Global Information Assurance Certification Paper

Ghosts in the machine: The who, why, and how of attacks on information security

Cary Barker
GIAC Security Essentials Certification (GSEC)
Version 1.4b (Option 1)
Dec 26, 2002

> "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat."
> –Sun Tzu, The Art of War

Abstract

Information Security is the field devoted to maintaining the confidentiality, integrity and availability of information [Harris]. Organizations from small home offices to multinational conglomerates have information that needs protected, not to mention the secrecy needs of nations and the bureaucracies that govern them. Billions of dollars are spent to provide the needed security every year. But who are we protecting ourselves against? What is the threat we face? Why are we being attacked? How can we use this knowledge to protect ourselves?

To better secure an organization, one should know something about the opposition. To provide the best security one, needs to know the enemy: who they are, why they are attacking, and how they attack. Even better would be using knowledge of the adversary to develop better defenses against such attacks.

Part 1: Know your enemy

'Know thy enemy' is the first commandment of Information Security. To defend an organization from attack, one should know who they are defending themselves against. Without knowledge of the adversary it is easy to be caught off guard, to be ill prepared and unsure of how to react to a threat. In order to increase that understanding the next section describes the varieties of adversary that may attempt attacks against your organization's information security. Some of them may not appear to specifically apply to your organization, but keep an open mind and read on – people you may not perceive as a concern may be more of a threat than you think.

The Who, the Why and the How

First I will describe the types of adversaries, then their motivations, and finally their methods. Keep in mind that only common adversaries, motivations, and methods are described - there are many more possibilities that could easily fill a book.

The Who

The types of attackers vary as much as their motivations and methods. They may be young or old, male or female, domestic or foreign. The similarity they all share is the desire to compromise some aspect of information security; whether it is by wiping out files (deletion), modifying information (alteration), or rendering it

inaccessible (denial of service). What follows is a list of the common types of attackers along with a description of their capabilities and the degree of destructive tendencies. Included with the descriptions are documented examples of clashes with these individuals and Information Security professionals, the police or government.

i. **The Explorer**

Some intruders just want to know how things work. While these people are mostly curious, it doesn't keep them from being potentially dangerous. Who knows what they may break/alter/delete in their explorations (although a more knowledgeable explorer will leave no trace and alter only enough to keep others from noticing their intrusions). The term 'Hacker' was originally used to describe these people, but the popular press has changed the meaning of 'hacker' to a blanket term for 'computer attacker'. The line from *The Conscience of a Hacker*, "My crime is that of curiosity" [Blankenship], sums up the description of this kind of individual.
The most famous example of an explorer would be Kevin Mitnick. He became involved with breaking into telephone networks in high school while living in Las Vegas. Over a period of years he grew to use a variety of tactics to gain access to various telephone companies and computer networks. Eventually his escapades drew the attention of local authorities and he was arrested . . . several times. In 1995 (while hiding from the FBI) Mitnick broke into Tsutomu Shimomura's computers. Shimomura became interested in the attack and tracked similar intrusions around the country. Finally the FBI, with the help of a Sprint cellular engineer and Shimomura, tracked down and arrested Mitnick by tracking his cellular phone use [Mitnick p3-4]. His reasoning for everything he did was a mix of curiosity and a superiority complex – he claimed he just wanted to know how things worked and to be able to best any type of security he encountered.

ii. **The Disgruntled Worker**

Past and present employees can cause massive amounts of damage to information systems, networks, and information security. Their knowledge of company policies, procedures and practices enable them to commit malevolent acts often without arousing suspicion. Past and present employees know best how to cause the most damage to a company. The damage can be done in many ways, but they all work by breaking one corner of the information security triangle: Confidentiality, Integrity, or Availability. With the aid of computers and the Internet, this damage can be done at a distance, thereby limiting the risk to the disgruntled employee by allowing him or her to remain anonymous [Mitnick p161].
An example of the disgruntled worker comes straight out of the news. In May of 1999 a list consisting of 116 names of spies and other intelligence officials working for MI6 was published on the Internet. The list was allegedly posted by Richard Tomlinson, a disgruntled former MI6 operative. Tomlinson had been dismissed from the MI6 in 1995 and had

been threatening to release sensitive information after an appeal failed. What makes this example stand out is that despite a British government issued 'D-list' gag order to the press and an injunction against several ISPs (to suppress the information), the list not only got out, but it spread through USENET newsgroups like wildfire. The end result was that the lives of several spies were put in jeopardy and the British intelligence service was set back several years in intelligence gathering capabilities [Ingram].

iii. **The Spy**

Spying is largely ignored by most US companies; however, foreign competitors and foreign governments seldom hesitate to spy on us or each other. To complicate matters, intelligence agencies that used to spy on other countries during the cold war have been repurposed. These agencies now commonly steal secrets from foreign competition and pass them on to domestic companies. Couple this with the fact that some multinational companies have intelligence divisions that are larger than some nations and the problem becomes apparent. Spying costs US companies billions each year. Why are US companies such a target? First, the US has some of the best technology in the world. Foreign companies (and foreign intelligence agencies) make the simple decision that it is cheaper to steal the technology than to spend the money to develop it themselves. Second, spying is not looked down on in other countries the same way that it is in the US. Most foreign intelligence agencies pass on industrial secrets they gather as a matter of course to their domestic corporate constituents. The laws governing foreign intelligence agencies are also different. The CIA is prohibited from giving industrial, commercial, or technical secrets it obtains to domestic companies while the French DGSE goes out of its way to steal secrets from American companies and give them to domestic French and especially French government owned companies.

Another problem with Spying is that countries that are thought of as allies have been stealing secrets from American companies for many years. A GAO report titled "Economic Espionage: Information on Threat from U.S. Allies", said the following about the problem: "The lessening of East-West tensions in the late 1980s and early 1990s enabled . . . intelligence services to allocate greater resources to collect sensitive U.S. economic information and technology." [Gao] Until recently, government knowledge of this spying had been a dirty little secret that got swept under the carpet in the interests of maintaining a coalition against Communism during the cold war. As evidenced by the GAO, the stance of ignoring friendly spies seems to be quickly changing as economic competition replaces military competition in the global economy. However, many in the intelligence community believe that American companies remain extremely naïve when it comes to espionage. American institutions continue to have their hard-earned secrets stolen at an alarming rate. For further review,

Appendix A contains a list of the most active intelligence agencies along with a quick description of their activities.

There are many examples of corporate espionage from which to draw. The most audacious example comes from the French-government owned company Cie. des Machines Bull. Bull, partly owned by the French government, had fallen on tough times by struggling to compete with IBM, Texas Instruments and other American companies. In order to help the foundering domestic company, the French secret intelligence service (the DGSE) hatched a scheme to steal promising technology from the most prominent US companies. IBM, Texas Instruments, and Corning were selected by the DGSE for their leadership in chips, computer technology and fiber optic cabling. For over a decade the DGSE supplied Bull with technology obtained by spies and moles inside the three companies. Things eventually got to the point where Bull sued Texas Instruments for infringing on patents. The irony was that these patents were filed using stolen research from none other than Texas Instruments itself! Texas Instruments (unaware of this) was fully prepared to settle with Bull when the FBI arrested some TI employees for participation as DGSE spies. When the truth came out, TI produced documents accusing Bull of obtaining the stolen secrets. As a result, Bull quickly changed heart and settled the case out of court. Because of the magnitude of the DGSE spying operation, officials from both the FBI and CIA went to France to confront the DSGE over the matter. The end result: Several employees who were passing information were fired; the French government issued an apology; and Pierre Marion, the head of the DGSE, said this: "This espionage activity is an essential way for France to keep abreast of international commerce and technology. Of course it was directed against the United States as well as others. You must remember that while we are allies in defense matters, we are also economic competitors in the world." [Noland]

iv. **The Terrorist**

While terrorist use of the Internet for attacks on Information security has not publicly happened, concern has risen greatly since the events of Sept. 11. Experts warn that terrorists are taking a great interest in computers and their use as a tool for carrying out terrorist attacks. As evidence, the FBI reported that a captured Al Qaeda laptop "contained [computer] models of a dam. . . Microstran, an advanced tool for analyzing steel and concrete structures; Autocad 2000, which manipulates technical drawings in two or three dimensions; and software used to identify and classify soils, which would assist in predicting the course of a wall of water surging downstream."[Barker] Separately these programs are fairly harmless, but together they suggested more sinister use. This example also illustrates another important point: information not directly sensitive to your company could still be used in an attack.

v. **The Thief**

Money motivates people. When an easy way to get money comes along, people will take advantage of it whether it is legal or not. Thieves attack information security in many ways, from stealing credit card numbers on an e-commerce site to breaking into bank computers and re-routing money to offshore bank accounts. Also, attacking information security for theft is by no means limited to computers. The following example shows how a thief stole millions from a bank by using a little social engineering: In 1978 Stanley Rifkin, who worked at the Security Pacific Bank, managed to get a look at the security codes in the wire transfer room while performing some other duties. Upon seeing the codes, Rifkin came up with a scheme to retire a little early. After careful planning, including setting up an overseas bank account, Rifkin decided to set his plan into motion. One day after performing some duties in the wire transfer room, Rifkin managed to again get a look at the security codes used for wire transfers. After finishing his job for the day Rifkin walked to a pay phone in the bank's lobby and made a call to the wire transfer room. He impersonated a bank manager and placed an order for a wire transfer – to a numbered Swiss bank account in his name. Rifkin was asked for the security code, which he gave. After thanking the teller and hanging up, Rifkin walked out of the bank and into legend - ten million dollars richer [Mitnick pp 4-6].

vi. **The Hactivist**

Hactivism is mostly considered a 'cyber' form of activism. The term was originally coined to describe protestors of the government in southern Mexico who defaced, crashed or DOSed government servers to call attention to their cause [ISN]. Hactivists make a political, social, or environmental protest through hacking. Generally their protests are limited to web page defacements, but they can quickly escalate. Examples of hactivism include:

- DDOS attacks against the RIAA in protest of RIAA-centric laws being passed;
- US government web page defacements and other cyber-attacks in response to the 1999 accidental bombing of the Chinese embassy in Belgrade [Kellan];
- Anti-globalization protestors hacking into the WTO during its 2001 conference. Hactivists stole then published private information on prominent members and attendees [ISN].

vii. **The Script Kiddie**

Script kiddies are people who use scripts or other automated attack tools without understanding how they work or what they are doing. Script kiddies are not very knowledgeable. They may not even know or understand how to use unauthorized access once they have it. They also have a tendency of failing to cover their tracks. A script kiddie's main

protection is the fact that their commonness makes prosecution unfeasible, and the tools they use are far more advanced than the kiddie using them [Jargon].
Sometimes one 'cracker', an unethical hacker, with more knowledge will have a small gang of script kiddies exploiting vulnerabilities and collecting a harem of 'owned' or compromised computer systems. The cracker acts as the leader, guiding and directing the group. These systems are then used for DDOS attacks or as jumping points for obscuring the source of a more complicated attack.
The examples of script kiddies and their escapades are numerous. They are remarkable only in the fact that they consistently are able to 'hack' sites of the most prominent companies today. A steady stream of companies like Intel, HP, The New York Times, Yahoo, eBay, and more continually have to deal with web-page defacements and DOS attacks. The main difference between a common vandal and a script kiddie, is that when the kiddie defaces a company's page everyone, in the world can see it, much to the embarrassment of the victim.

viii. **Hacker for Hire**

There are two kinds of hacker for hire. One type, commonly called a 'sneaker,' can be hired for ethical hacking. The other is the mercenary hacker, or hacker group. Here we are concerned with the mercenary hacker. The mercenary hacker can have a range of abilities; but nearly always this hacker has a history of being an 'explorer,' often has some social engineering abilities, and may have great skill in compromising Information Security through computer based attacks. Mercenary hackers range from Private Investigators who are hired to dig up dirt on other people to full fledged evil geniuses who sell their services to companies by exchanging stolen secrets for large sums of money. [Salkever]

ix. **The competition**

Rival companies in an ever more competitive industry, like high-technology, frequently attack each others' information security. As mentioned before in the case of Cie. des Machines Bull and Texas Instruments, companies often obtain stolen secrets from each other. Attacks can range from gathering embarrassing information, such as Oracle paying a PI to look for dirt on Microsoft [Edwards], to stealing an entire manufacturing process. Also, contrary to popular belief, many view the best targets to be small companies: small companies have innovative ideas, weak security, and few resources to combat an attack [McDermott].

x. **Enemy countries** (as part of Information Warfare).

Information warfare is not commonly a concern; however, its capabilities are being actively developed by several countries, including China. It is not fully known what the effects of an all out cyber-war would produce, but a safe bet would be a world-wide economic downturn after effected

companies, infrastructures, and financial systems would begin to fail. Information Warfare targets a nation's infrastructure as well as its economy, making any associated organization or company a target. Limited information warfare took place during the 1999 NATO-Serbia conflict and China-Taiwan tension the same year. The reason I say limited is because little or no official government involvement occurred in either case. In both cases attacks were limited to individual hackers breaking into web sites and releasing viruses against the other side [Hacker]. Using these two limited cases as examples, one can only guess at the destructive capabilities of a true military coordinated InfoWar attack.

xi. **Summary of the 'Who'**

People from all walks of life are involved in attacking information security. The old generalization that attackers are overweight teenagers with no friends and a lot of time does not hold true. Attackers may even live half a world away from their intended victim. Attacker's motivations vary from the benign to the horrific. You may not understand their culture; therefore, their motivation may be irrational and alien to you. With this in mind, it's important to know their motivations as best as possible - the 'why' motivating them.

The Why

The next section explores the psychology and motivations behind an attack. Understanding an attacker's motivation provides insight into how and what will be attacked. By using an understanding of the possible threats, a more comprehensive plan can be developed for protecting information assets.

a) **Money**

Money has been involved with the bulk of attacks on information security. Money is the most common way corporate and military turncoats are recruited for stealing secrets. Of the many cases of employees selling out corporate secrets, money has been the reason predominate behind their actions (even though spying, for some countries like Russia, has a history of paying very little considering the risk spies take). Other motivations involving money include extortion, defrauding, and personal financial problems as discussed below.

Extortion

It has become rather common to have data stolen and then have a threat made that the data will be released to the public. The most popular information to use for extortion seems to be customer credit-card numbers. The reason for extortion is simple: money, and lots of it. Perpetrators can make millions from a company by threatening to release its secrets. Compounding the problem, victim companies are unlikely to take the problem to law

enforcement. There are several reasons companies want to keep blackmail secret:

- The possibility that information will be released if law enforcement is involved;
- The fear of consumers loosing faith in the company if the problem is made public. Lost consumer trust in the company can cost more than paying off the attacker;
- Embarrassment and liability should the public be made aware of poor security practices. Once again it may be cheaper to pay off an attacker than face litigation from civil suits if the incident went public.

Attackers know that companies are reluctant to make blackmail public and use that reluctance to their advantage. The simple reasoning is that the victim wants the attack kept secret more than the attacker wants to avoid involvement of the law. There are a few examples of companies that made the threat public. The most notorious of these is the case of two Russian hackers.

For months during 1999 and 2000, Vasiliy Gorshkov and Alexey Ivanov ". . . cracked into victims' computers to steal credit card information and other financial information prior to attempting to extort money from the victims with threats to expose the sensitive data to the public or damage the victims' systems."[Leyden] The pair of hackers was so bold that they even e-mailed a resume including pictures to one of their victims, who refused to pay them $5,000. The victim, an ISP called Speakeasy, went to the FBI because of the threats and attacks, which had escalated into a daily occurrence [Ingalls]. Using information provided by Speakeasy and other tips, the FBI built a case and a plan to catch the two. The FBI created a dummy security company and contacted Ivanov and Gorshkov for a job interview in the states. Thinking they were going to get a great job in computer security, they came for the interview and were promptly arrested after demonstrating their abilities to undercover FBI agents. Ivanov and Gorshkov were convicted in 2002 of no less than five counts of extortion and more than 20 counts of conspiracy.

Defrauding

Other common money schemes are identity theft and misuse of access or information. Defrauding can be done very easily using the internet or by someone 'inside' a company. The most popular form of defrauding people is using stolen credit card numbers for purchases. This problem is expected to mushroom as companies rush to offer more goods and services over the internet without first implementing proper security mechanisms.

Financial problems
Financial problems and personal greed are common personal weaknesses used by attackers to compromise information security. Gambling problems, deteriorating credit, and other financial difficulties lead otherwise law abiding people to become moles, spies, or outright information thieves. This is so well known that knowledgeable attackers will identify and attempt to recruit individuals with financial problems in a target company. Most of the individuals recruited for spying today have financial problems or are disgruntled workers. They are lured into becoming spies with promises of lots of money. Once they start passing on information, they are frequently unable to stop due to the ability of the 'handler' to threaten leaking information of their activities to their employer or law enforcement.

b) **Curiosity**
Some people are just curious. In the modern world the Internet offers a fantastic outlet for people's thirst for knowledge and discovery. Unfortunately, that thirst can also lead them to knock on doors they should leave alone. Freely available tools allow curious attackers to probe networks for venerable systems and break into servers on a whim. Curious attackers are often not out to harm a company - it's more that they like the feeling of being somewhere they shouldn't be. These people get a thrill out of knowing things other people don't. Much like mountain climbers reaching a mountain top, they get a rush out of penetrating the layers of a company's security. Once the outer layers of information security are penetrated these attackers like to browse through a companies 'chewy center' of data and secrets before moving on to the next target. [Mitnick p84, Lockridge].

c) **Revenge**
Revenge is typified by a worker who was fired and wants to get back at their employer. The motivation for revenge can take many forms, and can be quite dangerous because the threat from the law does not deter the attacker or methods they may use. People plotting revenge often do not clearly think out the ramifications of their actions or who else may be harmed by their acts. These attackers only care about harming the person or organization they think harmed them [Ingram].

d) **Job security / milking clients**
As the Industrial Age comes to a close and the Information Age begins, people are becoming painfully aware that job security is a thing of the past. Today, companies don't think twice about laying off workers by the thousands to meet productivity and EBTDA (Earnings Before Interest, Taxes, Depreciation, and Amortization [What]) numbers that keep the price of a company's stock high. As a result of these business practices,

employees have lost the sense of loyalty to their employers. Instead of remaining loyal, employees jump ship for a raise, better health insurance, or an office with a window. Some employees use different tactics, secretly creating problems only they seem to be able to solve. Contractors also sometimes use this method to get more billable hours from clients. Here's how it works. First the consultant sets a system crash to happen in the near future. Once the system crashes the client calls the contractor in to deal with the emergency. The contractor then swoops in to save the day and skillfully averts disaster – all on overtime pay. Not only does the perpetrator get credit for solving the problem, but they also become perceived as a critical person to keep on the team. Even worse, this person becomes more trusted even as they cause thousands of dollars in damage and downtime.

I heard the following tale at a one-day overview session on a course on information security. The individual telling the story was a contractor working for a medium sized company. He was responsible for security and high-level network management. He had discovered that the company had 'fired' and refused to pay the last contractor for their work, so he decided to develop an insurance plan for himself. The plan consisted of a logic bomb designed to go off, after a several month delay, if his user account was ever locked or deleted. This bomb had been installed on the companies' critical servers for over a year, ensuring that any attempts to restore from backup would simply prime the bomb again. The contractor had also worked with a developer 'friend' to bury the bomb deep inside a piece of code in a custom application written for the company. The contractor was quite proud of his work, even to the point of describing how he gave his wife a sealed envelop containing directions for disarming the system in the event of his death. His main goal in setting up the logic bomb was to ensure that the client would come crawling back to him should he ever be let go.

e) **Political statement**

Activists may want to embarrass or otherwise hinder an organization by defacing their web pages, revealing sensitive information, or crashing their systems to hinder operations. Victims are carefully chosen to achieve the proper impact. For example, a government web site would be defaced to promote the cause of the other side, or a chemical company would have embarrassing documents about pollution stolen and posted on an activist web page. In nearly all cases attacks are done to draw attention and/or sympathy to a political cause while embarrassing or otherwise harming the opposition.

f) **Vandalism**

Vandals deface web sites or perform other malicious acts for similar reasons vandals spread graffiti – prestige and notoriety mixed with a little love of destruction. Generally script kiddies want to be seen, to get their

'work' and their handle noticed. Fame is usually the name of the game for these attackers. The more people that see the vandal's handle on a hacked web page the more respected they are. These are the script kiddies who gather together hundreds of zombie computers and run DDOS attacks against major companies. They get excited when their exploits make the news or when they deface a corporate web page with their logo. Sometimes these groups purport to have a political message; however, it is often lost in their misspelled grandstanding rants.
One word of warning - there are groups out there that are knowledgeable and almost surgical in their abilities and tactics. The most famous of these groups is Fluffy Bunny (no, I'm not joking). Fluffy Bunny has managed to penetrate several well secured systems. In September 2001, at the height of their activity, Fluffy Bunny gained access to a DNS hosting service and redirected 100,000 domains to a group propaganda page. It took several hours for the DNS provider to notice the problem, and longer still to get it fixed [Richardson, Leyden]. To date only two of the group's members, an American and a European, are believed to have been caught.

g) **Terrorism**
It's hard to go a day without hearing about terrorists any more. Threats of terrorism have been on the minds of most people if the western world since September 11 2001. While historically terrorists have used conventional bombs (with one exception of a cult using Sarin gas on a Japanese subway in 1995 [World]), they are known to be actively developing other methods to spread terror. Terrorists look for the following when planning an attack: **Asymmetric threats.** Terrorists look for ways to leverage their resources for maximum effect. On September 11 it took less than 20 terrorists to kill over 2000 people [Matai p2]. Terrorists are aware that they can cause wide-spread damage with a cyber attack while using few resources. They are also aware that if they can properly leverage a computer based attack the damage could be wide spread, even if less tangible than a conventional bomb. One of the best ways to get at a country in the western world is through its financial systems and economic backbone. The world trade center was largely chosen by terrorists because it was a symbol of the economic power of the US. Now, after September 11, stricter immigration security has made it more difficult for terrorists to travel. Now more than ever it is likely that terrorists will use the Internet or target a nation's associated infrastructure for future attacks.

h) **Espionage** (corporate or state sponsored)
Competitive organizations often steal secrets from one another in order to bolster their own operations. Rival companies, with the threat of increased competition and reduced R&D budgets, may decide that it's cheaper to steal a product than risk money developing one. Some companies simply don't have the in house talent to make technological

advances. A competitor may find that a new process is so efficient that stealing the secrets is the only alternative for staying profitable. Other possibilities include a company wanting to win the bid for a lucrative project, no matter what. [McDermott, Friedman]
Corporate-sponsored espionage presents a difficult situation for a company. They do not want to be associated with the unsavory details of stealing secrets. This 'dilemma of association' leads corporations to recruit outside talent to do their dirty work. Individuals recruited for these tasks may be mercenary hackers, ex employees of the target company, Private Investigators or ex government spies with advanced social engineering skills (the number of underemployed spies has grown since the cold war). By recruiting from outside the company a layer of insulation called ***plausible deniability*** is given to the company. Plausible deniability essentially allows the company to rightfully deny knowing where information came from and therefore avoid prosecution if caught.
Governments may see the technologies of foreign competitors as a threat to their way of life, the profitability of homeland corporations or even as a way to make their military 'cutting edge' without expending the time, effort or money necessary to acquire the technology. The countries actively involved in state-sponsored industrial espionage include friendly countries like France, Germany and Israel as well as the more traditional spying from China. GAO report: [Cooper].

> "France's security agency, the DGSE, is considered the most brazen of offenders. Its agents have posed as diplomatic officials to try to steal American 'stealth' aircraft secrets and stolen the garbage of American computer experts. The DGSE has planted 'moles' in the overseas branches of major U.S. corporations, including IBM, Texas Instruments and Corning Glass. One of the primary beneficiaries of its covert activities has been Compagnie Des Machines Bull, a big computer firm that is partly owned by the French government." [McDermott]

Note: Appendix A has more details on foreign countries involved with industrial espionage and other Information Security attacks.
Many foreign cultures see intelligence gathering as a necessary part of doing business. They are often confused by the American idea that spying is wrong. Most notable of the countries is Japan. Japanese businesses frequently gather information, including stealing secrets, on each other and competitors. Additionally, while the Japanese government seems to have no official spy agency, Japanese corporations have more than made up for it by developing their own spying capabilities. In fact, Japanese corporate spying is so large, coordinated, and efficient that they actually frequently pass important secrets on to the Japanese government for state use.

i) **War** (also called Information Warfare or Cyberwarfare)
During conflict, enemy countries may attack economic, financial, or business and consumer infrastructure. Targets may include telephone, highway, air travel, electronic commerce, and banking. By using

information warfare a country can fight battles while minimizing bloodshed. In fact, military strategy all but demands the use of information warfare. In the highly regarded treatise Sun Tzu on The Art of War, Sun Tzu declares, "The best thing of all is to take the enemy's country whole and intact . . . Supreme excellence consists in breaking the enemy's resistance without fighting." [Hart, sec. III num. 1]. What better way to wage war than to shutdown a country's infrastructure from the inside; to paralyze their military and deafen their communication systems so that an army can invade with impunity?

While several countries are developing Information Warfare capabilities (notably the US, China and Taiwan), no one knows what the true outcome of an all out 'digital Purl Harbor' style attack would be. Hopefully, countries will recognize that digital warfare has an inherent economic mutual deterrent; destroying an enemy's economy may well lead to your own economic crisis.

The Why - Summary

Motivations vary as much in the digital world as they do in real life. It is important to keep in mind is that the digital world is simply an extension of every day life. If a person wanted to steal money 50 years ago, they may rob a bank with a gun or develop an elaborate investment scheme. Now they use a keyboard. The motivations for attacks haven't changed much. It's the methods – the 'how they do it' that has changed drastically in the past twenty years.

The How

The next section goes over the more common methods for compromising information security. You will notice that several methods have nothing to do with computers or technology at all. This is because all organizations have a human component that can often be exploited more easily than servers and firewalls. Indeed, the vigilance of a company's employees is just as critical as maintaining proper physical and network security.

a) **Denial of Service**

Denial of service attacks work by either crashing a server or service, like the www service, or by flooding a network, server, or service with so many requests that the server can't keep up. Denial of service attacks can come from only one computer (referred to as DOS) or from many computers at the same time (called DDOS). The goal of a DOS or DDOS attack is to disrupt the availability of a company's service, such as access to the company web page. Large DDOS attacks can generate so much traffic that an entire network becomes unable to reach (or be reached) from the Internet. There are currently only a few ways to stop DDOS attacks once they start. To stop a DDOS attack, the victim usually calls their up-level Internet provider, like UUNET, and asks for filters and a 'trace back' the source of the attack. Filters are not always effective, leaving the victim at the mercy of the perpetrator for the attack to stop. DOS and DDOS attacks

are easy to set up and launch, making them a weapon of choice for script kiddies.

b) **Scripts and tools**

Most attack tools are free, documented, and easy to use. Because of this simplicity, scripts are widely used by individuals with little knowledge of how the program actually functions. Scripts and tools are used by security administrators and attackers to probe the security of networks. When in the hands of a security administrator, tools can point out security weaknesses that need attention. When used by an attacker, tools point out weaknesses that can be later used to gain unauthorized access. There are hundreds, if not thousands, of tools available on the Internet. Entire training courses and books devoted to the subject only scratch the surface of what is available for testing security. Some examples of tools are NMAP, which will automatically scan an entire network for a whole list of vulnerabilities, to LINNT, which allows access to Windows NT or 2000 NTFS drives and allows for the user to change passwords, including the administrator. A growing concern among information security professionals are the so-called *Zero-day exploits*. Zero-day exploits are malicious programs that exploit undocumented or recently patched vulnerabilities. The problem with these exploits is that they are not published; meaning the security industry at large may not even be aware of the problem. Tracking these exploits may be difficult for all but the most seasoned security experts. Additionally, software manufacturers who don't know about a problem with their software can't fix it. This allows Zero-day worms or viruses to potentially spread further and much faster before being contained.

This issue closely follows another trend in the security world, *anti-disclosure* **(**sometimes called anti-security). The hacker community has typically been very open when new security vulnerabilities are found. Because of this openness, vendors have usually been able to produce patches before an exploit reaches public distribution. With the growing tendency for anti-disclosure (fueled by the liability concerns of the DCMA millennium copyright act) publication of vulnerabilities may soon case. Anti-disclosure proponents also suggest that the script kiddie problem is largely caused by openly publishing vulnerabilities, and that anti-disclosure will deprive them of the ability to carry out their attacks.

c) **Social Engineering**

Social engineering is generally a blanket term used for an attack where information security is compromised by conning people in various ways. Social engineering is often done at a distance over the phone. Social engineers will avoid face-to-face meetings with their mark if possible; however, they are not above brazenly walking into a high-security company pretending to be a VP from a remote office. The methods used in their attacks require the use social skills as well as technical finesse. Social engineering is most often used in concert with other tools to penetrate a company's defenses. Social engineers may use the following schemes in various combinations to bypass security:

- It may sound simple, but asking for help is one of the most common ways for social engineers to penetrate security. To do this they will play on their target's sense of compassion (often by masquerading as a coworker in need);
- Social engineers learn and use the lingo of a company to appear as someone on the inside [Mitnick]. By appearing as someone in the know targets will more freely give the information they are asked for and are more likely to bend the rules when asked (again by being tricked into thinking they are helping a coworker);
- Another highly effective practice is pretending to be someone else. Social Engineers often masquerade as a subordinate to a VP or manager inside the organization. By appearing to proxy the request of a VIP the social engineer is able to get targets to perform tasks they would normally question or refuse;
- Social engineers like to masquerade as support or maintenance personnel. By using this method the attacker tricks the target into thinking they are being helped. Instead, the utility or patch they are told to load contains a Trojan or other tool the attacker can use to gain further access to the company. Other frequent ruses include tricking workers into giving their passwords out or performing a task (such as leaving their dialup modem turned on for support to run 'tests' later) as a return for the favor of 'fixing' a problem;
- Social Engineers do their best to be nice, courteous, and very friendly. A good social engineer will not burn bridges while performing their attacks. Frequently, social engineers will use someone with whom they have established a rapport several times during an attack. Successful attackers leave victims feeling good that that they helped someone avert a problem without having the faintest idea they have been used.

Social Engineers know how to find the weak spot in a company's security and exploit it. If a target company has superb network and perimeter security, attackers will simply develop a scheme to trick people on the inside into doing their dirty work. Social engineers tend to do significant research on their targets before launching an attack. Indeed, they may know more about a target company than most employees. Social engineers are also adept at dressing the part in order to blend in with other people. If they want to walk in through a security checkpoint, social engineers will dress like management and mingle with others as they 'piggyback' through secured doors and checkpoints. A successful social engineer will use their excellent social skills in conjunction with technical expertise during an attack. Social engineers plan operations well in advance with provisions for setbacks and unsuccessful steps. Once the attack is finished, the victims and their employer are often unaware that anything nefarious happened.

d) **Dumpster Diving**

Dumpster diving covers a whole range of activities but they all boil down to rummaging through a target's discarded materials. Attackers have gotten password lists, hard drives with critical information, and manuals detailing the

management of critical systems using this method. These secrets are obtained by going through the trash, buying old equipment for scrap, and piecing together shredded documents. Dumpster diving demonstrates one key failure in most security - things that were behind lock and key can end up available to anyone willing to go digging through someone's trash. Even shredding documents can be defeated with time, patience, and enough scotch tape. The best known example of this comes from Iran.

In November of 1979 Iranian students and protestors seized the American embassy in Iran. To their credit, the staff did as much as they could to shred the most sensitive documents - with only one problem. As it turned out, they used an inexpensive shredder that cut documents into little strips, rather than cross-cutting and burning (strip shredders work the same as shredders seen in most retail stores). The Iranians simply took the bags of shredded documents and put the pieces back together again with tape. The documents were then published in several volumes called "Documents from the U.S. Espionage Den" (you can still buy copies. I found a used copy available on amazon.com). These documents exposed U.S. intelligence operations in the entire region. The documents also detailed the inner workings of the Israeli intelligence agency, the Mussad. This incident was a massive setback for both U.S. intelligence and the Israelis, not to mention damaging U.S. relations with the entire region [Ignatius, Epstein].

Another, more recent, example has a quite different ending. While trying to show Microsoft's bad will regarding an antitrust suit Larry Ellison, the CEO of Oracle, decided to dig up some dirt on Microsoft's practices of creating grass roots organizations supporting Microsoft's side of the story. The plan took a strange turn when a detective agency, paid by Ellison, tried to pay off a janitorial service in exchange for the garbage from one of these organizations. Evidentially the PI wasn't well versed in social engineering. The janitor dutifully reported the incident to the authorities who traced the incident back to Oracle and Ellison. Instead of finding embarrassing information about Microsoft, Ellison and Oracle were themselves embarrassed once the media got hold of the story and dubbed it "Larrygate" [Edwards].

When thinking about security risks dumpster diving poses, think about this: What do you throw away at home? Do you throw away bills with credit-card numbers, old receipts and bank statements? Now think about what a company throws out and what would happen if it was discovered and used by attackers.

e) **Exploring and information gathering**

Information gathering is done before an attack is planned and carried out. Professional hackers, spies, and the competition will gather as much freely available information as possible to develop an understanding of a target. Information gathering includes looking at the target company's web site, marketing materials, and possibly even posing as a potential customer. Other less legal ways of gathering information include hiring ex employees, network and vulnerability scanning, and social engineering maneuvers designed to flesh out the inner working structure of a company. Once sufficient information is

gathered, it is summarized and analyzed for weaknesses. A plan for attack is then formed based on weak points discovered in the corporate security scheme.

f) **Spies and Moles**

Foreign governments frequently use of students to acquire knowledge from a university and/or a company. These governments will sponsor programs to send students out foreign institutions to become experts in a technology. Once the student has the desired skill and knowledge the government then persuades them to return home. The knowledge obtained from the student is then exploited to transfer the technology locally. This method is highly effective for stealing secrets from US companies and universities. The reason this happens so freely is the fundamental way organizations are run in the U.S. U.S. organizations are typically open, fluid, and diverse, which leaves them easy targets for infiltration. It is not unusual to have foreigners with H1B visas working on sensitive highly technical projects here in the U.S. Overseas it's a different story. Japanese companies would be loath to allow a foreigner into a project team working on a sensitive new technology. Because of this difference in culture, it is easy for foreign companies or intelligence agencies to plant spies in American institutions. At the same time, it is extremely difficult to American companies to plant spies in foreign institutions because other cultures are much more closed and distrusting to outsiders [Fialka].

An example of this is China's use of students to spend years acquiring knowledge from a foreign institution (Including universities and high technology companies), then have them return home. The obtained knowledge is then applied in local companies to transfer the technology locally. Every year thousands of China's best and brightest are sent abroad to acquire the newest technologies. China has been practicing this for years, allowing them to greatly enhance their technology and economic competitiveness at the expense of foreign institutions [Fialka].

g) **Breaking in**

Even though impractical and risky, breaking into a competitor's or an employee's home/hotel room provides a good opportunity to compromise information security. Information stored in these locations is frequently unencrypted, obviously placed, and likely somewhat sensitive. The tools of the trade include lock picking tools, a camera or copy machine, computer 'tools' (like a keylogger or Trojan) or even a portable USB hard drive for copying information. Security systems are an effective deterrent, but a determined attacker will likely be prepared for this eventuality.

The risk of having a break-in is highest for traveling businessmen. Hotel rooms often have poor security, no alarms, and no way to know who has accessed the room. Hotel room break-ins are a favorite of the French secret service and other state-sponsored intelligence agencies. There are several well documented occurrences of businessmen and government officials leaving documents and laptops in their room while staying in hotels in France. Later, while at a business meeting they would notice the other person would be referring to exact copies of

the sensitive documents. With this in mind, traveling business people should keep important documents with themselves at all times. They should also make sure their laptop data is safe, and beware of making phone calls where sensitive information is discussed.

h) **Back Doors**

Back doors are security holes installed or opened on a computer or network for purposes of debugging or bypassing security. They can be built in to the software by a rogue developer, company selling software, or even government agents (this allegedly happened with Mussad installing back doors in Checkpoint software, and Microsoft Windows operating system suggestively containing the letters 'NSA' in an obscure program module). However, most commonly a hacker installs a backdoor called a Trojan. Once installed the back door can be used by the attacker at their leisure. Once the attacker has this toe-hold on the inside of a network, these back doors are used as launching points for further breaches of information security.

One disturbing trend is that Trojans are becoming more frequently found hidden in open source software. This is not done by the developers, but by hackers who break in to the distribution server and attempt to burry nefarious Trojan code inside a legitimate application [Gray]. Based on these occurrences, it's unsettling to think how often this may be happening in non-open source software subject to less scrutiny.

Victims can be infected with a Trojan in a variety of ways:

- Attackers can bundle Trojans with legitimate programs then distribute then to unsuspecting users. A freely available program called Silk Wrapper does just this with a simple graphical interface;
- Somewhat knowledgeable attackers can make subtle changes in common Trojan programs, with the resultant Trojan being undetected by antivirus software;
- Commercial Trojan-like software does not raise an alarm on most antivirus software. If an attacker uses one of these commercially available products, a target's PC may have fully functional antivirus software with the latest definitions and never discover the infection;
- Highly skilled hackers can code custom Trojans that are all but impossible to detect. The FBI itself has developed one of these programs as part of project Carnivore. The software, named Magic Lantern, can be hidden in an e-mail and installed by exploiting security vulnerabilities on the target's computer (it is not known if the FBI uses known or undocumented exploits). Little is publicly known about Magic Lantern. What is known is that once installed, Magic Lantern can act as a keystroke logger. It can also be used to steal encryption keys which are later used to decipher encrypted files or messages [Sullivan].

i) **Spyware**

The term spyware generally denotes companies installing software to track user's Internet habits, with or without the user's knowledge or consent. This

could (and is) easily be used to gather more sensitive information. The difference between spyware and trojans can get somewhat fuzzy and some tools can act as both. The main difference is that spyware is designed to specifically monitor a user's behavior in some way. Trojans generally offer more remote-capability options, such as remote-control of the command line interface. Spyware can also refer to hardware devices such as keyloggers that attach directly to the keyboard cable or TEMPEST, which refers to monitoring (or protecting from monitoring) the electromagnetic emanations from electronic equipment. TEMPEST technology can even be used to remotely view a target's computer monitor by using radio equipment that eavesdrops on the electromagnetic 'junk' a monitor gives off during normal use. An entire cottage industry has developed around creating technology to both exploit and protect against TEMPEST. Other spyware includes bugs, mini cameras, shotgun microphones, and other devices commonly displayed in spy movies (minus the rocket-launcher equipped, submersible, bullet-proof sports car).

j) **Poaching**

A growing practice in the technology industry is hiring employees of a competitor, and then exploiting the employee's knowledge to augment the new employer's operations. Depending on the individual, secrets learned from an old employer may be used at the new employer in exchange for higher pay or better benefits. At a minimum, the knowledge and skills the employee developed at their previous employer are lost to the competition. This is one of the primary reasons why key employees with talent should be well compensated for their roles within a company. Sure, a company can get away with underpaying talent, but sooner or later the practice will backfire as talent leaves while less talented employees remain.

Occasionally, employees will keep sensitive documents on technologies in use at their old job. New employers may take advantage of this by obtaining and using that documentation to improve their own operations. The following case illustrates how harmful this breakdown in information security can be:

> "The most colorful and high-stakes case embroiled General Motors and Volkswagen for much of the 1990s. The cased hinged on a ring of Latin employees led by a hard-charging Basque expatriate named Jose Ignacio Lopez de Arriortua. Lopez was head of purchasing for GM and defected abruptly to VW in 1993. GM accused Lopez of masterminding the theft of more than 20 boxes of documents on research, manufacturing and sales. Much of the allegedly pilfered data involved blueprints for a super-efficient assembly plant--a factory that GM believed would topple VW's dominance of the small-car market in emerging markets of Eastern Europe, China and elsewhere.
>
> The world's largest international corporate espionage case officially ended in 1997, when VW admitted no wrongdoing but settled the civil suit by agreeing to pay GM $100 million in cash and spend $1 billion on GM parts over seven years.

In 1998, German prosecutors dropped criminal charges of industrial espionage against Lopez, who resigned from VW in 1996 and was injured in a car accident in Spain two years later. But Germany made Lopez donate $224,845 to charity. " [Konrad]

k) **If you can't steal it, buy it**

It may sound strange, but a good way to steal industrial secrets is to buy them outright. This can be done one of several ways:

- By dangling huge lucrative contracts with contingencies that the technology used be transferred and used locally. China commonly uses clauses in huge contracts to force companies into transferring technology to a domestic location [Fialka];
  An example of technology 'bought' by a big contract is McDonnell's 'plant 85'. In plant 85 were several high-technology machines used in the manufacture of aircraft parts. These "five-axis" machines produced quality parts to high tolerance specifications, but could also be used to produce guided missile parts as well as better military aircraft. As part of the contract the Chinese required McDonnell to move several of these machines to China for production purposes. Once there these machines could be reverse engineered or simply put to use making military equipment for the Chinese. Indeed, once obtained these machines were installed in dual-purpose facilities that made both commercial airplanes and military aircraft [Fialka].
- Technology can also be bought by acquiring a company with the desired technology. While not illegal or unethical, these purchases can be used to effectively transfer technology to another company or country. Another use is to acquire control of industrial secrets in order to deny them to competition. For example: Suppose two competing companies both use chips made by only one manufacturer. One company decides it wants to corner the market, so it attempts a take over of the chip manufacturer. If the takeover succeeds not only is the chip technology acquired, but the company now also has the ability to delay, deny, price gouge, or otherwise hinder chip deliveries to the competition.

l) **Path of least resistance/weakest link**

An attacker will look for the easiest way into a company. Attackers look for the easiest path through the security in an organization and exploit these weaknesses to get what they want. This is why performing 3rd party vulnerability assessments are so important. Identifying and fixing the weakest link in corporate security drastically increases the difficulty for a potential attacker. Properly implemented post-audit improvements make it more likely attacks will fail, and help to persuade attackers to look for easier targets.
Unfortunately, companies frequently fail to bother with improving security. Instead they choose to believe their systems are too complex or obscure for anyone else to use. As the following example illustrates, this thinking is seriously

flawed. People seem to follow the creed, "If you build it they will come. . . and try to break it".

Nearly all industrial and utility companies use SCADA (Supervisory Control and Data Acquisition) electronic control mechanisms to regulate their operations. For example, water companies use SCADA systems to control the flow of water through pipes and the floodgates of dams. Gas companies use SCADA to manage the distribution of gas throughout the country. Even Electric utilities use the technology to maintain the power grid. By now, you should be getting the picture; SCADA systems are the weak spot for most industrialized nations' infrastructure. SCADA controls the flow of oil and gas, governs the electrical grid and even manages traffic signals and subway systems. SCADA controls the water you drink and manages the sewage for entire cities. Why would an attacker bother to blow up a dam when they could simply open the floodgates and destroy a city anonymously [Gellman, Barker]?

Most would like to think the SCADA infrastructure is safe and sound, but history shows otherwise. For example: Vitek Boden, a disgruntled worker who was trying to milk the Maroochy Shire Council (a waste water treatment system co-op in Australia) for a job. Boden, who had previously worked on a project to install the SCADA system for the co-op, wanted the Maroochy Shire Council hire him permanently. After having his application for employment ignored, Boden hatched a plan to force the council to hire him. As part of the plan, he built a pirate radio control system and mounted it in his car. The pirate radio system would transmit control signals to the SCADA system, effectively seizing control of the Maroochy Shire sewage pumping stations. Once Boden's equipment had control, commands would be injected into the system. The resultant confusion would spread chaos through the SCADA system. Boden's equipment would command the SCADA system to dump large volumes of unsavory fluids into the most unexpected places. Once finished building his system, Boden would occasionally go for a drive down the Sunshine Coast; the pirate radio system in his car starting and stopping sewage pumps as he went. The result was millions of gallons of sewage pumped into local parks, rivers, and even the grounds of a large hotel. There were over 40 separate incidents of sewage spills before local police managed to catch up with him [Smith, Barker].

The sensitive nature of SCADA systems has not gone unnoticed by terrorist circles. A report by the NIPC indicates that Al-Qa'ida operatives have started gathering information on SCADA systems. While sketchy, the report indicates Al-Qa'ida has already gathered information from web sites containing content on SCADA controlled water and sewage systems. The full report is located at http://www.nipc.gov/publications/infobulletins/2002/ib02-001.htm.

m) **Gestalt**

Often little bits of information seem harmless; however, when put together they can create a big problem. For example, knowing a social security number isn't anything special. Neither is having a street address, a birthday, an employer name, or a mother's maiden name. Put all these pieces of information together and an identity thief has everything they need to sign up for a credit card in your

name. The same goes for companies and their information. Little bits may seem to make little difference, but pieced together they can cause great harm.
An example of the gestalt approach is a part of the FBI Carnivore system. The tool, called Cyber Knight, operates by matching up previously gathered encryption keys (obtained by using tools like Magic Lantern) with encrypted files and correspondence [Sullivan]. By using Cyber Knight, the FBI is able to bring together different informational fragments and use them to discover exactly what the target is doing, planning, and hiding.
More recently is the announced TIA or Total Information Awareness system, which is being undertaken as part of the homeland defense program. The TIA system, under development by DARPA (Defense Advanced Research Projects Agency), will eventually maintain a super-massive database. The undertaking is so big that new technology needs to be developed before the project can be finished [Total]. Once the system is operational, law enforcement and intelligence agents will be able to extract the details of anyone's life in the U.S. Ostensibly created to help ferret out terrorists, this system will collect and link far-flung sources of information such as spending habits, criminal history, driver's records, education, and more.

The How - Conclusion

Very seldom will only one isolated method be used in an attack on information security. An attacker with any sophistication will develop a plan using several of the above mentioned methods in an attack. The methods used in an attack will depend on a combination of the attacker's experience, the result of an analysis of the target's weaknesses, and the motivation behind the attack.
While modern technology allows humanity to leverage knowledge to enhance the quality of life, that same technology allows attackers to use their knowledge for leveraging attacks on information security. Technology works to level the playing field for adversaries. It allows small groups (or even individuals) with the right knowledge and tools to take on the largest multinational companies. Because of this, the Internet will play an ever larger role in the modern world; both as a tool for making life easier and as a weapon of choice for small groups with an axe to grind. In the case of information warfare, a much smaller and militarily weak country can strike against a large country that simply has no ability to systematically protect its entire infrastructure. Larger organizations simply present a much bigger target with associated gaps in security. No one in the industrial world is totally safe from this threat. 30 years ago it took large amounts of money, a well coordinated spy network, and a lot of luck for Israeli LAKAM intelligence operatives to penetrate the DOD. Now it can be done safely from a computer ½ a world away with little risk of getting caught. Modern attacks on information security are highly efficient, proven effective, and allow a degree of anonymity never before seen. If our modern society is to continue its steady progress these threats must be taken more seriously. More needs to be done to protect against these threats or the digital equivalent of a Purl Harbor or 9/11 is only a matter of time.

Part II: Defending against attacks

Defense against attacks on information security requires resources. To build and maintain an effective defense requires money, time, expertise, and training. Determining how much to spend and to what lengths to go can be daunting at first; however, there are documented procedures for determining how much time, effort, and money should go towards information security. The formulae boil down to determining how much the information is worth to the company. The procedure includes determining several variables.

- How much it would cost the company (in lost revenue or other costs) if the information were altered, stolen, lost, or unavailable?
- How much would the cost of replacement be?
- Determining how likely events causing these possible losses are.

Once these factors are determined, measures that mitigate the vulnerability, severity, likelihood or downtime (in case of fire, flood or other disaster) are evaluated to determine cost and how well they protect against possible losses. The result is a report that details the value of the information assets an organization has, how likely these assets are to be threatened, and what can be cost-effectively done to protect against dangers to the organization's information assets.

a) **Money**

Frequently it is difficult to justify spending money on information security. Due to security expenditures contributing to a company costs with no obvious return on investment, justifying security expenditures can be an uphill battle. Most security professionals use statistics from reputable sources to make their point that failing to protect information assets is a time-bomb waiting to go off. The losses from break-ins, theft, and espionage can bankrupt a company. Sometimes simple solutions, like off site storage of backups, may determine the fate of a company after a fire or flood. Finally, small companies that frequently cut information security corners are, in fact, the ones that need it most. Trends in information security incidents indicate that attacks on small businesses are growing in popularity. This is because small businesses have more innovative (lucrative) ideas and few resources to fight off attacks [McDermott].

If money is a problem but time and the manpower are available then open source software and good policies can be used to help shore-up the security of an organization. Open source software is free, requiring the user only have the hardware it runs on. Open source software is also well documented and widely used. This can be a benefit when the user is knowledgeable, needing minimal help with the software. However, open-source software is not without its problems. There is seldom any vendor support (and there are fees attached when vendor support is offered), the software can be difficult to install and manage, and there's always the possibility that the software will stop being improved as developers move on to other projects.

b) **Capable, competent staff**

Technology is useless if no one knows how to use it. Employees in charge of information security must know what they are doing. They must also be knowledgeable of the current state of the art technology in order to provide adequate security. Also beware of The Peter Principle- "In a hierarchy every employee tends to rise to his level of incompetence" [Peter]. A training program should be in place to make sure skills are up to speed and pertinent to current job responsibilities. Periodic reviews need to be done to ensure the right people are teamed with the proper duties. Additionally, rotation of duties and knowledge duplication both work to mitigate problems created by unknowledgeable workers as well as protect the company against the loss of any one individual.

Training is also important because of the rapid evolution taking place with information security. To put it simply if you don't keep up, someone else will. New attacks and security mechanisms are published at a dizzying pace, requiring significant attention be paid to staff development, maintenance and upgrades to security mechanisms, patch testing, and new deployments.

c) **Over-security – you can do too much**

Piling on too much security hinders daily operations of the company. Tasks that once took a few seconds may end up requiring the request of additional permissions, excessive paperwork, or mind-numbing security training seminars. It is important to balance security and efficiency within an organization. One of the dangers of over-security is that employees will give up, find ways around, or ignore burdensome policies and security mechanisms put in place. The resulting oppressive environment from over security leads to high employee turnover, low morale, and lost efficiency.

Implementing security measures without full knowledge of the effect can cause unforeseen problems. For example, overzealous network administrators frequently block all ICMP (ping) to networks they control, thinking it will allow them to avoid DOS attacks and other security problems. Unfortunately this breaks an important function ICMP provides; PMTU. PMTU is the process of a computer discovering how big it can make a packet of data before that packet gets chopped into little bits by Internet routers. Blocking ICMP (and in the process PMTU) disables this process, crippling access for legitimate users or customers. The result of blocking all ICMP may lead to downloading files hanging and web pages stalling for no apparent reason. Worse yet, the problem may appear to be intermittent! [Dibowitz]

d) **Penetration Testing**

The best way to determine how good a company's security mechanisms work is to have a third party simulate an attack on the information security of the company. Penetration testing does not just bang on the doors of a company's Internet connection. During the course of a penetration test, policies and procedures, staff's ability to follow security guidelines, and physical security are

all put to the test. The findings are later used to strengthen policies, network security, and other weak spots that were identified in the testing.
Penetration testing is expensive; however, going forward believing, "We're secure because we spent a lot of money on it" is a rather dangerous stance to take. The question to ask is, "Would you rather we find our weaknesses and fix them, or would you rather someone else find our weaknesses and exploit them?" The most important factor in a penetration test is finding the right people for the job. Some companies offering penetration tests simply run an intrusion scanner like Nessus and use the results for their report. These are not the people to use. A good candidate for penetration testing will provide an outline (either verbal or written) of how thorough the test is as well as give references from other clients that used their services in the past (CALL THEM!). Employees of the potential consultant should also have clean background checks and clean credit reports. At the completion of a penetration test, a detailed report of weaknesses will be provided. Based on this report suggestions for remedies should are given and the consultant may work with the company to fix the problems. The process is not complete once these fixes are implemented. Additional security audits should be performed periodically to ensure that proper security is maintained, policies and procedures are working, and evolving vulnerabilities are anticipated.

e) **Defense in breadth, not just defense in depth**

The best network security in the world won't protect you from someone walking through a propped open door and snatching your backups. While layered security is important, it also needs to be flexible rather than super-strong and brittle. Security should be made to degrade gracefully rather than outright break under the strain of an attack [Mann]. For example, servers under DOS attacks should use mechanisms that hinder an attack enough that littermate packets can still get through rather than crash under the load. Additionally, thought needs to be put into new 'cure all' security measures. For example, the idea of creating a national identity database may allow the FBI to data-mine for terrorists and drug dealers, but it also presents a tremendous risk for identity theft and abuse by information brokers.

M&M syndrome

Does your company have a hard layer of security on the outside with a soft chewy center? [Mitnick p79] Relying on any one mechanism to protect information security is a critical mistake. Even the best products have problems. Relying on only a one-layer perimeter firewall to protect your internal network can lead to serious problems should vulnerabilities be found in the software [Salkever].

Avoid the trap: Don't just secure the things you know and understand. Breadth of coverage in information security is critical. A common shortcoming in security is failing to cover all the bases. When creating a security policy it is important to use additional resources like legal, HR, input from management, and published industry standards.

f) **Policies**

Policies and procedures need to cover the human aspect of information security. Failing to provide adequate policies and procedures leave the company little recourse against breaches in information security. Formal policies and procedures need to be concise, understandable to the laymen, and comprehensive [Mitnick p191].

In order to effectively implement secure policies and procedures, management must support the effort. Without support from management at the highest levels policies and procedures will quickly develop inconsistencies in enforcement and hence become more easily compromised. Enforcement of policies must be uniform and consistent throughout the company in order to be effective. Further reason for uniform enforcement includes the legal system. Should an inconsistently enforced policy be used for grounds of termination or legal action, the case can quickly be turn against the employer due to accusations of discrimination. Such a case could easily leave the employee in a position to sue the company for wrongful termination.

To get employees to buy-in to the policies and procedures there must be an incentive. Normally the incentive is a warning or threats of termination. Other incentives could be bonuses for following the policies when an employee is tested during an audit, a penetration test, or having management recognize an employee for sticking to the policy in a difficult situation (for example, after having management attempt to circumvent the policy to see what happens). Once staff become aware that the company is serious about the policy, compliance will be achieved more easily. There's nothing quite like people knowing that the policies and procedures will be put to the test. Remember, without motivation no one will care and policies will be useless.

Finally, revising policies and procedures ensure that they remain pertinent and applicable to all employees. When large corporate changes take place it is especially important to revise policies and procedures to reflect the changes in the organization.

g) **Procedures**

Procedures within the company should be documented and easy to follow. Duties should be rotated so that more than one person can perform critical functions. Job rotation also helps to dissuade employees from forming plans on compromising information security. Rotation of duties helps to distribute knowledge among several staff, protects the company from losses due to individual resignations or from mass transit vehicles running amok.

Other critical procedures include plans for disaster recovery. Companies able to quickly recover from a fire or other catastrophe are much more likely to stay in business in the long term. A disaster recovery plan also needs to be tested. Having the disaster recovery plan routinely tested helps iron out any bugs in the plan as well as familiarizing staff with the procedures necessary to efficiently get the company back up and running after a disaster.

Defense in summary

The key words to remember are: layered, comprehensive, tested and proven, flexible rather than brittle, knowledge and skill. While it is impossible to anticipate every contingency, developing a well-rounded information security plan can help to dissuade all but the most determined attackers. With proper auditing systems such as audit logs, intrusion detection systems, and other mechanisms, incident response staff will have the right tools to determine what happened should a successful attack take place.

Finally, keep in mind that maintaining confidentiality, integrity, and availability of information requires significant recourses, time, and money. Security is not something that can be dropped in place and forgotten.

Conclusion: Is there a *real* problem – how bad is it?

Due to the nature of corporate culture, companies are extremely reluctant to admit when they have had a breach of information security. The reason is simple – companies do not want consumers to loose faith in them. This desire to keep problems secret skews the ability of researchers to accurately judge the frequency and amount of corporate losses due to breaches in information security.

Despite the difficulty in gathering statistics we are routinely bombarded with studies pointing to a drastically increased problem with Internet-based attacks, economic and industrial espionage, thefts, blackmail, and fraud. While the frequency of these attacks is hotly debated, the simple facts remain. It is seen in viruses and worms like Nimda and Klez. It is brought to us by teenagers taking on entire companies like E-bay and Yahoo and shutting them down for a day on a whim. These threats are real. These people are out there. If companies continue to fail in adequately protecting information assets they do so at their own peril.

Studies are also pointing to an unanticipated trend. Start-up and small companies with typically low security may be the most frequent targets. The reason is not necessarily so apparent, “Start-up companies are often where the most valuable new secrets are found.” [McDermott] While digital attacks on government systems seem to be decreasing, it is at the expense of businesses. A study in Great Britain concluded, “Small companies are a growing target: The overall trend for digital attacks is on an upward curve with 31,322 overt digital attacks recorded in 2001 and 64,408 - more than double - recorded in 2002 already. The revised projection for 2002 is for over 70,000 such attacks mostly targeted at small to medium size businesses.” [Hacker]

The trend is clear. In the not too distant future companies that fail to adequately defend themselves against attacks on information security will find themselves competing against their own, stolen, technology. Information security is becoming ever more critical to keep hard-earned technology and economic secrets from making their way into the hands of criminals or the competition.

Appendix A

The following is a description of several foreign intelligence organizations known to actively operate against companies.

Country	Agency	Description and notes
Japan	MITI JETRO Naicho Chobetsu	Japan is believed to run a decentralized but coordinated and efficient network of intelligence gathering, with the Ministry for International Trade and Industry [Schweizer p18] acting as a hub for Japanese intelligence gathering. Another branch of the Japanese government is JETRO. Ostensibly focused on promoting exports, JETRO is believed to be heavily involved to be an "economic and political intelligence gathering service." [Schweizer, p80]. Naicho, answers directly to the prime minister, coordinates intelligence gathering efforts for the Japanese government. It is responsible for intelligence on foreign interests and disseminating information to Japanese leaders [Schweizer p82] The Annex Chamber, Second Section, of the Investigation Division of the Ground Self-defense Forces (Chobetsu) is responsible for electronic eavesdropping and surveillance in the region. This agency has massive electronic surveillance capabilities; eavesdropping on China, Taiwan, North and South Korea as well as regularly tapping into business communications of foreign companies in the region. [Schweizer p84] Japanese corporate culture looks on spying differently than US companies. Japanese companies consider it a responsibility to gather intelligence from competitors and use it to improve their own products and services if at all possible. Japanese intelligence gathering includes acquiring trade secrets, technology and manufacturing processes.
Germany	BND	Germany's primary intelligence service is the BND or Bundesnachrichtendienst, known as the Federal Intelligence Service. The part of the BND responsible for technical and electronic intelligence collection is Division II. In 1989 the BND began project Rahab, which studied the feasibility of hacking into foreign databases as well as the uses of viruses in information warfare. In 1991 Rahab analysts hacked into the SWIFT network, which carries most of the worlds banking transactions. Keeping a toehold, Rahab agents have since used their access to SWIFT for gathering intelligence on financial transactions throughout the world. [Schweizer p158-163] The BND gathers economic, industrial and other secrets just as the French DGSE; however the BND is considered less blatant in their activities. Through project Rahab, the BND hacks into corporate systems and government servers of economic competitors. Division I of the BND also gathers intelligence (including economic and industrial espionage), although typically through the more classic methods of spies, moles and blackmail. Targets of the BND include almost any industrial country, with past operations conducted against French, American, and Japanese companies.
Russian Federation	KGB, SVR, GRU	Russia's primary intelligence service is the Russian Federation Foreign Intelligence Service (SVR, sometimes called the SVRR), formerly the KGB. Russia is thought to have interest mostly in military secrets. Not much information available on Russian intelligence other than out of date cold-war era publications. Some examples of cold-war Russian projects are the RYAD mainframe (using technology from the IBM 360 and compatible with software written for the IBM mainframe) and the Agatha personal computer (using reverse engineered technology from the Apple II). (http://reformed-

		theology.org/html/books/best_enemy/chapter_05.htm) The primary Information security problem Russia poses is not specifically Industrial espionage, but a large pool of under-employed talent in the computer industry. As a result of the unemployment rate, there has been a growing incidence of Mercenary hacking with Russians as the source. (http://www.infowar.com/hacker/01/hack_080301a_j.shtml)
France	DGSE	France's primary intelligence service is the Direction Générale de la Sécurité Extérieure (DGSE), formerly the Service de Documentation Extérieure et de Contre-Espionnage (SDECE). The DGSE is divided into several departments. The branch 'Service 7' is responsible for foreign intelligence and conducts espionage against the U.S. and other countries. Service 7 specifically likes to target businesses using bribery, prostitution, wiretaps (using French telephone networks), rummaging through hotel rooms (mostly in France), going through people's garbage and planting moles in foreign companies. [Schweitzer p16]
Israel	Mussad, LAKAM, AMAN	Israel's intelligence agencies include Mussad and the agency formerly known as the Scientific Affairs Liason Bureau (LAKAM), part of the ministry of defense [Schweitzer pp17, 217]. Israeli intelligence has three main objectives: keeping tabs on neighboring countries, obtaining military and economic technologies, and affairs of state. Israel's interests in industrial and economic espionage largely grew out of events after the six-day war. After the war, countries that previously sold arms to Israel refused any additional deliveries. In order to maintain their military edge in such a hostile region, the Israelis took the logical choice and developed a program to acquire weapons technology by any means. LAKAM rose to the task, targeting military, nuclear, economic and industrial technologies. These secrets also used to bolster government owned weapons manufacturers as well as domestic industry. The efficiency of Israeli spying capabilities is apparent; Israel is now a nuclear power and a leading exporter in arms. It is believed that in the 1960's LAKAM stole over 200 pounds of enriched uranium from a processing plant in Pennsylvania [Schweizer p222]. The Uranium was then used to create nuclear warheads, making Israel a nuclear power. If any other country had tried that, the US would likely have gone to war. LAKAM was disbanded due to a scandal that arose around a naval intelligence employee, Jonathon Pollard, who was caught spying for them. Remnants of LAKAM are believed to still exist, although operating in a new form under the Israeli air force.
China	MSS	Guojia Anquan Bu, or Ministry of State Security (MSS) is China's main intelligence gathering agency. The MSS recruits students to do a large part of China's technology gathering, enticing them to return home after they have the desired knowledge. When money is not persuasive, threats against family members back home often are. "China's Ministry of State Security was formed by combining the espionage, intelligence and security functions of the former Ministry of Public Security with the investigations branch of the Communist Party's Central Committee" [Fialka]. Secrets targeted for acquiring include military, industrial, economic, technology, and details of civil servants private lives for blackmail purposes.

South Korea	NSP, KCIA	The NSP (National Security Planning Agency), formerly called the KCIA (Korean Central Intelligence Agency) is believed to have one of the most extensive spying operations around. The NSP operates in mostly Asia (against Japan and Taiwan), but also frequently targets American companies for industrial and economic espionage.
United States	CIA, NSA	While the majority of this paper has referred to foreigners spying on US companies, the US has also been found to engage in economic espionage. One of the most recent cases happened in 1995 when the French government publicly asked several CIA operatives to leave the country after details their exploits were published in a French newspaper. [Waller] Additionally, other countries are becoming more concerned about American intelligence agencies committing industrial espionage. Their main concern is the much rumored Echelon world-wide surveillance system. The unofficial stance regarding this concern seems to follow the sentiment, 'just because you would doesn't mean we are'. [Inquiry]

References

Barker, Garry. “Cyber terrorism a mouse-click away”. The Age. 8 July 2002. F2 Network. 24 Nov 2002. <http://www.theage.com.au/articles/2002/07/07/1025667089019.html>.

Blank, Denis. “Hacker Hit Men for Hire”. Ed. Alex Salkever. Business Week Online. 3 May 2000. The McGraw Hill Companies. 19 Nov. 2002. <http://www.businessweek.com/bwdaily/dnflash/may2001/nf2001053_930.htm>.

Blankenship, Loyd. “The Conscience of a Hacker.” Phrack. Vol. 1 Issue 7. 8 Jan. 1986. par 14. 22 Nov 2002. < http://www.phrack.org/phrack/7/P07-03>.

Cooper, David E. “Economic Espionage Information on Threat From U.S. Allies” GAO. 28 Feb 1996. Dec 20 2002. < http://www.loyola.edu/dept/politics/intel/t-nsiad-96-114.pdf>.

Dibowitz, Phil. “MSS Initiative.” 15 Dec 2002. 22 Nov 2002. <http://home.earthlink.net/~jaymzh666/mss/>.

Edwards, Cliff. “High-Tech Spy vs. Spy Keeping High-tech Secrets Is no Laughing Matter.” ABCNews.com. 19 Nov 2002. <http://abcnews.go.com/sections/tech/DailyNews/transmetaspy000701.html>.

Epstein, Edward Jay. “Ten revelations from the C.I.A.’s Tehran archives – the greatest loss of classified information since World War II.” Oct. 1988. 22 Nov. 2002. < http://www.jonathanpollard.org/7890/100088.htm>.

Fialka, John J. “China and Economic Espionage”. 17 June 1997. JEC Research & Studies. 24 Nov. 2002. <http://www.house.gov/jec/hearings/espionag/fialka.htm>.

Friedman, Steven M. Ed. “Corporate espionage in the 21st century” . 19 Nov. 2002. Eueopemedia.net. 24 Nov. 2002. <http://www.europemedia.net/showfeature.asp?ArticleID=13725>

GAO. “Economic Espionage: Information on Threat from U.S. Allies.” 28 Feb 1996. 26 Nov 2002. <http://frwebgate.access.gpo.gov/cgibin/useftp.cgi?IPaddress=162.140.64.21&filename=ns96114t.txt&directory=/diskb/wais/data/gao>.

Gellman, Barton. “Cyber-Attacks by Al Qaeda Feared Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say”. 27 June 2002. WashingtonPost.com. 22 Nov. 2002. <http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26>.

Gibson, Steve. “The Strange Tale of the Denial of Service Attacks Against GRC.COM.” 05 Mar 2002. Gibson Research Corporation. 22 Nov 2002. <http://grc.com/dos/grcdos.htm>.

Gray, Patrick. “Linux utility site hacked, infected”. ZDNet News. 14 Nov. 2002. ZDNet Australia. 17 Nov 2002.< http://zdnet.com.com/2100-1105-965800.html>.

“Hacker attacks on Government systems declining year-on-year”. Mi2g. 13 Nov. 2002. 22 Nov. 2002. <http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=/cgi/mi2g/press/131102.php>.

Harris, Shon. CISSP Certification. Ed. Betsy Manini, et al. Berkeley: McGraw-Hill/Osborne, 2002.

Hart, Michael S. The Art of War. Ed. Lionel Giles. May 1994. Project Gutenberg. 22 Nov. 2002. <http://ibiblio.org/gutenberg/etext94/sunzu10.txt>.

Ignatius, David. “Bungles, Bobbles and Spies; The Tehran Papers: Portrait of the CIA in a Maze of Its Own Design”. The Washington Post. 06 Sept. 1999. 25 Nov. 2002. <http://www.davidignatius.com/journalismSiro.html>.

Ingalls, Chris. “KING 5 Investigators: FBI used Fake Company in Cybersting.” 07 Feb 2002. K5 Investigators. 29 Nov 2002. <http://216.239.53.100/search?q=cache:_oiKhF2WfSwC:www.king5.com/localnews/investigators/NW_020602INKcybersting.78a5ea2.html>.

Ingram, Mike. “How the British government failed to suppress list of MI6 agents” Censorship in the Information Age.” 18 May 1999. World Socialist Web Site. 26 Nov. 2002. <http://www.wsws.org/articles/1999/may1999/int-m18.shtm>.

---. “British secret agents named on Internet: Former MI6 officer Richard Tomlinson accused of leak.” 18 May 1999. World Socialist Web Site. 26 Nov. 2002 <http://www.wsws.org/articles/1999/may1999/mi6-m18.shtml>.

“Inquiry of Alleged US Spy Tool Suspended”. 11 May 2002. TechTV. 20 Nov. 2002. <http://www.techtv.com/news/politicsandlaw/story/0,24195,3327239,00.html>.

“[ISN] Anti-globalist protesters turn to hacking”. 22 Nov. 2002. <http://www.landfield.com/isn/mail-archive/2001/Feb/0046.html>.

“The Jargon File”. The New Hackers Dictonary. 22 Nov. 2002 <http://www.tuxedo.org/~esr/jargon/html/entry/script-kiddies.html>.

Kellan, Ann. “Hackers hit government Web sites after China embassy bombing”. 11 May 1999. CNN.com. 24 Nov. 2002. <http://www.cnn.com/TECH/computing/9905/10/hack.attack.02/>.

Konrad, Rachel. “Leaks and geeks: International espionage goes high-tech” news.com. 21 Sep. 2000. Cnet. par 19-21. 22 Nov 2002. <http://news.com.com/2102-1001-242620.html>.

Leyden, John. “FBI sting snares top Russian crackers”. The Register. 7 Oct. 2002. SecurityFocus Online. par 6. 21 Nov. 2002. <http://online.securityfocus.com/news/1040>.

---. “DNS mega-hack hits thousands of sites”. The Register. 14 Sept. 2001 SecurityFocus Online. 22 Nov. 2002. <http://www.theregister.co.uk/content/archive/21689.html>.

Lockridge, Rick. “Female Hacker Packs a Punch”. Tech Live. 24 April 2002. TechTV. 18 Nov. 2002. <http://www.techtv.com/news/security/story/0,24195,3382211,00.html>.

Mann, Charles C. “Homeland Insecurity” The Atlantic Monthly Sept. 2002. The Atlantic. 10 Dec. 2002. <http://www.theatlantic.com/issues/2002/09/mann.htm>.

Matai, DK “The World Beyond 11th September. Focus on Asymmetric Warfare” 22 Oct. 2001. 22 Nov. 2002 <http://www.mi2g.com/cgi/mi2g/reports/int_briefings/221001.pdf>.

McDermott, Michael J. “‘I Spy,’ 1990s Style”. The Business Opportunity Handbook. par 24. 24 Nov. 2002. <http://www.busop1.com/ispy.html>.

McWilliams, Brian. “Fluffy Bunny No Longer Energized”. 29 July 2002. Terra Lycos Networks. 15 Nov. 2002. <http://www.wired.com/news/technology/0,1282,54040,00.html>.

Merriwether, Dan. “Kevin Mitnick: Timeline”. Takedown. 16 Dec. 2002. <http://www.takedown.com/timeline/index.html>.

---. “Takedown Timeline”. Takedown. 16 Dec. 2002. <http://www.takedown.com/coverage/mitnick-timeline.html>.

Mitnick, Kevin D, William L. Simon. The Art of Deception. Ed. Carol Long, et al. Indianapolis: Wiley Publishing, 2002.

Noland, John A. “You don’t have to be General Motors to be a Target”. Security Technology & Design. Aug 1996. par 14. 17 Nov. 2002. <http://www.the-centre.com/library/gm.html>.

[NIPC] “Terrorist Interest in Water Supply and SCADA Systems” 22 Nov 2002. <http://www.nipc.gov/publications/infobulletins/2002/ib02-001.htm>.

“OpenSSH Security Advisory (adv.trojan)”. 22 Nov 2002. <http://www.openssh.com/txt/trojan.adv>.

Peter, Laurence J. The Peter Principal. Buccaneer Books. Oct. 1996.

Richardson, Tim. “'Fluffi Bunni' hacker declares Jihad”. The Register. 14 Sept. 2001. 23 Nov. 2002. <http://www.theregister.co.uk/content/57/21668.html>.

Salkever, Alex. “The Breach That's Shocking the Firewall Industry”. Ed. Douglas Harbrecht. Business Week. 26 May 2000. The McGraw Hill Companies. 23 Nov. 2002. <http://www.businessweek.com/bwdaily/dnflash/may2000/nf00526f.htm>.

Schweiser, Peter. Friendly Spies. New York: The Atlantic Monthly Press, 1993.

Smith, Tony. “Hacker jailed for revenge sewage attacks”. The Register. 31 Oct. 2001. 24 Nov. 2002. <http://www.theregister.co.uk/content/4/22579.html>.

Sullivan, Bob. “FBI Software Cracks Encryption Wall ‘Magic Lantern” part of new ‘Enchanced Carnivore Project.’” MSNBC.com. 20 Nov. 2002. MSN. 22 Nov. 2002. <http://www.msnbc.com/news/660096.asp?cp1=1>.

Sutton, Antony C. The Best Enemy Money Can Buy. Studies in Reformed Theology. 2000. Capt. 5. 19 Nov. 2002 <http://reformed-theology.org/html/books/best_enemy/index.html>.

“Total Information Awareness (TIA) Systems”. Information Awareness Office. DRPA. 24 Nov 2002. < http://www.darpa.mil/iao/TIASystems.htm>.

Verton, Dan. “Are cyberterrorists for real?”. Federal Computer Week. 26 June 2000. FCW.com. 29 Dec. 2002. <http://www.fcw.com/fcw/articles/2000/0626/pol-terror-06-26-00.asp>.

Waller, Douglas. “U.S. Firms Face A Wave Of Foreign Espionage.” Phrack. Vol. 4 Issue 39. 4 May 1992. pg 58, 22 Nov. 2002 <http://www.phrack.com/phrack/39/P39-09>.

“What is EBITDA?”. 22 Nov. 2002. < http://www.investorlearning.ca/question/en-ca/FAQQ2002150710en-ca.html>.

"World: Asia-Pacific Sarin gas attacker to hang". 30 Sept. 1999. BBC News 22 Nov. 2002 <http://news.bbc.co.uk/2/hi/asia-pacific/461406.stm>.

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event