2013

Online Privacy, Vulnerabilities, and Threats: A Manager's Perspective

Hy Sockel
DIKW Management Group

Louis K. Falk
The University of Texas Rio Grande Valley

Recommended Citation

Sockel, Hy and Louis K. Falk. "Online Privacy, Vulnerabilities, and Threats: A Manager's Perspective." Cyber Crime: Concepts, Methodologies, Tools and Applications, edited by Information Resources Management Association, IGI Global, 2012, pp. 101-123. https://doi.org/10.4018/978-1-61350-323-2.ch108

Chapter 1.8
Online Privacy, Vulnerabilities, and Threats:
A Manager's Perspective

Hy Sockel
DIKW Management Group, USA

Louis K. Falk
University of Texas at Brownsville, USA

ABSTRACT

There are many potential threats that come with conducting business in an online environment. Management must find a way to neutralize or at least reduce these threats if the organization is going to maintain viability. This chapter is designed to give managers an understanding, as well as the vocabulary needed to have a working knowledge of online privacy, vulnerabilities, and threats. The chapter also highlights techniques that are commonly used to impede attacks and protect the privacy of the organization, its customers, and employees. With the advancements in computing technology, any and all conceivable steps should be taken to protect an organization's data from outside and inside threats.

INTRODUCTION

The Internet provides organizations unparalleled opportunities to perform research and conduct business beyond their physical borders. It has proven to be a vital medium for worldwide commerce. Even small organizations now rely on Internet connectivity to communicate with their customers, suppliers, and partners. Today, employees routinely work from areas beyond their office's physical area. They regularly transport sensitive information on notebook computers, personal digital assistants (PDAs), smartphones, and a variety of storage media: thumb drives, CDs, DVDs, and even on floppies. It is not uncommon for employees to work offsite, at home, or out of a hotel room. Outside the office, they often use less

DOI: 10.4018/978-1-61350-323-2.ch1.8

than secure Internet connections—dial-up, cable, Internet cafés, libraries, and wireless.

Organizations often employ portals to share information with their stakeholders, however; these portals are not always secure from would be attackers. In order to protect the organization from vicious and malicious attacks, management needs to understand what they are up against. Even if the organization does not conduct any business on the Internet, they are still not out of harms way. Viruses, Trojans, and spyware can come from multiple sources; floppy discs, CDs, thumb drives, and even from mobile phones. To complicate the matter even more, the information technology (IT) environment at many organizations has become obscure—partially due to new regulations and industry standards. The standard has changed, it is no longer enough to be secure and protect the businesses assets, organizations need to be able demonstrate that they are compliant and that security is an ongoing concern; failure to do so could leave them facing stiff penalties (Forescout, 2007).

The purpose of this chapter is to address some of the potential threats that come with conducting business in an online environment. The chapter highlights the relationship between privacy and vulnerability and threats. It delves into techniques that are commonly used to thwart attacks and protect individuals' privacy. In the age of unrest and terrorism, privacy has grown even more important, as freedoms are compromised for security.

The news is loaded with stories about security breaches. For example:

In May of 2007, the news of the TJ Maxx security breach shook up the banking and retail industry. At first it was estimated that hackers had downloaded at least 45.7 million credit- and debit-card numbers; however, court filings indicated that number was closer to 96 million. Estimates for damage range from $216 million to $4.5 billion. The breach was blamed on extensive cyber thief activity within TJ Maxx's network from 2003 through June 2004 and then again from mid-May 2006 through mid-December 2006 (Schuman, 2007). However, others blame the breach on weak wireless security—Ou (2007) revealed that the "retailer's wireless network had less security than many people have on their home networks."

Another example is:

In April 5, 2002 hackers exploited vulnerabilities in a server holding a database of personnel information on California's 265,000 state employees. The state responded, and the world listened. California is one of the largest economies in the world, bigger than most countries. The attack included in its victims, the then Governor Grey Davis and 120 state legislators. The breach compromised names, social security numbers, and payroll information. In response, the state legislature enacted a security breach notification law Senate Bill (SB) 1386.

To put this in perspective, if online privacy is described in terms of a risk "triangle," the three corners are vulnerabilities, threats, and actions. Where actions represent anything the organization can (and should) do to mitigate attacks. Applications, like ships, are not designed and built to sit in a safe harbor, they were meant to be used in churning chaotic waters. It is important to understand threats and vulnerabilities enough to have a good idea to of what to expect, so that strategies and tools can be put in place to mitigate the consequences (Bumgarner & Borg, 2007).

VULNERABILITY

Software vulnerabilities are not going away, in fact they are increasing. According to the Coordination Center at Carnegie Mellon University (CERT, 2007) there was an average of over 10 vulnerabilities discovered every day in 2003 (3,784 in total). This number has jumped to over 5500 in the first nine months of 2007.

Software flaws have become the vulnerabilities of choice for attackers. Flaws cut across the entire enterprise application stack—including Web and application servers, databases, and operating systems. Dr. (Rear Admiral) Grace Hopper (1906-1992), a highly respected and accomplished computer scientist indicated that all software has problems and that it is impossible to have a "perfect" system. She articulated this point using the following example...if the probability of an individual module having an error in the code was just one in a hundred (1%), and that the system had several hundred modules; then the net probability of an error for that system would be 100%. This observation is particularly relevant in that most commercial software developers use complex computer software program development toolkits (SDK) to improve their productivity and effectiveness.

Qualsys (2006), a security vendor, studied over 40 months of data scans (September 8, 2002 to January 31, 2006) and identified nearly 1600 unique critical vulnerabilities from a total infestation of more than 45 million vulnerabilities. The data scan showed more than 60% of critical vulnerabilities were in client applications such as Web browsers, backup software, media players, antivirus, and flash.

The Third Brigade found that vulnerabilities generally fall into one of the following categories (Aberdeen Group, 2005):

- Vulnerabilities caused by incorrect configured systems
- Failure to turn off factory defaults, guest accounts, outdated software
- Failure to maintain anti-virus and spam updates
- Failure to change default values leaving holes
- Well-know bugs in system utilities
- Poor or ignorant policy decisions
- Unapplied vendor security systems patch; Aberdeen states that 95% of attacks are against known vulnerabilities for which patches are available.

Vulnerabilities do not have to be broken program code; Norman (1983) indicated that errors in system designs, which provoke erroneous entries by users can also be considered as vulnerabilities that can be intentionally exploited by attackers.

Individually and collectively vulnerabilities can create major risks for organizations. Weak policies and protection can result in the release of personal private information (PII). The release of PII is not the only the problem. Another issue is that hackers can obtain important data and modify it. Suddenly, there are additional names on the preferred lists, payroll, and accounts payable; and outsiders could be given authority or consideration that they are not entitled to. An organization's strategic plans could be compromised. Additionally, the release of PII can weaken the public's confidence in the organization, subject the organization to litigation, large fines/reparation costs, and to rigorous investigations, as well as oversight.

THREATS

Threats are not the same as vulnerabilities; threats are things that take can advantage of vulnerabilities. Security threats, broadly, can directly or indirectly lead to system vulnerabilities (Im & Baskerville, 2005). An analogy might be an army fort surrounded by the enemy where someone accidently left the fort's front gate wide open. The open gate is a "vulnerability" and the threat is the "opposing force." Translating this analogy to data-information, the vulnerability would be a "poorly protected" system, and the threat is the criminal hacker community. In this case, poorly protected could be construed to be any of a number of things including absolutely no protection, software that is not updated, inappropriately defined security rules, and weak passwords.

In general, it is important to ensure that sensitive information and systems are protected from all threats, both internal and external. Typically, this is done by separating the systems from the networks. However, this is not always possible; with the advent of e-business there is a need for organizations to share information.

For example: an organization gives its partners (A) and (B) permission to look at its online schedule (instead of calling a clerk as they had in the past). This can create the opportunity for partner A to look at (or modify) partner B's data. If the data is of a personal type, say medical, several laws could easily be violated. If it is indicated in the privacy policy that data/information is not shared, the individual whose data is released may have rightful cause to institute litigation.

Clearswift, a leading provider of content security products, has categorized five major message traffic threat types as: asset theft, disruption, repudiation, content abuse, and denial of service.

Asset theft happens via spoofing or social engineering; when an outsider pretends to be an authorized user and requests information not available to an unauthorized user. However, more commonly, it is the sending of sensitive information inadvertently or by disaffected "insiders."

Disruption is a common threat, which includes anything that keep users (and services, i.e., e-mail, fax ...) from doing what they are suppose to do. Other workplace disruption can include dissemination of personal, pornographic, or "non-business" information.

Repudiation (denial) is concerned with either party (sender or receiver) being able to declare that an event did not happen. Techniques like Diffie-Hellman Key Exchange permit digital signatures, which provide assurance that the message was actually sent and/or received by the intended parties. Digital signatures are accepted as evidence in a court of law. This is critical because oftentimes parties involved in transactions do not know each other.

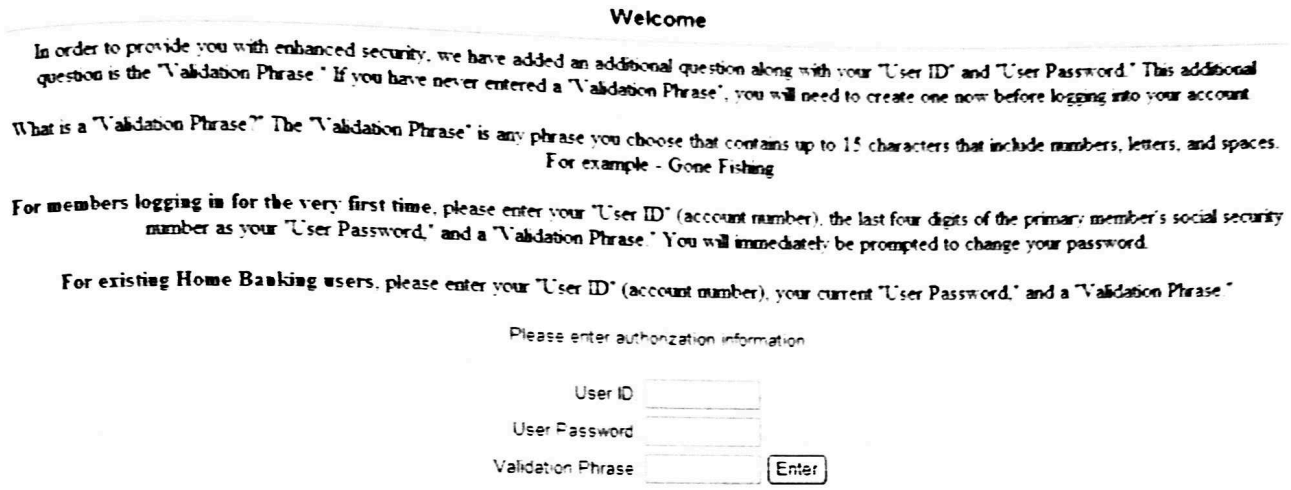
Content abuse is similar in scope of repudiation, but is focused on the content of the message and not whether it was sent or received. It deals with issues between the sending and receiving parties over what was sent and what was received.

Denial of service (DoS) and **distributed DoS (DDoS)** results when a party is bombarded with more messages than it can handle, causing the system to use all its resources to handle non-legitimate traffic. This can happen by bombarding the victim's machine with thousands to millions of messages so that it cannot respond to legitimate requests or responds so slowly that it is effectively unavailable. DOS attacks are considered violations of the Internet Architecture Board's (IAB) Internet proper use policy concerning Internet ethics passed January 1989 (often referred to as RFC 1087; see http://tools.ietf.org/html/rfc1087). In the U.S. (and many countries), DoS is a serious federal crime under the National Information Infrastructure Protection Act of 1996 with penalties that can include fines and imprisonment.

SOCIAL ENGINEERING

It is not always a technical issue—a perpetrator can use chicanery and/or persuasion to manipulate unsuspecting people into either revealing sensitive information (such as logon and password) or compromise perimeter defenses by installing inappropriate software or portable storage devices (that are seeded with malware) on computer networks. For example, an approach of phishing is to ask a user to fill out a simple fake online form. The form itself asks almost no personal information; instead, it pre-fills the form with some of the info that the sender already knows about the victim. It asks for a person to make up a login name and a password. The criminal hackers know that most people suffer from password overload and tend to reuse the same passwords over and over again. Figure 1 is a representative sample (taken off the net November 4, 2007):

Figure 1. Ploy to capture personal information



RISK

Risk is involved in everything, every process, and every system. Operational risk is often defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Risk is one of those things that no one can escape and is hard to define. In general, risk is the probability of a negative outcome because some form of threat will be able to exploit vulnerabilities against an asset. Many define the value of a risk attack as: the value of an asset times the probability of a threat times the probability of an undiscovered vulnerability times some "impact factor (representing reparations) times the possibility of the event. While the formula (see Equation 1—risk dollar value) is straight forward, coming up with the values and probabilities is not. The important issue is not the devised dollar value, but what does the asset really mean to the organization and how are they going to use it?

Equation 1—risk dollar value

Risk $ = Asset value * Threat * Vulnerability * Impact * Likelihood * Uncertainty

Elimination of risk is categorically impossible; the best that can be hoped for to get it under control. Even if it were possible, the cost and scalability issues of risk avoidance have to be weighed against the cost of the probable losses resulting from having accepted rather than having eliminated risk (Pai & Basu, 2007).

Qualys, Inc. (2006) analyzed a global data pool of more than 40 million IP scans with their product QualysGuard. Data analysis revealed the six axioms of vulnerabilities. These axioms are important because they help management understand the nature of possible attacks and why and how their data could be at risk of being compromised. Qualys Inc. (2006) believes that "Understanding the behavior of vulnerabilities is essential to setting effective security strategy and proactively implement security solutions."

The axioms of Qualys's Research:

1. **Half-life:** Is the average time it takes an organization to patch (or apply a fix) to half of the most dangerous vulnerabilities. The 2006 findings indicate a decrease in the half life to 19 days (down from 30 in 2003) on external systems. They found that the exposure of unpatched systems continues

during the significantly long period of half-life dissipation and increases as the severity decreases.

2. **Prevalence:** Prevalence is the degree to which the vulnerability poses a significant threat. They found that half of the most prevalent critical vulnerabilities are replaced by new vulnerabilities each year. This means there is ongoing change to the most important threats to our networks and systems.
3. **Persistence:** The life spans of some vulnerabilities are unlimited as soon as the current infection is addressed, a variant may appear. In one day Sophos found over 300 variants of the "Stranton" virus. The risk of re-infection can happen during deployment of machines with a faulty unpatched operating system
4. **Focus:** The 2006 study data revealed that 90% of vulnerability exposure is caused by 10% of critical vulnerabilities.
5. **Exposure:** The time-to-exploit cycle is shrinking faster than the remediation cycle. Eighty percent of critical vulnerability exploits are available within the first half-life after their appearance. Since the duration of vulnerability announcement-to-exploit-availability is dramatically shrinking, organizations must eliminate vulnerabilities faster.
6. **Exploitation:** Nearly all damage from automated attacks is during the first 15 days of the outbreak. Automated attacks pose a special hazard to network security because they inflict damage swiftly with little time for reaction.

Cannon and Kessler (2007) believe that the rapid increase in breaches and incidents can be directly related to technology. They indicate that the increase in 1) computer processing power and data storage capacity and in 2) higher data transmission bandwidth have acerbated the problem. This in conjunction with the massive connectivity of information systems afforded by the Internet and World Wide Web allow for the mass collection and misuse of sensitive personal data.

ELECTRONIC RISK MANAGEMENT

There is a large group of people that believe that in the final analysis of security breaches, that most problems should not be blamed on hackers or malicious employees, instead the instances should be blamed on lack of common sense. To them, the vast majority of breaches can be classified under the title of carelessness. As in people not paying attention to what they are doing, such as putting a letter in the wrong envelope, adding a copy to an e-mail, or losing equipment or hardware, the real culprit is a lack of following procedures (Padilla, 2007).

However, regardless of how breaches are caused: by ignorance, carelessness, inside users, or criminal hackers, there are a lot of them. The Privacy Rights Clearinghouse (2007); indicates that more than 48 million records containing sensitive personal information have been involved in some form of a security breach in just January 2007 alone. Cannon and Kessler (2007) define "A data breach as the unauthorized access to and acquisition of data in any form or format containing sensitive information that compromises the security of confidentiality of such information and creates a reasonable risk of its misuse."

IDC indicates that strong corporate governance is the foundation of successful protection of corporate assets from a wide variety of threats (CNET, 2004). To that end, organizations need to establish, educate, and enforce their policies to effectively ensure the protection they need.

1. **Establish:** Establish clearly written policies and procedures for all employee communications. The rules must deal with acceptable and unacceptable behavior for the Internet, P2P (peer-to-peer), e-mail, IM (instant messaging), and blogging.

2. **Educate:** Educate and support written rules and policies with company wide training. The employees need to understand that the policy is a living document (it will mutate as new threats and issues arise) but compliance is mandatory. This can be a critical issue for an organization because misuse (whether deliberate or accidental) can result in the organization being held responsible by the legal principle of vicarious liability.
3. **Enforcement of written rules and policies Enforce policies:** With a combination of disciplinary action and software. If there is any doubt about employee willingness to adhere to the organization's usage and content rules, consider applying a technological solution to the people problem. Tools can help the installation of hardware, software, and/or appliances, and enforce established policies. The organization can block access to inappropriate sites and stay on top of employees' online activity. Failure to discipline employees for e-mail-related misconduct may encourage other employees to abuse the system and could create liability concerns for the organization. It is important to communicate the policies and to adhere to them. The American Management Association (2005) Electronic Monitoring & Surveillance Survey found that most companies monitor employee Web site usage (76%) and use filters to block access to inappropriate Web sites (65%). Slightly more than a quarter (26%) of responding organizations indicated they went further admonishing individuals, they terminated them for misuse of e-mail or the Internet.

The World Bank indicates that to reduce the e-security risk, day to day augmentation of e-security internal monitoring and processes are needed. They indicate that proper "Risk management is achieved through a comprehensive checklist per the cyber-risks that affect the network as a whole." They have refined a "technology risk checklist" based upon standards set by ISO 17799 (Glaessner, Kellermann, & McNevin, 2004).

MALWARE

The term malware (malicious software) is typically used as a catch-all to refer to a variety of forms of hostile, intrusive, or annoying software designed to infiltrate or interrupt services from a single computer, server, or computer network without the owner's informed consent. The term malware includes all types of trouble makers: such as: viruses, worms, kiddy scripts, Trojan horses, and macro (script–context) viruses. Malware seeks to exploit existing vulnerabilities on systems. Malware can utilize communication tools to spread and oftentimes it goes unnoticed. McAfee Avert Labs (Bernard, 2006) has recorded more than 225,000 unique computer/network threats. In just 10 months between January and November of 2006, they found 50,000 new threats. Google researchers (as part of the Ghost in the Browser research) warned that one in 10 Web pages is hiding embedded malware (Provos, McNamee, Mavrommatis, Wang, & Modadugu, 2007).

The term malware is often associated with the characteristic attributes of a virus; self-replicating, something that embeds itself into other programs, which in turn can infect other programs. The notion of a self-replicating program is not new, it dates back to John von Neumann's 1949 lectures. Neumann postulated the theory that a program could reproduce itself. Nearly 35 years later, November 1983, Professor Fred Cohen substantiated Neumann's work by creating and demonstrating the first computer virus in a computer security seminar. The name "virus" was provided by Len Adleman (the A in RSA); (http://en.wikipedia.org/wiki/Malware) and (http://all.net/books/virus/part5.html).

In 1989, John McAfee (of McAfee Avert Labs) defined a virus as a computer program created to

infect other programs with copies of itself. It is a program that has the ability to clone itself—so that it can multiply and constantly seek new host environments (McAfee & Haynes, 1989). Today, not all computer viruses *inject* themselves into their victims, nor is cloning considered mandatory. Researchers now make distinction between different malware varieties based on whether it is considered viral or non-viral malware (Cafarchio, 2004):

- Viral malware typically replicates rapidly and fairly indiscriminately, its behavior has a very visible impact. Viral infections might be used as part of distributed denial of service attack; worms like Code Red are able to spread worldwide in a matter of hours.
- Non-viral malicious software does not replicate. It is planted by hackers, or unknowingly downloaded by unsuspecting users, or foisted on systems as part of a software package to track the user's behavior and/or software usage. Non-viral malicious software is designed to be "inconspicuous and stealthy." These types of infections can go undetected for long periods of time.
- There are some virus types of malware that are design merely to harass the users and not to intentionally damage files or the operating systems. Malware like the Bearded Trojan are of this style. The Bearded Trojan displays a nude female and while it is potentially offensive or embarrassing, it often makes people realize that they are vulnerable and could have been infected with a virus that acts as a key logger, or a Web bot (Harley, Slade, & Gattiker, 2001).
- Another example of a non-viral virus is the "ANSI bombs;" thankfully, they are not common and they do not reproduce. An ANSI bomb is a sequence of characters that is meant to redefine key(s) on a keyboard. Thus, when the user presses a key the normally assigned characters for that key are not sent to the terminal or computer, but rather the redefined string. This string may contain any ASCII characters, including <RETURN> and multiple commands. A function key or even the space bar could be assigned a string that invokes a program to do something the user does not want to happen—copy, delete, or send material (Harley et al., 2001).

Adware/Spyware

A particular annoying and dangerous form of malware is adware/spyware. The terms are communally used as interchangeably. The goal of this technology is to gather information without the target person's knowledge or permission. This type of software is used to watch and record which Web sites and items on the Internet the user visits in hopes of developing a behavioral profile of the user that can later be exploited. The slight difference between the two terms is the intent of the software agent. Adware has an advertising aspect in the information it collects, while spyware tracks and record user behavior (in the traditional sense of the word "spy").

The problem with spyware is that users typically store all sorts of sensitive and personal information in their machines that should not be made public. Some information is protected by law, trade secrets, and financial data. The loss of personnel and customer information could wreak havoc for the organization. Additionally, the theft of stored information such as: bank account numbers, credit card numbers, social security numbers, and pictures could also devastate the individual.

Another thing that makes adware/spyware so pernicious is that *anti-viruses & firewalls* are not very effective against them. While a good anti-virus program (AV) is an absolutely essential for any machine, even those that do not connect to a network (especially if the machine accepts removable media), it is not enough. AV software

will not protect user machines from spyware. Viruses and spyware have different properties; because spyware does not propagate itself like other forms of malware, it is not likely to be detected by traditional AV methods.

BOTNETS

Vent Cerf, one of the "founding fathers" of the Internet, believes that one in four computers (approximately 150 million out of 600 million) connected to the Internet are compromised and likely to be unwilling members of a botnet (Fielding, 2007). These machines are often used as proxies for illegal activities like spamming and credit card fraud. Botnets have been a growing problem on the Internet since at least 2002. A bot (short for robot) is a software agent released onto a computer connected to the Internet. The bot can download malicious binary code that compromises the host turning it into a zombie machine. The collection of zombies is called a botnet. The servers hosting the bot binaries are usually located in countries unfriendly to the United States. The bots are transparent and run in the background. Bots can open a channel to a "bot controller" machine, which is the device used by the perpetrator (the bot herder) to issue commands to the bots (Baylor & Brown, 2006).

Bot herders typically use "bot controllers" to harvest user accounts via screen-capture, packet-sniffers, and key-logging techniques. They are routinely used for phishing (some estimate that over 70% Internet spam is due to them), click fraud, and malware.

Botnets can be used for attacking various Web sites by unleashing a barrage of requests against the site, so that the victim site spends more time processing the requests coming at it, than it does doing the job it was intended for. These attacks employ a technique known as distributed denial of service (DDoS) attack. The idea behind the DDoS is to flood a machine, server, or cluster faster than the server can respond to them. DDoS chew-up bandwidth and resources, effectively shutting down the attacked network. In this manner a large botnet can wield an amazing amount of power. If several large botnets are allowed to join together, they could literally threaten the national infrastructure of most countries. On April 27, 2007, a series of DDoS attacks crippled the financial and academic Web sites in Estonia (Kirk, 2007).

"Botnets are no longer just annoying, spam-pumping factories—they are big business for criminals. This shift has awakened large businesses, which historically have either looked the other way or been in denial about bots infiltrating their organizations" (Higgins, 2007). The Anatomy of a Typical Botnet Attack

- **Step 1:** The bot herder loads remote exploit code onto an "attack machine" that might be dedicated to this purpose or an already compromised machine. Many bots use file-sharing and remote process control (RPC) ports to spread.
- **Step 2:** Attack machines scan for unpatched (not current with updates) victim machines to launch attacks against.
- **Steps 3 & 4:** The victim machine is ordered to download files (binaries) from another server (frequently a compromised web or FTP server).
- **Step 5:** These binaries are run on the victim machine and convert it to a bot. The victim machine connects to the bot controller and "reports for duty."
- **Step 6:** The bot controller issues commands to the victim to down load new modules, steal account details, install spyware, attack other machines, and relay spam.
- **Step 7:** The bot herder controls all bots by issuing commands via the bot controller(s).

World's Biggest Botnets

Storm

There is a new threat, that of the super botnet. While few agree on the actual size of these botnets, they are huge: where the number of active members per 24 hour period (not just attached zombies) of the net can be in the hundreds of thousands. Currently, the largest of the new breed of botnets is "Storm." Storm broke away from the mode and uses a decentralized peer-to-peer (P2P) communication, instead of the traditional centralized Internet relay chat (IRC) model. The P2P makes it tough to track and tougher to kill; you cannot render it mute by disabling one or two central control machines.

Storm uses a complex combination of malware, which includes worms, rootkits, spam relays, and Trojans. It propagates via a worm or when a user visits an infected site or clicks on a link to one. It is very stealthy, it employs a balance "use" approach and a "fast-flux." The purpose of fast-flux is to circumvent the IP-based black list technique (see black list). It does this by rapidly rotating DNS records to prevent discovery (Higgins, 2007).

Rbot

Rbot is generally considered the second largest botnet. It employs an old-style communication structure using Internet relay chat. Because it uses an IRC approach, it does not scale very well and is unlikely to rival reach Storm's size. Rbot's underlying malware uses a backdoor to gain control of the infected machine, installing keyloggers, viruses, and even stealing files from the infected machine, as well as the usual spam and DDoS attacks. The real scary part is that Rbot [malware] is readily available to anyone who wants try to apply some kind of criminal activity in the bot arena (Higgins, 2007).

Whose Fault Is It?

The answer to this question depends on who you ask. It can easily be argued that it is the users' fault. If the user keeps their antivirus up-to-date and stays away from traditional types of sites that harbor malware (celebrity), the problem should be lessened. However, variants of viruses have been tracked in the hundreds per day; it is hard to keep current on protection when there is a whole industry working against you.

Since it may not necessarily be the user then it must be the developers, or the publisher for not creating a product that cannot be usurped. Unfortunately, there are highly skilled, university trained hackers that strive to develop the right code. After all, there is really only one reason for botnets: and that is to make money. Some people blame law enforcement or government for not quick prompt and decisive action. However, many of the bot herders are in countries in which the U.S. does not have jurisdiction. Politicians can pass laws, but never be in the position to have them enforced.

To that end, in 2007, Senators Orrin Hatch (R-Utah) and Joseph Biden, Jr. (D-Delaware) introduced the Cybercrime Act to update existing laws and close what they say are loopholes that online criminals can exploit. The bill takes a multifaceted attack. It lowers the threshold of evidence, it address not only damaged computers but also to individuals. It prohibits the creation of botnets that could be used in online attacks. It makes the threat of revealing (extortion) confidential information illegally obtained from computers a crime (Savage, 2007).

Botnets: FBI Operation Bot Roast

In the second week of November 2007, John Schiefer of Los Angeles, California agreed to plead guilty to felony charges for building and using a botnet as large as 250,000 nodes to steal personal identifying information (PII). The botnet was used to invade individuals' privacy by

intercepting electronic communications being sent over the Internet from the zombie computers to PayPal and other Web sites. Later, data mining techniques were used to garner PII such as username and passwords. With the usernames and passwords, they accessed bank accounts to make purchases without the consent of the true owners. The botnet was also used to defraud a Dutch advertising company. This was the first U.S. prosecution under the U.S. federal wiretap statute for conduct related to botnets (Wilson, 2007).

The FBI and Department of Justice in an anti-botnet sweep label as "Operation Bot Roast" has arrested three individuals for assembling botnets. They are charged with felonies. One of the three arrested is alleged to have used a large botnet network to send tens of millions of unsolicited e-mail messages. Another is charged with infecting more than 10,000 computers worldwide, including two Chicago hospitals. "The 'bots' caused the infected computers to, among other things, repeatedly freeze or reboot, causing significant delays in the provision of medical services." It took the hospitals more than 1,000 man-hours to clean up after the infections (Keizer, 2007; Albanesius, 2007).

The government is working in conjunction with industry partners to uncover these schemes. These include the CERT Coordination Center at Carnegie Mellon University as well as Microsoft, and The Botnet Task Force, (a low-profile organization initiated by Microsoft in 2004 that acts as a means of building awareness and providing training for law enforcement).

In the process, the FBI has identified more than 1 million hijacked personal computers. The majority of victims are not aware that their computers have been compromised or their personal information exploited. The FBI said because of the widely distributed abilities of botnets they not only harm individuals but are now considered a threat to national security, as well as the information infrastructure and the economy.

SEARCH ENGINES

A problem with most search engines is that they are ambivalent to content permissions. Certain individuals (such as the head of payroll) may have permission to view all of the company's information. While other individuals (such as the head of personnel) are limited in the type of data are allowed to see. An employee may be given permission to see their own information but not that of the person working next to them. There may also be certain individuals that are not allowed to see any information at all. Because search engines typically can not take data ownership and coordinate it with user permissions, problems can arise when responding to a request.

"When implemented carelessly, search engines have the potential to uncover flaws in existing security frameworks and can expose either restricted content itself or verify the existence of hidden information to unauthorized users" (Vivisimo, 2006). In this regard, poorly implemented search engines could release large amount of personal identification information. Imagine typing the name of the CEO in a search engine and receiving a page that lists his personal phone number, salary, and home address.

WIRELESS MEDIA

Organizations may think their mobile workers are safe with their new wireless notebooks, but recent WLAN tracking at the RSA security conference showed a multitude of vulnerabilities. Some common faults were that many users were using hotspots, but had no idea who was sponsoring the ports. In some cases, it was discovered that the users were actually talking to other local computers that also had their connections active (Shaw & Rushing, 2007).

Wireless devices often remember the "last good" site they were connected to and attempt to use them first. Which means that if the user did

not shutdown the port (disconnect from a hot spot correctly), the computer will look for that spot first, even if there is a more secure connection available. Another issue is that the port will continue to actively search for a signal. A critical situation can arise if the user forgets to disable the wireless card, and then plugs his/her device into a wired network. A couple of things could happen—the network will see the other port and might adjust its routing information to accommodate it, in the process it could bypass firewalls and border security. Another thing that may happen is the device might also connect to another device via the wireless port, again bypassing some security, but elevating the permissions and authority of the newly connected user to that of the legitimate user. In either case, the result is a huge hole in security (Shaw & Rushing, 2007).

Organizations are paying a very high price for wireless management. The Aberdeen Group estimates that it costs nearly 10 times more to manage wireless services and devices compared to wired-lines (Basili, 2007). In spite of that, Aberdeen found that 80% of respondents were planning increases in mobile wireless access.

The RSA Conference is an event that draws thousands of computer users. Many of them bring their wireless laptops (and other devices). AirDefense (2005), a wireless security company, credited by many as the founder of the wireless security industry, found that more than half of the 347 wireless devices it monitored during conference were susceptible to attack. What is truly amazing is not that it happened once, but just 2 years later it happened again at another RSA conference. AirDefense once again found that more than half of the wireless devices at the conference network were themselves unsecured and were vulnerable to attacks; thus leading to the conclusion that the people responsible for protecting enterprise data were not doing a very good job of protecting their own assets (Cox, 2007).

Telephones

Wireless telephones with computer-enabled features (such as e-mail and Internet access) have been compromised; Trend Micro Inc. announced it had found security flaws on MS Windows Mobile, a popular operating system used in the smartphone. Many individuals that used these devices are executives who routinely access sensitive information. In this case, the main risk is not malware, but the risk of lost devices.

Mobile Encryption

The news regularly reports that laptops with thousands of sensitive records on customers or employees are lost or stolen each month. Organizations know the risks and the threats. These threats are easy to understand but most organizations do not allocate the resources necessary to protect themselves. Encryption is an effective safe guard for most mobile devices, and one that will relieve some of the legislative pressures. However, it is far from being fully adopted; a survey by Credant (see McGillicuddy, 2006) asked respondents to list reasons why their companies had not adopted encryption for mobile devices.

- 56% indicated it was due to a lack of funding;
- 51% said encryption was not a priority; and
- 50% said there were limited IT resources; in other words: "No one wants to pay for it."

Mobile devices are often seen as low-powered, low-capacity corporate tools. To which there is considerable fear that encryption will add little, but in the end will slow them down. Critics cite that the idea behind mobile devices is to make the user more productive by added convenience. Anything that slows down the devices would ultimately detract from the user's productivity. Additionally, encrypted devices are harder to

diagnose, repair, and recover. However, these concerns are more applicable to older less powerful devices (McGillicuddy, 2006).

DATA

Organizations accumulate a wide breath of data, that if stolen could potentially hurt the enterprise. Loss or theft of confidential information: such as blueprints and engineering plans, tenders, budgets, client lists, e-mails and pricelists, credit card and other financial information, medical or other confidential personally identifiable records, classified, restricted or personal information, scripts, storyboards, source code, database schemas, or proprietary trade secrets can severely impact the integrity and profitability of a corporation. "This risk is amplified by the prevalence of portable computing devices as a part of normal business activities and by the increasing levels of online transactions that occur routinely" (GFI-2, 2007).

Fundamentally, there are two types of security. The first type is concerned with the integrity of the data. In this case the modification of the records is strictly controlled. The second type of security is the protection of the information content from inappropriate visibility. Names, addresses, phone numbers, and credit card details are good examples of this type of data. Unlike the protection from updates, this type of security requires that access to the information content is controlled in every environment.

The Internet makes it easy for organizations to collect personal identifying information, such as: names, addresses, social security numbers, credit card numbers, or other identifiers (Shimeall, 2001). If this information were disclosed inappropriately, it would put these individuals at risk for identity theft (Wang, Lee, & Wang, 1998). To guard against such an outcome, laws worldwide have been passed to aid in data protection.

The Threat from Within

Within the U.S., the Gartner Group estimates that 70% of all unauthorized access to information systems is committed by employees. The CSI/FBI survey found that 68% of respondents claimed losses due to security breaches originating from insiders (Gordon, Loeb, Lucyshyn, & Richardson, 2006). Of course, the magnitude of insider malfeasances depends somewhat on how one slices and dices the numbers. The U.K. Scotland Yard Computer Crime Research Center, (2005) found that 98% of all crimes committed against companies in the U.K. had an insider connection. In the USA, surveys conducted by the U.S. Secret Service and CERT coordination center concluded that: "Respondents identified current or former employees and contractors as the second greatest cyber security threat, preceded only by hackers" (Keeney, Kowalski, Cappelli, Moore, Shimeall, & Rogers, 2005).

ENDPOINT (PERIMETER-BASED) SECURITY

The term endpoint, as its name implies, is any place that a device can interact with another device. Generally speaking, an endpoint is an individual computer system or device that acts as a network client and serves as a workstation or personal computing device. Endpoints are often mobile and intermittently connected and in the mobile society, they are becoming indistinguishable (Forescout, 2007; Endpointsecurity, 2004).

Laptops have become so popular they have almost caught up with desk top machines, as office use goes (40% to 45%—CSI/FBI survey, 2006). Because laptops are not tethered to the desk, they are routinely out of the protection of the organization's network. Additionally, if removable media (floppy's, CDs, DVD's, flash drives) are used on laptops or office machines, they are an easy entry point for malware. A further security

concern is the construct of engineering devices for easy maintenance. These easy maintenance devices can allow a person to literally remove the internal hard drive from a laptop in less than a minute and make off with all of the private data that is in the machine.

Endpoint security is the total measures taken to implement security sending and receiving data. These measures include assessing the risk to the clients' antivirus and personal firewalls, as well as protecting the network from themselves. Endpoint security logically extends to the management and administration of these security measures. It also deals with risk, reporting, and knowledge management of the state and results of these measures (Positive Networks—Endpoint security).

Endpoint Components

Firewalls

In general terms, a firewall is software or a hardware device that controls the flow of traffic between two networks or entities. A packet filter firewall works by inspecting the contents of each network packet header and determining whether it is allowed to traverse the network. There are basically three types of firewalls: packet filter, "stateful" inspection, and application proxy.

In the case of a personal firewall, it controls the network traffic between a computer on one side, and the Internet or corporate network on the other side. A firewall is a network (hardware & software) node that isolates a private network from a public network. The firewalls' job is to keep unwelcome traffic from the Internet out of the computer, and also to keep in the traffic that you do not want leaving the computer. To that end, organizations may have several firewalls to create barriers around different layers of their infrastructure. Firewalls are often compared to a "bouncer" at a nightclub: they are located at the point of entry; they enforce rules to determine who gets in (and out); and they inspect all that passes through the doors they are guarding. With a layer approach, it is possible that a firewall can insure that even if a password is compromised an intruder will only have restricted access to the network.

However, firewalls are neither the first nor the last word in endpoint components. Hardware and software firewalls have a serious flaw in that they typically do not look at the contents of a packet; they only look at its headers. As written earlier, antivirus software is not very effective against spyware, the same is true with a firewall.

PREVENTIVE MEASURES

The open nature of PCs in most organizations has resulted in users installing a wide variety of applications that they use to get through their day, and several that they should not. Some IT managers attempt to prohibit the use of unauthorized peripherals (removable media) and applications with the hope that this process will shut out malware. The usage of portable devices at work could impact corporate network security through the intentional or unintentional introduction of viruses, malware, or crimeware that can bring down the corporate network and or disrupt business activity.

Even with the tightest security net, it is possible for a destructive breach to occur. Failure to implement a security audit process to meet government regulatory requirements can result in significant fines, in addition to the possibility of imprisonment. The risks are real and affecting businesses on a daily basis (Juniper Research, 2006).

Further, not only are devices a threat to data and machine integrity, but also to worker productivity. An employee can use company hardware and software to enhance digital photos, play computer games, or work on freelance projects. The control of USB (universal serial port) ports can limit unauthorized use and prevent intentional or accidental attacks against a company's network (Muscat, 2007). Control of the USB ports can be

made either programmatically or by physically locking & blocking them (PC Guardian).

Additionally, there are emerging technologies that monitor the movement of data and enforce actions on the data based on company policies. These products from vendors such as Orchestria and Vericept work at the network and desktop levels, and can monitor movement, as well as prevent data from being copied from the originating application to external sources, such as USB drives.

Another approach relies on detecting the departure of an authorized user. A wireless USB PC Lock will lock and unlock a PC based on a user's proximity to the machine. A small transmitter is carried by the user, if s/he is more than two meters away, the machine's screen will be programmatically locked, once the user returns in range the screen is unlocked.

The End User

While the chapter is aimed at management, we would be amiss if we did not describe some things that the end user can do. This list is far from complete and some may argue about the order of which items are presented. They might also point that import suggestions have been admitted. The caveat is that this list is not for corporate users, it is for the home user. For the home user, the advice is simple:

1. Get a good antivirus package and keep it up to date.
2. Let your system download system updates (patches) from a trusted site.
3. Deactivate Active X components.
4. Do not install items from unknown sources.
5. Do not open e-mails from people or organizations that you do not know.
6. Never click on an embedded e-mail link; copy it or use a book mark.
7. Be extremely careful about what sites you visit.
8. Strangers that send you mail, want something!
9. You will not win something if you did not enter.

In an organizational environment, the mentioned still applies. However, the user is usually burdened by user names and passwords. The number one suggestion is pick a strong password and do not share it with anyone for any reason. If you need to have multiple sign-ons, tailor the passwords for each application. For example your password for accounts payable may begin with AP. The easiest way to pick strong passwords is to create an acronym out of your favorite song lyrics. Take the first letter of each of the first 12 words, your application code and some important number, like the middle digits of your first home address.

The Human in the Equation

According to CompTIA's IT security survey, human error, either alone or in combination with a technical malfunction, was blamed for 74% of the IT security breaches (Cochetti, 2007). Human involvement in systems is not limited to making errors; during the day users often take breaks to surf the Web, e-mail, or IM their friends.

However, Web surfing can do more than relieve stress and waste time; it can expose users and organizations to dangerous Web sites, data leakage, and e-mails with inappropriate or dangerous content. Further, it can lead to installation of non-authorized software, which besides prompting civil and criminal investigations, can introduce piracy robbing malware. This type of publicity has a negative impact on the bottom line. To protect themselves, organizations should abide by a strong user access policy (Shinder, 2007).

Instant messaging (IM) has begun to be embraced by organizations because it provides a cost effective means to electronically communicate both synchronously and nearly instantaneously. IM presence awareness and permission-based lists

give the perception of a low risk of receiving spam or other unwanted messages. The rapid adoption of public IM services (such as AOL, MSN, and Yahoo) has raised serious concerns about security risks and compliance with regulatory requirements. IM and e-mail can be used as a tool for deliberately disseminating private information; or it may provide a channel that could inadvertently admit spyware, worms, or viruses. Since instant messaging involves free electronic communication with internal employees and anyone designated as a "trusted" colleague, unauthorized information dissemination may proliferate via unmonitored (Webex, 2006).

Roger J. Cochetti, group director—CompTIA U.S. Public Policy states "... security assurance continues to depend on human actions and knowledge as much, if not more so, than it does on technological advances." He indicates that failure to follow security procedures (human error) was blamed by more than 55% of the organizations as the factor that contributed the most to security breaches (Cochetti, 2007).

LISTING: WHITE, BLACK, AND GRAY

Listing is a response to malware's continuous mutation of their signatures, which results in a continuous flow of zero-day attacks. The basic idea is to restrict execution of programs based on a list. Listing comes in three distinct styles: white, black, and gray.

White listing basically consists of allowing users/workstations to run only software that has been pre-approved by the organization. Implementing this approach requires conducting exhaustive inventory of all applications in use as well as their version. Once the inventory is completed, each application must be reviewed to ensure it is required. After the review, the software implementations and versions need to be made consistent across the "protected" network segments.

Black listing is the opposite of white listing. Workstations are prevented from running applications or visiting Web site that are specifically listed. Thus, sites that are found to be perpetrators of malware and spam are "banned" from user activity. While this may seem to be a viable approach for the business managers, it is weak, and can be very risky, if not supported by additional controls. A missed module can be disastrous. Further, new malicious or highly vulnerable applications are created or identified faster than they can be placed on a blacklist.

Gray listing is a conditional blacklist, and has a high risk of false positives, blacklisting someone by mistake.

Hybrid listing is a combination of features that combine the features of white, black, and gray listing. It is designed so that management can approve some software and ban other software that is not needed or wanted, thus preventing the first execution of any new unknown software. Because the hybrid approach prevents the first execution, not the installation, the approval/authorization process can be centrally managed in real time.

Browser-based listing relies on a modern browser to check that the site a user is going to is not a forgery. One option downloads a list of known Web forgeries (see Figure 1—ploy to capture personal information): but this technique only offers real protection for a few moments after it is downloaded. Another technique would be to have the browser check with an authority (such as Google) each time a URL or site is entered.

Mozilla indicates that users can protect themselves from Web forgeries by:

- That instead of following links from a e-mail to banks or online commerce sites, always either type the Web page address in manually or rely on a bookmark;
- They also recommend using a Password Manager to remember passwords instead of entering them manually; and

- They recommend using an e-mail product that will detect and alert the user about suspect web sites.

Least Privilege Authority

In an organizational environment, the information systems/information technology group struggles to give users the access they need and want, while attempting to ensure that security is not sacrificed. Programs that perform useful functions of work are known as applications. Applications need certain capabilities to create, read, update, and delete data—these privileges often go by the acronym CRUD. Applications need access to certain services that are only granted access through the operating system or the system administrators: such as scheduling new tasks, sending information across applications, and verifying passwords. In order for that to work the application/user needs to be at a high enough level of trust (permissions/privileges/authority) so that they know what they are doing.

With the principle of least privilege, the goal is to give users only the minimal access and privileges they need to complete the task at hand. In most cases this will be for the entire logon session, from the time they logon in the morning till they leave for the night. The concept of principle of least privilege is a prophylactic—kind of a safety belt; if the machine is not attacked by malware, it is not necessary and does no harm; but if it is, it's an extra layer of protection. Therefore, the construct of least privilege is becoming a common phrase as organizations scramble to protect network assets and resources.

Vulnerability Management

The process of patch management can be complex, difficult, and is often sacrificed when an organization is in a "crisis" mode. If shortcuts are taken, they will almost always comes back to haunt the organization. Patching in the programming has long been defined as "trading an error that is known for one that is unknown." It is not the thing to rush through. Vendors spend considerable time researching vulnerabilities and devising repairs or work-arounds. Many of the repairs are dependent on updates being already applied. Failure to stay current on updates is one of the main reasons that enterprises struggle with bot infections (Symantec).

Patching is a tradeoff between the time required to repair a problem responsibly and completely versus the hacker's window of opportunity to exploit a specific vulnerability. Vulnerability management has become a critical aspect in managing

application security. Patching vulnerabilities (depending on the severity) can be a time consuming job. To do it safely, the patches should be applied and tested in an isolated environment against a copy of the system.

- **New components of distributed architectures:** Standardization and plug-and-play are not always positive, they come with a price. Standardize code makes it easier for all involved the developer and the criminal hacker. Each module represents a unique addressable attack point—a target at which criminal hackers can aim their exploits.
- **Multiplying network access points** can act similar to an open wound, if one is not careful, it will allow in all sorts of viruses and the like. With organizations opening their networks to suppliers, clients, customers, employees, and contractors, security has become a mandate. Multiple entry points have raised the importance of controlling the traffic that comes and goes through the network. Within this regards, firewalls and antivirus products are important parts of an effective security program.
- **Wireless network access points** bring their own set of issues. With wireless, the perimeter (endpoint) security is critical. It is important to have IDS (intrusion detection system) and to monitor all traffic.
- **Simply relying upon firewalls and antivirus** is not an effective strategy. Understanding the network and understanding its weaknesses (vulnerabilities) can provide insight on how to manage and protect critical data.

CONCLUSION

No matter how hardened a network perimeter is, there are a number of weaknesses that can allow breaches to occur. It is usually recommended that a layer defense approach be adopted to strengthen protection. However, care needs to be taken that additional layers actually add protection instead of just protecting against the exact same vulnerabilities or threats. Reckless implementation or selection of software may not produce the desired outcome. A layered approach may be more like buying overlapping warranty coverage. The harm is that businesses may confuse this approach for real security. Ultimately, they could end up spending more money and resources on implementing the wrong security mechanisms without gaining complete security (Ou, 2007).

Remember the organization is responsible for maintaining the privacy of the stakeholder's consumer while also preserving a harassment-free, discrimination-free, crime free, and civil business environment. The development, implementation, and enforcement of a comprehensive Internet policy can help in that goal. Whether employees intentionally violate Internet policy or accidentally surf to an objectionable Web site, under the legal principle known as vicarious liability, the employer can be held responsible for the misconduct of the organization's employees—even if the employer is completely unaware that there is a problem.

Simply following security best practice by limiting access rights may be a good first step, but it is just a step. No single approach is going to be totally viable against all malware and protect privacy. The best protection comes from using a layer approach. In addition to using technology it is important to:

- Create and enforce policies and procedures
- Educate and train
- Monitor the network and the systems
- Require Penetration testing
- Ban inappropriate sites and prohibit wasted resources and productivity

Aberdeen Group's (2005) research shows that technology, by itself is not the primary indicator for success—this was true despite differences in technology usage, loss rates, or firm sizes. They

also found that organizations performing as best in class leaders focus on managing four areas to maximize results for the money being spent on security:

1. Sharing of data and knowledge to improve results
2. Processes in place for executing against objectives
3. Organizational structure and strategy to manage to results
4. A security technology maturity that influences results

Of the four, they indicate that the most important focus area is the managing of data and knowledge to improve results.

This chapter presented an overview of the concerns that organizations must address while working within the Internet community. It was meant to inform management of the potential threats and pitfalls that must be addressed to be a viable player within the Internet realm. While there are many technical areas that need to be attended to, nothing is more important than ensuring maintaining the users' confidentiality, integrity, and authenticity (CIA). Hackers and con-artists are devising clever and inventive techniques to violate a user's privacy for the purpose of committing illegal activities. If left unchecked, these issues threaten the viability e-commerce and e-business.

FUTURE RESEARCH DIRECTIONS

This chapter lays out some of the issues that must be concentrated on. With the most emphasis being placed upon a strong organizational Internet privacy and security policy, followed by education and training of users and stakeholders.

Future research should focus on how large and small organizations create, maintain, and monitor privacy and security policies. Because organizations are of differing sizes and have different resources available, research should investigate how large and small organizations vary on their approaches and implementation. Future research should also focus on how existing protections can be expanded to protect tomorrow's technology. Finally, research needs to be conducted on how protecting portable storage devices from misuse, as this type of media is bound to proliferate.

REFERENCES

Aberdeen Group. (2005). *Third brigade—business value research series—most important security action: Limiting access to corporate and customer data.* Whitepaper. Retrieved October 2007, from http://www.thirdbrigade.com/uploadedFiles/Company/Resources/Aberdeen%20White%20Paper%20--%20Limiting%20Access%20to%20Data.pdf

Air Defense Press Release. (2005, February 17). *AirDefense monitors wireless airwaves at RSA 2005 conference.* Retrieved October 2007, from http://airdefense.net/newsandpress/02_07_05.shtm

American Management Association. (2005). *Electronic monitoring & surveillance survey.* Retrieved October 2007, from http://www.amanet.org/research/pdfs/EMS_summary05.pdf

Basili, J., Sahir, A., Baroudi, C., & Bartolini, A. (2007, January). *The real cost of enterprise wireless mobility* (Abridged ed.). The Aberdeen Group. Retrieved October 2007, from http://www.aberdeen.com/summary/report/benchmark/Mobility_Management_JB_3822.asp

Baylor, K. (2006, October 26). *Killing botnets McAfee.* Retrieved March 2007, from http://blogs.techrepublic.com.com/networking/?cat=2

Bernard, A. (2006). *McAfee's top ten security threats for 2007.* Retrieved October, from http://www.cioupdate.com/print.php/3646826

Bumgarner, J., & Borg, S. (2007). *The US-CCU cyber security check list*. Retrieved November 2007, from http://www.usccu.us/documents/US-CCU%20Cyber-Security%20Check%20List%202007.pdf

Cafarchio, P. (2004). The challenge of non-viral malware! *TISC Insight Newsletter, 4*(12). Retrieved October 2007, from www.pestpatrol.com/Whitepapers/NonViralMalware0902.asp

Cannon, D. M., & Kessler, L. (2007). Danger—corporate data breach! *Journal of Corporate Accounting & Finance, 18*(5), 41–49. doi:10.1002/jcaf.20322

CERT. (2007). *Vulnerability remediation statistics*. Retrieved November 2007, from http://www.CERT. org/stats/vulnerability_remediation.html

Clearswift. (2006 October). *Simplifying content security—ensuring best-practice e-mail and web use. The need for advanced, certified email protection*. Retrieved October 2007, from http://whitepapers.zdnet.com/whitepaper.aspx?&scid=280&docid=271750

Cochetti, R. J. (2007, June). *Testimony of the computing technology industry association (CompTIA), before the house small business committee subcommittee on finance and tax, sata security: Small business perspectives.* Retrieved October 2007, from www.house.gov/SMBiz/hearings/hearing-06-06-07-sub-data/testimony-06-06-07-compTIA.pdf

Computing Technology Industry Association. (2004). *Annual study.* Retrieved October 2007, from http://www.joiningdots.net/library/Research/statistics.html

Cox, J. (2007, February 9). RSA: attendees drop ball on wi-fi security—many IT security experts at conference used unsecured devices. *Network World.* Retrieved October 2007, from http://www.networkworld.com/news/2007/020907-rsa-wifi-security.html

Endpointsecurity. (2004). *What is endpoint security?* Retrieved October 2007, from http://www.endpointsecurity.org/Documents/What_is_endpointsecurity.pdf

Fielding, J. (2007, January 28). *25% of all computers on Botnets*. Retrieved http://blogs.techrepublic.com.com/networking/?cat=2

Flynn, N. (2005). E-policy best practices a business guide to compliant & secure internet, instant messaging (IM), peer-to-peer (P2P) and email communications. *The ePolicy Institute; Executive Director, St. Bernard Software*. Retrieved http://www.securitytechnet.com/resource/security/application/iPrism_ePolicy_Handbook.pdf

Forescout. (2007). NAC enforcement and the role of the client. *Infonetics Research, Inc.* Retrieved July 2007, from www.Forescout.com/downloads/whitepapers/Infonetics-NAC-Enforcement-and-the-Role-of-the-Client.pdf

GFI. (2007). *The threats posed by portable storage devices*. Whitepaper. Retrieved July 2007, from http://www.gfi.com/whitepapers/threat-posed-by-portable-storage-devices.pdf

Glaessner, T. C., Kellermann, T., & McNevin, V. (2004). *Electronic safety and soundness securing finance in a new age* (World Bank Working Paper No. 26). Washington DC Retrieved http://siteresources.worldbank.org/DEC/Resources/abstracts_current_studies_2004.pdf

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). CSI/FBI computer crime and security survey. *Computer Security Institute.* Retrieved November 2007, from http://www.cse.msu.edu/~cse429/readings06/FBI2006.pdf

Harley, D., Slade, R., & Gattiker, U. (2001). *Viruses revealed: Understanding and counter malicious software*. New York: McGraw-Hill/Osborne.

Higgins, K. (2007, November 9). *The world's biggest botnets*. Retrieved November 2007, from http://www.darkreading.com/document.asp?doc_id=138610

Im, G. P., & Baskerville, R. L. (2005, Fall). A longitudinal study of information system threat categories: The enduring problem of human error. *ACM The DATA BASE for Advances in Information Systems, 36*(4), 68–79.

Juniper Research. (2006, February). *Security information & event management*. Retrieved http://www.juniper.net/solutions/literature/solutionbriefs/351178.pdf

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., & Rogers, S. (2005). Insider threat study: Computer system sabotage in critical infrastructure sectors. *U.S Secret Service and CERT Coordination Center/SEI*. Retrieved November 2007, from http://www.CERT. org/archive/pdf/insidercross051105.pdf

Kirk, J. (2007, May 17). Estonia recovers from massive denial-of-service attack. *InfoWorld, IDG News Service*. Retrieved November 2007, from http://www.infoworld.com/article/07/05/17/estonia-denial-of-service-attack_1.html

McAfee, J., & Haynes, C. (1989). *Computer viruses, worms, data diddlers, killer programs, and other threats to your system*. New York: St. Martin's Press.

McGillicuddy, S. (2006, November 1). Encrypting mobile devices: A best practice no one uses *SearchSMB.com*http://searchSMB.techtarget.com/originalContent/0,289142,sid44_gci1227295,00.html?asrc=SS_CLA_300336&psrc=CLT_44

Muscat, A. (2007, January 17). Perils of portable storage. *Computer Reseller News*. Retrieved http://www.gfi.com/documents/32686_crn_eprint.pdf

Norman, D. (1983). Design rules based on analysis of human error. *Communications of the ACM, 26*(4), 254–258. doi:10.1145/2163.358092

Osterman Research Inc. (2003). *The impact of regulations on email archiving requirements*. ORI white paper sponsored by Information Management Research. Retrieved October 2007, from http://www.Ostermanresearch.com/whitepapers/or_imr01.pdf

Ou, G. (2007) Wireless LAN security myths that will not die. *ZDNet*. Retrieved July 2007, from http://blogs.zdnet.com/Ou/?p=454

Padilla, R. (2007). Root out data breach dangers by first implementing common sense. *TechRepublic*. Retrieved July 2007, from http://blogs.techrepublic.com.com/tech-manager/?p=312

Pai, A. K., & Basu, S. (2007). Offshore technology outsourcing: overview of management and legal issues. *Business Process Management Journal, 13*(1), 21–46. doi:10.1108/14637150710721113

Privacy Rights Clearinghouse. (2007). *A chronology of data breaches*. Retrieved October 2007, from http://www.privacyrights.org/ar/ChronDataBreaches.htm

Provos, N., McNamee, D., Mavrommatis, P., Wang, K., & Modadugu, N. (2007). The ghost in the browser analysis of web-based malware. *Google, Inc.* Retrieved http://www.usenix.org/events/hotbots07/tech/full_papers/Provos/Provos.pdf

Qualys. (2006). *The laws of vulnerabilities: Six axioms for understanding risk*. Retrieved October 2007, from http://developertutorials-whitepapers.tradepub.com/free/w_qa02/pf/w_qa02.pdf

Savage, M. (2007, October 23). *Proposed legislation would strengthen cybercrime laws*. Retrieved November 2007, from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1278341,00.html?track=sy160

Schuman, E. (2007, November 14). TJMaxx's projected breach costs increase to $216M. *eWEEK*. Retrieved November 2007, from http://fe42.news.sp1.yahoo.com/s/zd/20071114/tc_zd/219495

Shaw, K., & Rushing, R. (2007). *Podcast, Keith Shaw (NetWorkWorld) talks with Richard Rushing chief security officer at... data, listen to this podcast*. Retrieved October 2007, from http://www.networkingsmallbusiness.com/podcasts/panorama/2007/022807pan-airdefense.html?zb&rc=wireless_sec

Shimeall, T. (2001, August 23). *Internet fraud,* Testimony of Timothy J. Shimeall, Ph.D. CERT®, Analysis Center Software Engineering Institute, Carnegie Mellon University Pittsburgh, PA; Before the Pennsylvania House Committee on Commerce and Economic Development, Subcommittee on Economic Development, retrieved October 2007, available http://www.CERT. org/congressional_testimony/Shimeall_testimony_Aug23.html

Shinder, D. (2007, February 9). *How SMBs can enforce user access policies*. Retrieved April 2007, from http://articles.techrepublic.com.com/5100-1009_11-6157054.html?tag=nl.e101

Staff, C. N. E. T. (2004, September). *Spam volume keeps rising*. Retrieved September 2007, from http://news.com.com/2114-1032-5339257.html

Symantec. (2006, September 19). *Symantec finds firms recognize importance of application security, yet lack commitment in development process*. News release. http://www.symantec.com/about/news/release/article.jsp?prid=20060919_01

Vivisimo. (2006). *Restricted access: Is your enterprise search solution revealing too much?* Retrieved October 2007, from via http://Vivisimo.com/ or http://www.webbuyersguide.com/bguide/whitepaper/wpDetails.asp_Q_wpId_E_NzYyMQ

Wang, H., Lee, M., & Wang, C. (1998, March). Consumer privacy concerns about internet marketing. *CACM, 41*(3), 63–70.

Webex.(*2006*). On-demand vs. On-premise instant messaging. *Webex Communications, Ease of Communications—On Demand EIM Solutions*. Retrieved October 2007, from http://www.webbuyersguide.com/bguide/Whitepaper/WpDetails.asp?wpId=Nzc4MQ&hidrestypeid=1&category=

Wilson, T. (2007, November 12). *ID thief admits using botnets to steal data*. Retrieved November 2007, from http://www.darkreading.com/document.asp?doc_id=138856

Yank, G. C. (2004 December 21). *Canning spam: Consumer protection or a lid on free speech?* Retrieved October 2007 from http://www.law.duke.edu/journals/dltr/articles/2004dltr0016.html

ADDITIONAL READING

Bächer, P., Holz, T., Kötter, M., & Wicherski, G. (2005). Know your enemy: tracking botnets; using honeynets to learn more about bots. *The Honeynet Project & Research Alliance*. http://www.honeynet.org Retrieved October 2007, from http://www.honeynet.org/papers/bots/

Cohen, F. (1984). Experiments with computer viruses. Fred Cohen & Associates. Retrieved October 2007, from http://all.net/books/virus/part5.html

Commission of the European Communities. (2000). *Proposal for a directive of the European parliament and of the council concerning the processing of personal data and the protection of privacy in the electronic communications sector*. Retrieved October 2007, from http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/com2000-385en.pdf

Computer Crime Research Center. (2005). *Security issues: find the enemy within*. Retrieved October 2007, from http://www.crime-research.org/analytics/security-insider/

Endicott -Popovsky. B., & Frincke, D. (2006). Adding the fourth "R": A systems approach to solving the hacker's arms race. In *Proceedings of the 2006 Symposium 39th Hawaii International Conference on System Sciences*. Retrieved October 2007, from http://www.itl.nist.gov/iaui/vvrg/hicss39/4_r_s_rev_3_HICSS_2006.doc

European Parliament and the Council of the European Union. (2003). *Annex 11 computerised systems, Labcompliance*. Retrieved October 2007, from http://www.labcompliance.com/documents/europe/h-213-eu-gmp-annex11.pdf

Federal Trade Commission. (1999). *Gramm-Leach bliley act*. Retrieved October 2007, from http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Federal Trade Commission. (2006). *ChoicePoint settles data security breach charges; to pay $10 million in civil penalties, $5 million for consumer redress*. Retrieved October 2007, from http://www.ftc.gov/opa/2006/01/choicepoint.htm

Henry, P. A. (2007, June). *Did you GET the memo? Getting you from Web 1.0 to Web 2.0 security. (In Today's Risky Web 2.0 World, Are You Protected?)*. Secure Computing Corporation.

King, S. T., Chen, P. M., Wang, Y., Verbowski, C., Wang, H., & Lorch, J. R. (2006). *SubVirt: Implementing malware with virtual machines*. Retrieved October 2007, from http://www.eecs.umich.edu/virtual/papers/king06.pdf

MessagesLabs. (2007). *Effectively securing small businesses from online threats*. Retrieved October 2007, from http://www.messagelabs.com/white_papers/secure_smb

SANS Institute. (1999, May). Management errors. In *Proceedings of the Federal Computer Security Conferences held in Baltimore*. Retrieved October 2007, from http://www.sans.org/resources/errors.php

Sarbanes-Oxley. (2002). *Sarbanes-Oxley act of 2002*. Retrieved October 2005, from http://www.sarbanes-oxley.com/section.php?level=1&pub_id=Sarbanes-Oxley

Shinder, D. (2002). *Scene of the cybercrime* (Computer Forensics Handbook). Rockland, MA: Syngress Publishing.

United Kingdom Parliament. (2000). *Freedom of information act 2000*. Retrieved October 2007, from http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm

U.S.A. Department of Health & Human Services. (1996). *Health insurance portability and accountability act of 1996*. Retrieved October 2007, from http://aspe.hhs.gov/admnsimp/pl104191.htm

U.S.A. Federal Trade Commission. (2002). *How to comply with the privacy of consumer financial information rule of the Gramm-Leach-Bliley act*. Retrieved July 2002, from http://www.ftc.gov/bcp/conline/pubs/buspubs/glblong.shtm

This work was previously published in Online Consumer Protection: Theories of Human Relativism, edited by Kuanchin Chen and Adam Fadlalla, pp. 33-56, copyright 2009 by Information Science Reference (an imprint of IGI Global).