identify vendors of all software and hardware used in the organization, and make sure their mailing addresses, phone numbers, and Web site addresses are up to date.

- Document all changes made to hardware and software.
- Get a comprehensive insurance policy for computers and network facilities. Periodically review the policy to make sure coverage is adequate and up to date.
- Set up alternative sites to use in case of a disaster. Cold sites have the right environment for computer equipment (such as air conditioning and humidity controls), but no equipment is stored in them. Hot sites, on the other hand, have all the needed equipment and are ready to go.
- Investigate using a collocation facility, which is rented from a third party and usually contains telecommunication equipment.
- Check sprinkler systems, fire extinguishers, and halon gas systems.
- Keep backups in off-site storage, periodically test data recovery procedures, and keep a detailed record of machine-specific information, such as model and serial number. Backup facilities can be shared to reduce costs.
- Keep a copy of the disaster recovery plan off site.
- Go through a mock disaster to assess response time and recovery procedures.

If disaster strikes, organizations should follow these steps to resume normal operations as soon as possible:

1. Put together a management crisis team to oversee the recovery plan.
2. Contact the insurance company.
3. Restore phone lines and other communication systems.
4. Notify all affected people, including customers, suppliers, and employees.
5. Set up a help desk to assist affected people.
6. Notify the affected people that recovery is underway.
7. Document all actions taken to regain normality so you know what worked and what did not work; revise the disaster recovery plan, if needed.

CONCLUSION

This paper examined seven recent real life cases related to computer and network security breaches, vulnerabilities, and successful security enforcements. The experiences and insights gained from these cases provided a background and guidelines for the proposed seven checklists for managers to consider when designing a security system. A number of lessons were learned from these cases that have been integrated into the proposed seven checklists. The checklists included (1) understanding the landscape of computer and network security, (2) putting together the basic safeguards, (3) identifying security threats, (4) identifying security measures and enforcement, (5) understanding the services of computer emergency response team, (6) preparing a comprehensive security system, and (7) the business continuity planning. If these steps are followed they should increase the chances of success in designing and implementing a security system and keeping the hackers and computer criminals at bay.

REFERENCES

Anderson, H. (2010). Case Study: The Motivation for Biometrics. HealthCareInfoSecurity.com. Accessed 6 October 2016 @ www.healthcareinfosecurity.com/articles.php?art_id=2686.

Bidgoli, H. (2017). MIS7. Mason, OH: Cengage Learning.

Bidgoli, H. ed. (2008). Global Perspectives in Information Security: Legal, Social and International Issues. Hoboken, NJ: John Wiley.

Bueb, F. & P. Fife. (2006). Line of Defense: Simple, Complex Security Measures Help Prevent Lost and Stolen Laptops. California Society of Certified Public Accountant and Gale Group. Accessed 6 October 2016@

www.thefreelibrary.com/Line+of+defense:+simple,+complex+security+measures+help+prevent+lost...-a0155477162.

Cooney, M. (2011). U.S. Needs to Be On Guard for a Big Cyberattack. Computerworld. Accessed 6 October 2016 @ www.computerworld.com/s/article/9220018/U.S._needs_to_be_on_guard_for_a_big_cyberattack.

Corbin, K. (2013). Cyber Crime Costs U.S. Economy $100 billion and 500,000 Jobs. InfoWorld. Accessed 6 October 2016@ www.infoworld.com/d/security/cyber-crime-costs-us-economy-100-billion-and-500000-jobs-223352?source=IFWNLE_nlt_sec_2013-07-25.

Elgin, B., Riley, M., & Dune, L. (2014). Home Depot Hacked After Months of Security Warnings. Bloomberg Businessweek. Accessed 6 October 2016 @http://www.businessweek.com/articles/2014-09-18/home-depot-hacked-wide-open.

Kitten, T. (2013). DDoS Attacks on Banks: No Break in Sight. BankInfoSecurity.com. Accessed 6 October 2016 @ www.bankinfosecurity.com/ddos-attacks-on-banks-no-break-in-sight-a-5708/op-1.

Kuchera, B. (2011). Sony Admits Utter PSN Failure: Your Personal Data Has Been Stolen. arstechnica.com. Accessed 6 October 2016 @ http://arstechnica.com/gaming/2011/04/sony-admits-utter-psn-failure-your-personal-data-has-been-stolen/.

Lederman, J. (2012). IRS Missing Billions in ID Theft. Associated Press. Accessed 6 October 2016 @ http://news.yahoo.com/irs-missing-billions-id-theft-164707999.html.

McCumber, J. (2004). Assessing and Managing Security Risk in IT Systems. Boca Raton, FL: Auerbach.

Perlroth, N. & Hardy Q. (2013). Bank Hacking Was the Work of Iranians, Officials Say. New York Times. Accessed 6 October 2016@ www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0.

Samson, T. (2013). Cyber Criminals Tying Up Emergency Phone Lines Through TDoS Attacks. InfoWorld. Accessed 6 October 2016@ www.infoworld.com/t/cyber-crime/cyber-criminals-tying-emergency-phone-lines-through-tdos-attacks-215585?source=IFWNLE_nlt_sec_2013-04-02.

Saunders, S. (1996). Putting a Lock on Corporate Data. Data Communications. 78–80.

Schiesel, S. (2011). PlayStation Security Breach a Test of Consumers' Trust. New York Times. Accessed 6 October 2016@ www.nytimes.com/2011/04/28/arts/video-games/sony-playstation-security-flaw-tests-consumer-trust.html.

Stuart, K. (2011). PlayStation 3 Hack—How It Happened and What It Means. Theguardian.com. Accessed 6 October 2016@ www.guardian.co.uk/technology/gamesblog/2011/jan/07/playstation-3-hack-ps3.

Talbot, D. (2012). Computer Viruses Are 'Rampant' on Medical Devices in Hospitals. MIT Technology Review. Accessed 6 October 2016@ www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals.

Team, T. (2014). Home Depot: Could The Impact Of The Data Breach Be Significant? Forbes. Accessed 6 October 2016 @ http://www.forbes.com/sites/greatspeculations/2014/09/24/home-depot-could-the-impact-of-the-data-breach-be-significant/#74700ace237f.

Unknown. (2002). The Sarbanes-Oxley Act of 2002. Accessed 6 October 2016 @ www.soxlaw.com.

Unknown. (2009). Prevent Data Theft Using Removable Devices. Get Safe Online. Accessed 6 October 2016 @ www.getsafeonline.org/nqcontent.cfm?a_id=1103.

Unknown. (2014). Home Depot Data Breach Worse Than Initially Reported. VOANews.com. Accessed 6 October 2016 @ http://www.voanews.com/content/home-depot-data-breach-worse-than-initially-reported/2511548.html.

Vijayan, J. (2011). 90 Percent of Companies Say They've Been Hacked. Computerworld. Accessed 6 October 2016 @ www.infoworld.com/d/security/90-percent-companies-say-theyve-been-hacked-118.

Weaver, C. (2013). Patients Put at Risk by Computer Viruses. Wall Street Journal. Accessed 6 October 2016@ http://online.wsj.com/news/articles/SB10001424127887324188604578543162744943762?mod=djem_jiewr_IT_domainid.