2

Cyber Security

Barry Lunt, Dale Rowe and Joseph Ekstrom
Brigham Young University
USA

1. Introduction

Prior to HTML, browsers, and the WWW, computer interconnections were localized and limited. Since the early 1990s, web technologies have made it easy for everyone to access and post content on the Internet. Before long, there were thousands, then hundreds of thousands, and soon tens of millions of computers, all connected together via the Internet. As noted by Robert Metcalfe, and as later codified in what became known as "Metcalfe's Law", the value of a network goes up as the square of the number of users. Regardless of whether we accept his exact quantification of the value, there is no question that a few interconnected computers are more valuable than the same computers not being interconnected, and that many (or all) computers being interconnected has much more value than only a portion of them.

This is the situation today: essentially all desktop, notebook, netbook and tablet computers are interconnected via the Internet, and the same is true for the majority of cell phones. Additionally, even a significant portion of embedded computers are being connected via the Internet, as well as most industrial control and monitoring computers. Suffice it to say that, if the trend continues, and the evidence is very strong that it will, most computers, mobile devices, and even embedded systems either are or soon will be connected via the Internet.

While this has dramatic advantages for a free and open society, there has always been an element of society that would attempt to take advantage of this openness in ways that are damaging to other computers, users, the data, or to society as a whole. The need to protect our computers, users, data, and society, from this type of abuse, is the field of information assurance and security.

2. Guarding our information

Most businesses today would recognize the need to follow the most economical path to maximum profit. Frequently an organization's profit margins form the primary indicators as to their success. Even government agencies must admit to being somewhat cost-driven. With the recent economic downturn and increased competition to stay one foot ahead, businesses may be tempted to consider security as an afterthought, rather than an integral part of their business models and practices. In this Chapter we will look at some of the devastating implications of this error and why every genre of organization must place security at the forefront of business planning and practice.

Consider the owner of an expensive luxury vehicle who, each day outside his workplace, leaves his doors unlocked, with the keys in the ignition. The foolhardiness of the owner is apparent, and some readers may go so far as to suggest he would deserve to have his vehicle stolen. Yet in our modern information-driven organizations, corporations and agencies that depend on their information and data in their day-to-day operations often omit security entirely from consideration. At best it is an afterthought, akin to putting a 'do not steal' sign on the aforementioned vehicle and hoping this will deter all potential criminals.

In 2010, for the first time, the worldwide cost of information and electronic data theft (excluding piracy) rose 9.3% from 2009 to surpass all other theft (Kroll, 2010). In the UK alone, the cost of cyber-crime to businesses, individuals and government cost $43 billion US dollars (2010). In the 2011 series of cyber-attacks against Sony, some analysts believe the long-term costs to be in excess of $24 billion (Sebastien, 2011). Staggering as these figures are, the truth remains that most of these breaches could have been prevented had security been integrated into the victim's plans and policies.

It may be hard to understand why cyber-attack costs can reach such staggering figures. It can often come as a surprise to a victim that the true cost of an attack can far exceed the cost of hardware technology assets, or an annual IT budget. Indeed, the failure to comprehend the true risk of attacks and associated costs is in part what has led to such a prevalence of successful breaches. To be secure requires more than a retrofitted firewall installed merely as an afterthought. Organizations must understand the true cost, impact and consequences of cyber-attacks in order to identify what steps should be taken to protect their most valuable assets.

3. Visualizing the cyber-landscape

The first step in better understanding cyber-attacks is to become aware of how intricately connected information systems and technology have become. A system should not be thought of as a series of devices connected by wires, but rather a combination of people, technology and networks that function within defined parameters to achieve a specified objective. As organizations begin to view their systems from this perspective, it becomes obvious why few technical measures, even if expensive and state-of-the-art, may be ineffective in ensuring their protection from a cyber-attack.

Some academics have claimed that cyberspace is defined more by social interactions than technical implementation. Morningstar and Farmer argue that the computational medium in cyberspace is an augmentation of the communications channel between real people (Morningstar & Farmer, 2003). This concept of a socially interconnected system of systems was further visualized in an IBM video published on YouTube in 2010 ("Smarter Leaders vPanel: Tackling Urban Traffic with Social Computing", YouTube, 2010; http://www.youtube.com/watch?v=-thvI-IjwgY). These interconnections between social computing and cyber-security are perhaps the most overlooked aspects in providing effective security. From a defensive standpoint, we should treat cyberspace as the nexus that allows for the potential and very real connections among international organized crime, terrorists, hackers, foreign intelligence agencies, military and civilians.

The balance between usability and security is a fundamental concept that encourages security professionals to be mindful of the user needs. Even so, the visualization of social interactions using technology presents a new challenge for those responsible for cyber-security planning. Understanding the possible motivations and means behind a cyber-attack can better equip enterprises to prepare for and respond to an attack. Research has shown that on average, the cost of cyber-crime is reduced by 38% by companies which implement Governance, Risk Management and Compliance (GRC) measures across their enterprise (Ponemon Institute, 2011).

The mistake of assuming security is someone else's problem often comes with tragic consequences. It is not the responsibility of engineers, consultants, IT professionals or even management to undertake alone, but is the responsibility of every user. Granted, there are many specific roles required in security planning, but if the plan does not include each and every user as a member of the security team, it will be doomed before it has even been implemented.

The domain of cyber-security is highly subject to external pressures. These definitional forces include the following (Agresti, 2010): 1) *Rebranding exercise* – the former term "information assurance and security" is being replaced by "cyber-security", as the term "cyber" creeps further into many technologies of our era; 2) *organizational imperative* – the Internet has become essential for most modern companies; 3) *cyberspace domain* – this portion of our lives is now ubiquitous and pervasive and must be understood from that perspective; and 4) *national defense priority* – our potential vulnerability to cyber attacks is of increasing importance.

Focusing further on the last of these definitional forces – *national defense priority*, Agresti states:

"Progress in cybersecurity depends on attaining a richer, more quantitative, and more visually rendered understanding of cyberspace's size, scope, contours, composition, architecture, properties, traffic patterns, oversight, end points, and – ultimately – its vulnerabilities to malicious activities.

"The national defense sector faces the entire spectrum of security challenges: defects and malicious code in software on individual workstations, insider threats, vulnerabilities in networks, malicious intent, and attribution." (Agresti, p. 103)

4. The cyber-security arena

In 2010, the US government received on average, 60 million attempted cyber-attacks per day. This problem is not limited to government; Facebook recently announced that it receives over 600,000 attempted cyber-attacks per day (Enzer, 2011) although this is small compared to their one billion daily logins. Staggering as these numbers are, they show the volume of attacks that companies and even individuals now face while connected to the Internet. Managers, IT professionals, and IT security professionals must take a holistic view of security in their planning. This is crucial if a company is to survive amidst today's onslaught of cyber-attacks.

The cyber-security arena has expanded dramatically. Cyber-security now includes mobile phones, embedded computers (widely employed in our infrastructure), cloud computing,

and all types of data storage. And cyber-crime has become a business, operating without borders, and has become increasingly difficult to arrest (BCS Security Forum, 2010).

5. The motivation for cyber attacks

An important question to ask IT professionals is how they would make a system completely secure from any and all attacks. The authors have done this in a number of settings, and have observed that many individuals reach the conclusion that disconnecting all network interfaces and powering down the system is the only way to ensure security. However, physical security – when viewed as a component of cyber-security - suggests that the only true way to be totally secure is to not exist in cyberspace at all!

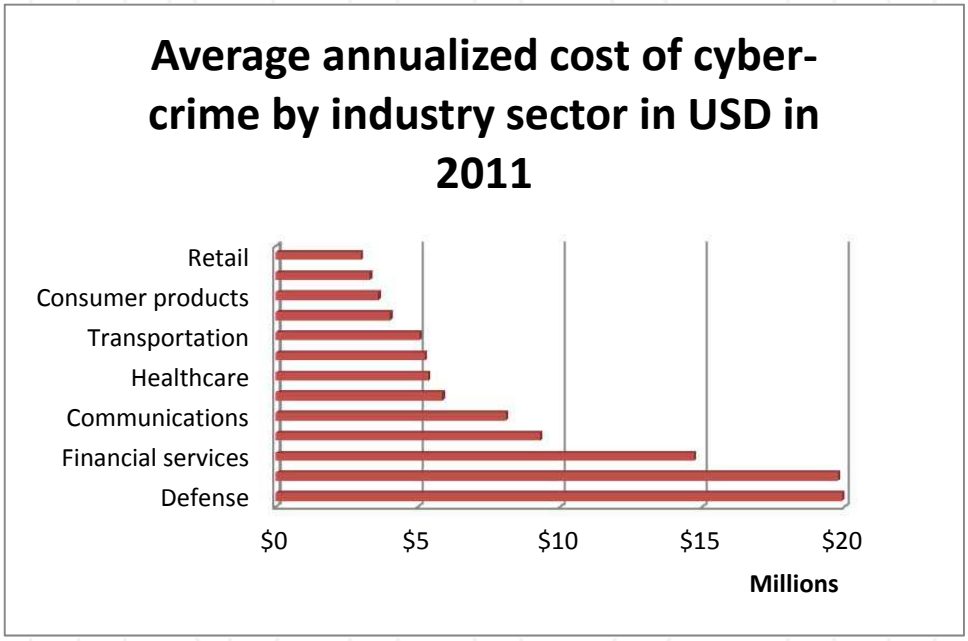


Table 1. Cost of Cyber Crime. Data sourced from the 2011 Ponemon Institute Research Report

The point of this discussion is to illustrate that every system is a target. Information is one of our most valuable assets and wherever it is stored, transmitted or processed it becomes a target for cyber-attackers. In November 2011, the US Office of the National Counterintelligence Executive drew significant media attention for their 2009-2011 congressional report which reported the headline "Foreign Spies Stealing US Economic Secrets in Cyberspace". (Security Counterintelligence, 2011). The 31-page report is rife with examples of industrial espionage by foreign state actors using a variety of cyber-attacks. Among the responses from the accused, the Chinese government pointed out the West's

tendency to outsource information technology projects to Asia. This tit-for-tat accusation and response is by no means a recent development, with China and Russia frequently mentioned in counterintelligence reports over the last twelve years (ibid).

Very few press reviews of the preceding congressional report covered the alarming discussion of a growing number of other unnamed countries, as well as activist and terrorist groups, who are increasing in their cyber-attack capabilities. Today we see an evolving marriage of capability and intent from groups with far more sinister objectives than espionage. Some of these groups have sought to wreak havoc and damage critical infrastructure and have shown no aversion to the taking of human life.

Until recently, the principal threat to the private sector has been from 'traditional hackers' – skilled individuals seeking information freedom, money or fun, and 'script kiddies' – using tools created by others primarily for personal entertainment. The aforementioned events and reports indicate a very obvious shift of intentions. The cost-to-benefit tradeoff of a successful cyber-attack, and the availability of the internet as a delivery mechanism, effectively arms the masses. With the right skills, anyone, anywhere, can launch a potentially devastating cyber-attack. Several of these attacks were discussed in a recent whitepaper that analyzed the cyber-attack capabilities and vulnerabilities of Libya under the anti-Gadaffi uprising (CSFI, 2011). For example, a SCADA targeted cyber-attack against Libya's oil refineries could limit Gadaffi's funding, but risks severe economic damage to already-struggling countries such as Italy and Ireland who are dependent on Libya for most of their oil.

In the last few years, studies have highlighted the vulnerability of critical infrastructure to cyber-attack. Nuclear plants, electric smart-grids, gas pipelines, traffic management systems, prison systems, and water distribution facilities have all been identified as at risk from a cyber-attack. Fortunately at the time of this publication, actual attacks like these remain the subject of academic discussion. Many security analysts fear this situation will be short-lived.

It should be clear by now that there is no such thing as an uninteresting target for cyber-attackers. We know that certain industries and organizations may be targeted more persistently and receive more attacks than others, but should realize that every system and organization is at risk. Understanding the motivation an attacker may have to attack our systems can help us to be more prepared for the eventuality of an attack.

In summary, the motivation for cyber-attacks may include:

- Intellectual property theft
- Service disruption
- Financial gain
- Equipment damage
- Critical infrastructure control & sabotage
- Political reasons
- Personal entertainment

In the next section, we shall see how recent cyber-attacks are being targeted to realize these objectives and describe their potential impact to information systems and organizations.

The actors that typically have these motivations can be categorized as: organized groups; loosely-organized groups; and lone wolves. These categories are points in a continuum.

An example of an organized group would be the espionage organization of a nation (such as the CIA); an example of a criminal organized group would be the Russian Business Network. These groups are typically highly organized, they pursue specific objectives, and they are well funded.

More recently, there has been a surge in the category of loosely-bound groups with varying motivations. Some of the best-known of these groups include Lulzsec and Anonymous. Collectively these groups are responsible for dozens of the highest-profile attacks in recent times (Wikipedia, 2012). Indeed, many of the aforementioned attacks against Sony came from one of these groups (Security Curmudgeon, 2011). Their targets range from governments, to corporations, to religious institutions (to date having hacked the Vatican twice). Self-labeled as part of the 'Antisec' movement, they encourage other groups to join their cause and represent a politically and geographically diverse group of individuals with skills ranging from basic script kiddie, to more advanced exploitations. Recently, a new group known as The Consortium (BBC News Technology, 2012) claimed affiliation with Anonymous in a hack against a pornography website resulting in the loss of subscriber information. While some may argue that these groups have political motives, it appears that they seek organizations with a low-security profile to publically embarrass at every opportunity.

A lone wolf or solo hacker, often incorrectly stereotyped as a basement-dwelling spotty teenager, can in some instances pose an equal threat. An example of the lone wolf includes the case of the Scottish systems administrator, Gary McKinnon, and is perhaps one of the more famous of these. Driven by self-curiosity he hacked into multiple US government agencies before being apprehended (Boyd, 2008). Such hackers are greatly assisted by organizations or individuals that provide tools for creating malware.

6. Cyber-attack types

In a sample study of 50 organizations conducted in 2011, researchers found that on average a successful cyber-attack occurs over than 70 times per year, or on average, 1.4 times per week. This represents an increase of 44% from 2010. If this growth continues, fifteen years from now organizations will be responding to a **successful** attack every 30 minutes (Ponemon Institute, 2011).

The exact type of attack can vary in type and sophistication. Fortunately, many of these attacks are fairly simple in nature. Automated vulnerability probes along with known and recognizable self-propagating malware (worms) form the bulk of attack attempts. These are generally easy to detect and prevent using standard off-the-shelf firewalls, and intrusion protection/detection systems. The primary danger in these attacks is the noise they generate, which can make it difficult to locate the more serious threats. In excess, however, they can constitute a Denial of Service (DoS), or Distributed Denial of Service attack (DDoS), leading to a much more serious degradation of service, unpredictable behavior and even complete loss of service. Although relatively infrequent, DoS and DDoS attacks are one of the most costly types of attack.

Another type of cyber attack against infrastructure is stealing Internet access. An example of this type of security compromise is the case of Ryan Harris, the owner of TCNISO. His company produces products that enable users to steal Internet service (Poulsen, 2009).

One very successful form of attack today focuses on exploiting vulnerabilities in websites and web applications. These attacks pose the greatest danger to most organizations due to the relative simplicity with which they may be attempted and with the immense volumes of valuable information that can be stolen if successful. Many websites are connected to backend databases, which not only contain information that may be of interest to criminals, but provide an entry point into the organization's internal network. The latter form of attacks are known as pivoting attacks and enable the attacker to pivot from a principal entry point to attack other systems deeper in an organizations infrastructure. Pivoting attacks are a severe form of web-based attacks as they allow attackers to completely bypass perimeter security controls at the network edge.

Web attacks involve the attacker identifying a potential vulnerability in a web system. There are several types of vulnerabilities that allow for different forms of attacks. The most common of these are cross-site scripting (XSS) and SQL injection.

Cross-site scripting allows an attacker to plant malicious code in an organization's website and from there attack clients visiting a company's site, stealing passwords, subverting network traffic, and monitoring communications. In many instances, XSS attacks enable attackers to leverage further vulnerabilities in client web browsers to install malicious software on the visitor. Thus unknowingly a visitor of an infected site can become themselves infected, and in some instances, part of a group of infected computers known as a botnet. This form of client infection is known as a drive-by-download and is one of the principal ways attackers gain control of systems. Controlled systems can be used for a variety of purposes including sending unsolicited e-mails (SPAM), targeted cyber-attacks against organizations, and DDoS attacks. Using a victim's system to attack another victim is known as an indirect attack and can be done with relative anonymity.

The vulnerability to these type of attacks can be easily reduced by careful website programmers who include checks to validate the length of user-entered information, and remove any illegal characters. Failing to do this introduces a significant probability that the site is vulnerable to both cross-site scripting and SQL injection attacks.

An SQL injection permits the attacker to access and manipulate a backend database, revealing customer records, intellectual property and even opening routes deeper into the organization's network. Most experts agree that SQL injection attacks were used in most of the 21 independent successful attacks against Sony that occurred between 21 April and 7 July 2011 (Security Curmudgeon, 2011). Targeted attacks of this nature currently form the majority of successful cyber-attacks and are the most cost-effective for attackers.

A further category of attacks are known as Advanced Persistent Threats, or APT's. These attacks are becoming more common as attackers become more skilled, knowledgeable and resourceful in infiltrating specific networks for a specific purpose. Their title reflects the danger posed by these attacks. APT's can be technically advanced and contain advanced attack techniques, use an advanced combination of simpler attacks for a specific purpose, or

both. They are persistent, indicating that the attacker has a defined objective and often will not quit until their goal is realized. This can often lead to attacks being multi-pronged, where the organization's systems and security are studied and monitored for months before an actual attack, or series of attacks, take place. APT's pose a significant threat with a high probability to succeed and be damaging to an organization. This can indicate external funding or support that provides resources for the development and deployment of the attack.

The only positive aspects of APT's are that they are targeted against a specific organization and hence are much less prevalent than other threat types. In other terms, they are akin to the sniper who studies his prey and observes its habits. The sniper waits, sometimes for days, for the perfect moment to take his shot, with a high degree of accuracy. It is very difficult to locate the sniper before the attack, and after the attack, the damage is localized but still significant, and often costly. Non-APT attacks in contrast may be thought of as 'the shotgun approach', or 'spray and pray' tactic of many video gamers. The attacker will point in a general direction, and blast away, hoping to hit something. With enough shots, a kill is guaranteed. These attackers generate a lot of noise, and can do a lot of damage if they are lucky enough to land a hit. If unsuccessful, an attacker will often move on to another target. Success at a low cost, against any target, is more important than any specific target.

Understanding the type of attack in the context of its objective and sophistication allows those responsible for information systems to gain insight to the potential damages caused. This next section looks at some of the costs a cyber-security breach can incur.

7. Cost of a successful cyber-attack

By our nature, humankind often finds it easier to respond or retaliate than to plan and prepare. Analyzing every potential outcome of a scenario can consume significant time and resources. Surely it is cheaper to only respond to the successful cyber-attacks than commit resources to risk management and incident response?

Recent history has shown this idea to be erroneous. It is often impossible to calculate the precise damage of a cyber-intrusion. The consequences of an attack can be far-reaching and long-term. The damage may often be irreparable; no amount of money can undo what has been done. Some of the effects of a cyber-intrusion include:

- Financial loss from service unavailability
- Loss of customer/client confidence
- Market shift to competitors
- Lawsuits and liabilities from those who have had information stolen
- Cost of recovery
- Cost of security measures to prevent a repeat attack
- Cost of staff or consultants to investigate and identify the method of attack
- Fines from regulatory bodies
- Cost of informing customers of theft
- Theft of intellectual property
- Loss of human life

The effects of cyber crime are listed above. Some previous sections have said other things about cost in specific instances. Many successful cyber attacks have been widely reported in the media, yet the frequency of successful cyber attacks continues to increase, along with associated costs.

In their second annual report, the Ponemon report (Ponemon Institute, 2011) had the following key takeaways:

- Cyber crimes can do serious harm to an organization's bottom line. We found that the median annualized cost of cyber crime for 50 organizations in our study is $5.9 million per year, with a range of $1.5 million to $36.5 million each year per company. This represents an increase in median cost of 56 percent from our first cyber cost study published last year.
- Cyber attacks have become common occurrences. The companies in our study experienced 72 successful attacks per week and more than one successful attack per company per week. This represents an increase of 44 percent from last year's successful attack experience.
- The most costly cyber crimes are those caused by malicious code, denial of service, stolen devices and web-based attacks. Mitigation of such attacks requires enabling technologies such as SIEM and enterprise governance, risk management and compliance (GRC) solutions. (Executive Summary, p. 2).

The time it takes to resolve a successful cyber attack is a key factor in the cost. The sooner the organization detects, analyzes and contains the attack, the lower their recovery and post-recovery costs will be, and the lower the overall cost will be. Therefore, it is important that all organizations constantly be on the alert against cyber attacks.

Table 2, taken from this Ponemon report, gives the average annualized cyber crime cost, weighted by the attack frequency. While the institutions studied in this report are not necessarily representative of the industry as a whole, the data are highly informative.

Type of Attack	Average Annualized Cost
Denial of service	$187,506
Web-based attacks	$141,647
Malicious code	$126,787
Malicious insiders	$105,352
Phishing & social engineering	$30,397
Stolen devices	$24,968
Botnets	$1,727
Malware	$1,579
Viruses, worms, trojans	$1,517

Table 2. Types of attacks and their associated costs (Ponemon Institute, 2011).

Table 1 includes only the direct costs. There are also indirect costs, including increasing frustration on the part of computer users, increased time spent on working with necessary security measures, lost business opportunities, and a tarnished reputation.

Worldwide, cyber crimes have cost in the neighborhood of $388 billion in 2010, according to the 2011 Norton Cybercrime Report (Norton, Inc., 2011). This figure includes both direct and indirect costs, and is a staggering amount. And unfortunately, this figure has only been increasing for the past several years, with no sign of major improvement.

8. Interested parties

The list of interested parties has grown in direct proportion to the number of connected entities. It would probably be much easier to list those who need not be concerned with cyber crime, because IT has become an integral part of companies, government agencies, the military, our infrastructure (including water, electricity, roads, bridges, natural gas, etc.), health care, research, and our personal lives, and because a very large portion of all IT is now connected via the Internet. Anyone who has any device connected via the Internet – and this includes cell phones, MP3 players, computer gaming equipment, and ALL forms of computers – anyone with any of these devices should be concerned about cyber crime. All of these devices have fallen victim to cyber crime, and it is unlikely that this will change.

Perhaps the parties most difficult to convince of this are the general public. Only a small percentage of the population is deeply aware of how easily the security of their connected devices can be compromised. And because only a small percentage are affected by cyber crime each year, the general public remains relatively uncommitted to deploying the latest and best security software. And as long as this remains true, it is inevitable that cyber crime will continue to increase.

9. Outstanding issues

The most difficult issue in any defensive endeavor is knowing what to defend against. One of the most famous large investments that failed to protect against the real risk was the Maginot line. It was a set of fortifications and tank obstacles designed to give the French time to mobilize. The line proved useless for defending France because the Germans simply conquered Belgium and went around the defenses. This led to the adage that "generals always fight the last war, especially if they have won it" (Kemp, 1988). Unfortunately there are numerous examples of companies that sit behind their line of firewalls believing that they are safe while the enemy simply goes around their defenses.

The canonical example of this class of problem in cyber-security is called a “zero-day exploit”. An exploit is actual code that acts on a vulnerability or combination of vulnerabilities. A zero-day exploit is an exploit that takes advantage of vulnerabilities that are unknown or considered to pose insufficient risk to worry about; then a malefactor figures out an automated exploit and hundreds or thousands of computers are compromised in a few hours. The computers join a botnet. We can see that an opponent that

exploits a vulnerability the first time has the advantage of surprise. No matter how rapid the response by software developers and security vendors to a zero-day exploit, the black hats have a significant window of opportunity to attack vulnerable systems until a remediation and/or a signature for the malware is deployed to the defenses on the platform. Cyber-security will always be a race between malefactors who want to compromise systems and the vendors, developers, and legitimate users of computing systems who want to secure their systems.

A major hurdle is that decision makers often think like the French government before WWII, they think their large investment in firewalls will protect them while the reality is that new software and hardware are continuously being deployed to add functionality and remediate vulnerabilities and no static defense can provide protection in a dynamic environment. Experience teaches that the fixes often create new vulnerabilities. At the same time malefactors are continuously searching for vulnerabilities and creating exploits for the vulnerabilities that they isolate. Thus the problem becomes one of continuously defending a relatively slowly changing target from an unknown, rapidly moving and evolving attacker.

In the current world of IT, attackers have a huge advantage. The majority of machines deployed in businesses and homes run the same platform software. Microsoft platforms got the reputation for having poor security because their platform provided a large set of targets that made the value of an exploit much greater. Finding vulnerabilities and developing exploits is a technically demanding and uncertain process. A large monoculture to attack provides the incentive to invest in exploits. There is now an active underground market in zero-day exploits that are sold to the highest bidder. An active market provides incentives for skilled individuals to invest time and expertise to create "products" that are in demand.

10. Implementing security

A likely question at this stage is what can be done? How can we realistically and affordably protect our information under this continuous barrage of attacks? Often in these circumstances, managers may find themselves facing the responsibility to choose between large numbers of different technology-based solutions. This can quickly overwhelm, and actually create more problems than it solves. In order to implement effectual security controls, we must first understand the risks posed by different threats to our business model.

There is no shortage of security frameworks for analyzing risk and implementing security controls, and plenty of excellent books for a variety of audiences on this topic. For the purposes of this chapter, we shall present security implementation from a greatly simplified model that should enable an organization to effectively prepare and respond to security threats.

The Cyber Security space can be broken down into three areas, or domains. These are:

- Prepare
- Defend

- Act

These domains should not be seen as sequential steps in which each is terminated prior to the commencement of the next, but rather three continual processes that form the foundation of organizational security.

10.1 Prepare

Preparation includes planning, risk assessment, policy, business continuity planning, countermeasure deployment, training, education and accreditation. These are all essential in optimizing our readiness for cyber attacks.

Accreditation is a particularly interesting term in this context. Security accreditation is management acceptance of the risks associated with a system. This is no small responsibility in the event of an attack. To increase assurance and reduce associated risk, a thorough penetration test should be carried out as standard part of an accreditation process. Conducting a penetration test is effectively paying someone to hack your organization's systems. A skilled penetration tester will be able to locate vulnerabilities and advise on cost effective ways to reduce their risk. Organizations should be careful of individuals marketing themselves as penetration testers without the appropriate skills. A tester should carry recognizable certifications (GIAC, CEH, etc.) and be a member of an accredited or approved organization (such as (ISC)2) that requires a member code of ethics.

After the test, a report should be provided which will indicate the specific vulnerabilities found with suitable fixes, and recommend process improvements that will reduce the risk of future vulnerabilities going unchecked.

10.2 Defend

In the context of defending against cyber attacks, defensive processes include ongoing risk mitigation, service and device hardening, and incident detection. A recent study (Schwartz, 2011) showed that up to 96% of organizations are unaware they have been hacked. Believing themselves either untargeted or immune to cyber attacks, they remain blissfully ignorant of information theft, espionage and other malicious attacks taking place right under their noses. Organizations must ensure, at a bare minimum, that they are able to detect security incidents when they occur. To fail in this opens the door to potentially expensive lawsuits and even criminal proceedings depending on the type of information that has been lost.

10.3 Act

Finally, we should establish procedures and protocols to ensure that in the event of an incident we act appropriately. We avoid the use of the term 'react', as it tends to carry a negative connotation of a knee-jerk 'reaction' that is ill conceived and inflammatory. Actions in response to a cyber-attack should be carefully planned to facilitate the effective response that minimizes expense and collateral damage. The word act is hence deliberate and suggests that organizations should be proactive rather than reactive.

The continual application of these three domains cannot be emphasized enough. External consultants who are experienced, certified security professionals can be invaluable resources in maintaining an effective cyber-security posture and ensuring our businesses remain unhindered by an attack they were unprepared to handle.

11. Current research

Historically the attackers have also had the advantage that the majority of home PC owners and many businesses have been lax in applying fixes and upgrading their platform software. Thus attackers can have years to find and exploit vulnerable machines. Buffer overflow and other code injection attacks often depend on the static layout of the code and data in memory for their effectiveness. Historically network risks were mitigated by building a fortress around systems. This approach led to network architectures with components with names like DMZ (Demilitarized Zone), a boundary location that has both public and private addresses so that "bastion hosts" could be hardened to live in the DMZ while normal systems would be deployed behind the "firewall". This provides a static environment that allows an attacker almost unlimited time to search for a vulnerability in the attack surface. The advent of APT attackers that patiently probe for years against a target of particular interest make these fortress designs vulnerable. Just as WEP-based wireless networking was vulnerable to attack because it used static encryption keys, static networks that can be mapped over time are more vulnerable than more dynamic designs.

In order to defeat these threats in a slowly evolving infrastructure, some new products and research results demonstrate that significant gains in security can be achieved by adding random dynamic behavior to systems. Starting with Windows Vista and improved in Windows 7 and Server 2008 SP1, the operating system loads the parts of the operating system into different random locations every time it boots (Microsoft, 2011). Microsoft does not claim that this eliminates the threat of attacks - it just makes it significantly more difficult.

Vendors have begun to sell network appliances that randomize the footprint of the network by using Network Address Translation (NAT) technology and randomizing outbound connections over a set of IP addresses, as well as other dynamic behavior (Masking Networks, 2011).

The military is looking at many similar approaches to improve the security of its networks, especially combat control systems (Baker et al, 2011; Jones, 2011; Okhravi, et al, 2011; Wright, 2011). In November 2011, the Defense Advanced Projects Research Agency (DARPA) announced plans to increase cyber-security research by 50% (Hoover, 2011).

The next generation of networks may be significantly more robust, as could hardware and software systems. This will probably be accomplished by introducing more and more random behavior into the operational characteristics of systems which will overcome many of the disadvantages of our current environment of the majority of systems being identical platform software deployed on identical hardware connected in static networks

running on a single vendor's equipment (Jajodia, et al, 2011). Much will depend on decision makers recognizing the threats and being willing to invest both intellectual and financial capital in understanding the risks and applying appropriate defensive technologies.

12. Conclusion

At this point in time, the outlook for cyber security is not as rosy as the authors would prefer. Attackers continue to find new ways to exploit weaknesses, while developers continue to fix the known problems and attempt to develop new operating systems and applications with fewer vulnerabilities. Because there is very ample motivation (the chance for success is high), and because the possibility of being caught is relatively low (the risk is not terribly high), the area of cyber security continues to attract many black hats with many motivations.

In many senses, it is just like physical (aka "kinetic") warfare. As soon as one side develops a new weapon, the other side begins to develop a counter-weapon or a work-around. Additionally, the more aggressive side continues to probe the target for all possible points of weakness, and exploits these weaknesses when found. History has shown that this cycle of probing, exploiting, developing, and counter-developing can continue *ad infinitum*. Our belief is that the white hats will continue to make life in the cyber-world tolerable, minimizing risk and continuing to make improvements that provide major advantages to offset the associated problems. It will take a great deal of effort by many parties to keep cyberspace widely useful.

13. References

Agresti, William W., "The Four Forces Shaping Cybersecurity", *Computer*, Feb 2010, pp 101-104.

Baker, Jill, et al., "Winning in Cyberspace: Air Force Space Command's Approach to Defending the Air Force Network", *High Frontier*, v 7 #3, May 2011.

BBC News Technology, "Porn site breached in hack attack", Mar 12, 2012, http://www.bbc.co.uk/news/technology-17339508.

BCS Security Forum, *ISNOW*, Winter 2010, pp 6-13.

Boyd, Clark, "Profile: Gary McKinnon", BBC News, July 30, 2008, http://news.bbc.co.uk/2/hi/technology/4715612.stm.

CSFI (Cyber Security Forum Initiative), "Project Cyber Dawn – Libya", Apr 17, 2011, www.unveillance.com/wp-content/.../Project_Cyber_Dawn_Public.pdf.

Enzer, Georgina, "Facebook unveils extent of cyber-attacks on site", *ITP.net*, Oct 30, 2011, http://www.itp.net/586887-facebook-unveils-extent-of-cyber-attacks-on-site.

Greene, Tim, "Cybercrime costs rival those of illegal drug trafficking, *Network World*, Sept 7, 2011, http://www.networkworld.com/news/2011/090711-cybercrime-250580.html.

Hoover, J. Nicholas, "DARPA Boosts Cybersecurity Research Spending 50%", Information Week, Nov 7, 2011, www.informationweek.com/news/government/security/231902495.

Jajodia, S.; Ghosh, A.; Swarup, V.; Wang, C.; Wang, X.S. (Eds.), Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats Series: Advances in Information Security, 1st Ed, 2011.

Jones, Andrew T., "Preparing the Air Force for Computer Network Operations", *High Frontier*, v 7 #3, May 2011.

Kemp, Anthony, *The Maginot Line: myth and reality*. Military Heritage Press. p. 14, 1988

Kroll (2010). Global Fraud Report. Global Fraud Report - Annual Edition. USA, Kroll Consulting.

Masking Networks, "Network Address Vulnerabilities", white paper 2011, http://www.maskingnetworks.com/network-masking-technology/network-address-vulnerabilities

Microsoft, "Microsoft ASLR: Loading DLLs at a different location every boot", Feb 9, 2011, http://blogs.technet.com/b/virtualization/archive/2011/02/09/windows-7-and-windows-server-2008-r2-sp1-add-new-virtualization-innovations.aspx

Morningstar, Chip and F. Randall Farmer. The Lessons of Lucasfilm's Habitat. The New Media Reader. Ed. Wardrip-Fruin and Nick Montfort. The MIT Press, 2003. 664-667.

Norton, Inc., "Norton Cybercrime Report", 2011, http://www.symantec.com/content/en/us/home_homeoffice/html/ncr/.

Okhravi, Hamed, et al., "Achieving Cyber Survivability in a Contested Environment Using a Cyber Moving Target", *High Frontier*, v 7 #3, May 2011.

Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies", Aug 2011.

Poulsen, Kevin, "Feds Charge Cable Modem Modder With 'Aiding Computer Intrusion'", Wired, Nov 2, 2009.

Schwartz, Matthew J., "Most Businesses Don't Spot Hack Attacks", *Information Week*, Oct 5, 2011; www.informationweek.com/news/security/attacks/231900054.

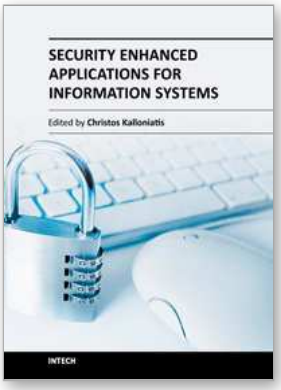
Sebastien, M. (2011, 25 May, 2011). "Infrographic: Cost of Sony's data hack could reach $24 billion." PR Daily. Retrieved 9/13/11, from http://www.prdaily.com/Main/Articles/Infographic_Cost_of_Sonys_data_hack_could_reach_24_8359.aspx.

Security Counterintelligence, Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011", Oct 2011.

Security Curmudgeon, "Absolute Sownage: A concise history of recent Sony hacks", June 4, 2011, http://attrition.org/security/rants/sony_aka_sownage.html.

U.C. Office, London, "The Cost of Cyber Crime", 2010.

Wikipedia, "Timeline of events involving Anonymous", http://en.wikipedia.org/wiki/Timeline_of_events_involving_Anonymous.
Wright, John D., "Air Force Cyberspace Strategic Planning Factors", *High Frontier*, v 7 #3, May 2011.
YouTube, http://www.youtube.com/watch?v=h2br2_twHfw, 2010



Security Enhanced Applications for Information Systems

Edited by Dr. Christos Kalloniatis

ISBN 978-953-51-0643-2
Hard cover, 224 pages
Publisher InTech
Published online 30, May, 2012
Published in print edition May, 2012

Every day, more users access services and electronically transmit information which is usually disseminated over insecure networks and processed by websites and databases, which lack proper security protection mechanisms and tools. This may have an impact on both the users' trust as well as the reputation of the system's stakeholders. Designing and implementing security enhanced systems is of vital importance. Therefore, this book aims to present a number of innovative security enhanced applications. It is titled "Security Enhanced Applications for Information Systems" and includes 11 chapters. This book is a quality guide for teaching purposes as well as for young researchers since it presents leading innovative contributions on security enhanced applications on various Information Systems. It involves cases based on the standalone, network and Cloud environments.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821