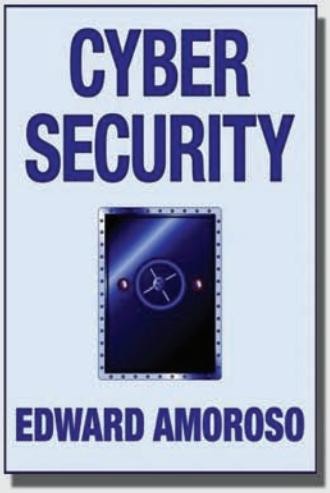

PURCHASE THIS BOOK

CYBER SECURITY

BY EDWARD AMOROSO

AN EXCERPT: CHAPTER 3 - THE EFFECTS OF CYBER ATTACKS

CHAPTER 3

THE EFFECTS OF CYBER ATTACKS

COMPUTER SECURITY EXPERTS have a favorite, albeit somewhat worn, joke question that they never seem to tire of posing to unsuspecting victims. Here's how it goes:

"So, have you ever been hacked?" asks the cyber security expert to the unknowing victim.

"Uh, no. We haven't been hacked," goes the response.

The expert then raises an eyebrow.

"You mean, there haven't been any attacks that you've *noticed*."

The point here, in case you missed it, is that you cannot measure what you do not observe. So, anytime someone says that they've never been hacked, you can challenge their claim as outlined above (hopefully without having to repeat this bad joke).

With this consideration in mind, I will state that to my knowledge no one has ever *noticed* catastrophic problems for government or business infrastructure as a result of cyber attack. Perhaps a massive e-catastrophe is occurring right now under our noses, but its effects have not yet been noticed. Again, you cannot measure or even comment on what you do not notice; my point is that nothing of enormous consequence and reach has been noticed.

Certainly, we have seen our share of cyber security-related effects across a range of computer and network systems. Peter Neumann from SRI International moderates a comprehensive list of reported risks to the public from computer malfunction and attack. A brief perusal of his list

(Internet search terms: Neumann, Risks) shows immediately that the effects of cyber security can be considerable.

Some familiar examples: Companies regularly get hacked and their email services are corrupted, especially by phishing attacks. Government agencies experience breaches that disrupt the services they offer. A school grading system is compromised by a thirteen-year-old who gives himself an 'A' in Earth Science. Individuals have their PCs infected with viruses that make it hard to run applications normally. Networks get infected with worms that cause volumes of packets to bring processing to a screeching halt. The list goes on and on.

In spite of these examples, we must acknowledge that while businesses, governments, and individuals have felt the negative impact of cyber attack, no digital Pearl Harbor cyber attack has been broadly noticed in any country or business. At the risk of beating a dead horse, we repeat that this *does not* mean that such attacks cannot ever occur. It just means that one probably hasn't happened yet – thankfully.

Four Types of Security Threats

If you were enrolled in my graduate course on cyber security at the Stevens Institute of Technology, you'd learn during the first lecture that the effects of cyber security attacks come in four flavors: disclosure, theft, integrity, and denial of service. Here is a brief list of what each entails:

Disclosure: This is when secret information leaks to the bad guys. This information could be credit card numbers, government secrets, battle plans, or your latest video rentals. The disclosure threat can cause a range of impacts from personal embarrassment to national security consequences.

Theft: This involves something of value being stolen. Network service providers worry quite a bit about this problem, which they refer to as fraud. In the telecommunications industry, fraud protection has matured steadily over the past few years – primarily to avoid lost revenue.

Integrity: This threat involves an asset being intentionally damaged. Examples include your PC being corrupted, files being infected, or some system attribute being changed. Any time a virus gets into your computer and causes problems, that is an integrity threat.

Denial of Service: This is when some service is intentionally blocked. This usually involves the denial of authorized access to network service or telephony. Some experts believe this to be the most difficult of all threats to deal with effectively.

As we will see, security in computing is thus not some monolithic notion, but rather a spectrum of damage that can occur with respect to computer and network systems. “Bad things,” writes Ian Witten in a classic 1987 essay about cyber security, “range from minor but rankling irritations, through theft of information, to holding users ransom.”

For example, consider that the theft of someone's personal identity is quite different from the theft of wartime logistic information – even though both would be referred to as security issues. Similarly, blocked access to a financial Web site is quite different from blocked access to a children's game site. In either case, a very different constituency (and age group) would be targeted in the attack. Furthermore, different attack motivations and methods would be employed in the security solution.

To properly understand the true consequences of cyber attack, we need to zero in on these four different types of security threat – focusing on their history, impacts, likelihood, and preventive measures. The resultant insight will not only help the reader better

understand cyber security, but will also highlight some serious public issues for the protection of critical infrastructure.

Disclosed Secrets

The disclosure threat involves sensitive information falling into the hands of bad guys. In the context of national cyber attack, bad guys are probably a given nation's hated enemies. For Americans, this could range from al Qaeda terrorists, to organized cyber attack groups stealing information from sensitive government or corporate systems.

Ordinary individuals tend to worry about disclosure in the context of their personal information. Imagine, for a moment, that you've left a copy of your tax return papers on the copy machine at the office. You'd probably drive fifty miles in the dead of night to retrieve it. The obvious problem is that when this sort of information is available on-line, then all the driving in the dead of night will provide no protection whatsoever. Furthermore, an on-line attack doesn't require proximity.

One curious and rarely discussed aspect of people's private lives involves on-line browsing habits. If a person's browsing habits are mundane, then compromise might be of no consequence. But for those who enjoy visiting more marginal sites, this information is often best kept private. Your service provider, for example, should protect this information from prying eyes – including those of their own employees. "There's a fine line between customer service and stalking," writes cryptography expert Bruce Schneier.

In the mid 1970's, United States government researchers began seriously studying the disclosure threat as it related to computers. This early research wasn't so much concerned with personal information as it was with traditional Cold War tensions. As a result, the vast majority of early disclosure research was preoccupied with the threat that the Russians would use computers to peek at American military secrets.

Two creative researchers from the Mitre Corporation, David Bell and Len LaPadula, were among the first to publish meaningful results in this area. They examined how the United States military protected paper documents. They looked at the process of document classification, which allowed the military to define which people could gain access to which types of information. They found that a document classified as top-secret, for example, could only be read by someone with a top-secret clearance. Similarly, an unclassified document could be read by anyone.

Bell and LaPadula quickly realized that this disclosure concept could be applied to the multi-user, shared computers that were coming into use at the time. Their approach worked roughly as follows: All of the information on a shared computer would be marked to some security classification, such as secret or top-secret. Then, all users on that system would be associated with clearances, generally based on their background or job function. The operating system on the computer would enforce the desired security policy.

In practice, things were more slightly complicated because the military partitions information into "need-to-know" categories. Thus, within the top-secret classification, data must be compartmentalized into more specialized groupings. To manage the complexity, most classified government projects – then and now – employ teams of people to keep the security scheme straight. Bell and LaPadula knew that the computer version of this would require similar administration.

Some Unix-based computer operating systems were actually built in the 1980's to implement this type of military security policy. At AT&T, Chuck Flink led an effort aimed at trying to get the concept correct for Unix. The resulting system, referred to as multilevel secure, could enforce the familiar policy that highly cleared users could read any file in any directory, but that lowly cleared users were restricted to less sensitive

information. Thus, a user would have to be cleared to top-secret to open and read a top-secret document. So far, so good.

But the policy also stipulated that highly cleared users could not write information into lesser-classified documents. This ensured that classified information didn't find its way into an unclassified document. An assumption was being made here that users logged into the system in "top-secret" mode, could only generate top-secret information. This is not a reasonable assumption, but it was made nevertheless.

Furthermore, the policy allowed for lesser-cleared individuals to write content to pretty much anything they wanted. After all, what was the harm in unclassified information making its way into a classified document? The result of this was the weird anomaly that unclassified users could write information into a top-secret document, but could not then read or review what they had written. This was called a blind write. (Are you confused yet?)

The clumsiness and inconvenience of such operation, combined with a generally low concern for computer security across the globe at the time, dealt multilevel secure systems a painful blow. As the public Internet and the Web emerged, most computer users' tolerance for restriction of information grew even lower. After all, what was the Internet for, other than to share, rather than restrict access to data? Products that supported military disclosure functionality died slow and painful deaths.

Since that early research, very little progress has been made in the prevention of disclosure threats on computers. Some researchers have since created more refined mathematical models of disclosure based on how people deduce information. But to be honest, very few people in the computing community even noticed this work. It didn't help that most of these papers could only be understood by people with PhD degrees in very specialized branches of mathematics.

Encryption has certainly been one method that has been used at length to try to prevent disclosure problems. Encrypting data has always worked especially well for information that is in transit. The military encrypts voice, for instance, using special "secure" phones. To listen in, the enemy would have to tap and decrypt the information in real-time – a task that has proven particularly difficult for good encryption methods.

When information is stored, however, encryption protection hasn't proven as dependable. One reason is that the keys used to decrypt stored information must be stored. If these keys are lost or mishandled, the information could be lost forever. This leads to baroque escrow schemes in which third parties keep emergency copies of the key information. Law enforcement has taken the extra step of suggesting that such escrowed keys could be used to decipher encrypted conversations. As you might guess, this has not been a popular suggestion.

In spite of all this, organizations have not stopped trying to create encryption schemes for protecting both their in-transit and stored information. The payment card industry, for example, recently enacted a series of privacy-oriented security requirements on its participants. These requirements include provision for encrypting all customer sensitive data. This turns out to be especially difficult for legacy applications that include no support for such encryption.

Ironically, many of the companies in this industry have wasted more time complaining about the problems implementing encryption than they have actually trying to create a workable scheme. Time will tell whether encryption of stored information has much impact on prevention of privacy problems.[1]

The potential disclosure of information in enterprise networks run by organizations is often addressed poorly as well. Most companies tend to operate their entire network at one common security level – usually

[1] By the way, disclosure issues, in a personal context, are referred to collectively as privacy.

something related to proprietary markings. In most companies, the perimeter of the organizational Intranet is the vehicle for such protection. So, if you are a legitimate employee, then you can see everything; otherwise you aren't able to see anything – or at least that's the intent.

The perimeter protection of an Intranet is typically accomplished using devices called firewalls. The sad news is that firewalls can be penetrated or by-passed quite easily in most environments. Furthermore, Intranets are notorious for having unauthorized and unknown connections to the outside through which bad guys can gain access and peek at information (Hint: think WiFi). As a result, disclosure protections in many organizations are little more than a sham.

Suppose, for example, that you are an evil criminal and you want to obtain intellectual property and sensitive information from Bank XYZ. You could try to hack your way in, but that might be messy. Perhaps a better approach would be to just apply for a job at the bank. Then, once you're at your new job, you build a volume of downloaded information from their Intranet (you're an employee, remember?). After you have what you want, you can quit and move on to the next bank. It's reasonably foolproof in most environments.

For information stored on PCs, the disclosure threat is addressed through mostly non-technical means. Specifically, most people will try to delete what they do not think they need, such as their temporary Internet files and any cookies that might reside on their hard drive. They will then protect the remaining files and data by simply turning off the PC and, if it's a laptop, storing it in the closet.

We all know, however, that when PCs are connected to networks, they are immediately exposed to all sorts of security threats. This is not to say that every time you connect your PC to the Internet hackers peek in at your checking account, but there are often no controls to ensure that this cannot happen.

Theft

Suppose that a well-dressed young man hops aboard a southbound Amtrak train in Baltimore. It's very early in the morning, and hardly anyone else is on the train. The conductor comes over to the passenger requesting a ticket, but the young man pleads for mercy.

"Sir, I don't have a ticket because I don't have any money," he explains. "I'm on my way to an interview in Washington. This is my big chance. Can you please let me ride without paying?"

The conductor frowns.

"Please, sir," the young man pleads. "There aren't many other passengers in this entire car. I'm not bothering anyone. My presence is having absolutely no negative effect on the operation of this train. Can't you please let me ride down to my interview in Washington for free?"

The conductor takes off his cap and scratches his head as he ponders this little dilemma. What harm, he wonders, is this kid really causing? He knows that Amtrak is a big company and if the young man is allowed to ride for free, maybe some good will come if it. Maybe he will even bring the money back later, after he gets his job.[2]

This train conductor's dilemma is similar to the fraud decisions that security engineers must make as they ponder the impacts of theft. Service providers, in particular, have been forced to consider such scenarios in great detail. The services in question are most often telephony or Internet access, and the excuses for theft are just as creative and real as we saw with the young man riding the train to Washington.

You probably already know that theft of phone and Internet services is so common that some youngsters believe it to be a socially acceptable activity. The early activist Abbie Hoffman urged his followers to rip off the phone company at every opportunity. Today, the hacking community openly targets

[2] When I pose this scenario to my students, the responses are split between throwing the bum off and showing mercy. I have no idea what this means other than that half are destined for upper management (I won't say which half).

telecommunications in their mischievous explorations. In response, most phone companies today have established large security and fraud divisions that deal on a day-to-day basis with people trying to steal service.

It turns out that stopping fraud on the Internet is a bit more difficult than with traditional voice services. The identity and location of end points, for example, are tough to accurately determine on the Internet. Furthermore, the motivation to stop Internet theft is somewhat more complex than with voice service. For example, if someone is stealing expensive minutes on your long distance service, then it pays to stop this. But if someone is stealing time on an Internet or voice account that is already flat rate for unlimited use, then what's the problem? Would you even notice if someone was occasionally borrowing your on-line account to browse the Web?

Identity theft is the newest form of cyber theft, and it is rather alarming in its potential consequences. The most common identity theft method involves the use of a technique known as *phishing*. In a typical phishing scam, email notifications are sent to unsuspecting users that they must take some immediate action, such as re-enrolling for their Internet service by supplying personal information. Bogus Web sites on hacked systems are often established to support such theft operations.

"Warning," such messages might start, "to ensure the fine quality of service you are used to, you must immediately go to the following Web site (the link would be embedded) to verify your account information. We'll need your email password, your mother's maiden name, and your social security number. Failure to take this action immediately will result in your account being terminated."

Once the unsuspecting user visits the Web site and provides this private information, the thieves grab it, catalogue it, and sell it. Such information might end up in the hands of people who will charge items to your credit cards; or it could end up in the hands of criminals who sell identities on underground Web sites; or it could be placed in the hands of a cyber criminal using this information to establish anonymous on-line accounts. All of these are frightening prospects.

Unfortunately, few good solutions exist to stop phishing. A recent study in the State of New York showed a that sizeable percentage of employees sent a test phish, went ahead and took the bait. Many took the bait again, after being warned that the original phish was a test! So while end-user education and awareness campaigns are necessary, they don't always work too well.

One promising technique that has been discussed involves using stronger forms of authentication for any type of interaction between, say, a bank and its customers. The idea is that you would be issued something like a hardware token by the bank when you agree to do on-line banking. Thus, even if your identity were stolen via a phishing attack, the thieves would not be able to clean out your checking account unless they also had your hardware security token. This may be a good approach, but it has sizeable cost implications.

With the recent rush of phishing attacks, companies have now begun to take serious notice of the threat. While many companies remain ambivalent about employees being caught in identity theft scams, as phishing scams have expanded in scope, organizations now realize that viruses can be delivered to the enterprise via this technique.

The paradoxical result is that companies are now being forced to address fraud, not so much to protect the personal information of their employees, but rather to preserve the integrity of their corporate computer and network systems. Regardless of the motivation, one should expect the risk of identity theft and phishing problems to diminish for those who access the Internet from an organizational Intranet.

For normal citizens, one already sees service providers beginning to accept the task of protecting their users from these types of scams. Certainly, extensions to anti-virus and anti-Spam software packages exist to help identify theft situations in various types of malware, but the truth is that people remain pretty gullible. The only protection many Internet users will ever have is if some omnipotent provider steps in and makes the problem go away. This is not easy, but the benefit is significant enough that we should expect broadband providers to begin working this more aggressively.

In the meantime, my advice is that if you receive an email asking you to supply any sort of personal information, even if it appears to be coming from someone you trust, please reach for the delete key and just say, "no."

Destroying and Deleting Assets

Several years ago, a team of young New York paralegals had just finished working days and nights preparing a lengthy legal document. They'd worked like dogs getting every sentence perfect and every punctuation mark just so. After all, even a minor error in this document could change its meaning and cost the firm millions.

Just before the document was to be printed and delivered to the court, the paralegals were all called into a room and fired. While they were packing to leave, however, one person decided to take some revenge. He went back to the computer and made a few creative adjustments in the document – ones that would be tough to find. In computer security terms, we would say that the integrity of the overall document was degraded. Its validity was now in question and its contents could no longer be trusted.

This law firm might have protected themselves from such an attack by a few simple steps. Treating their employees with respect would have been a good start, since removing the motivation for an attack is always the best approach. But functional strategies do exist for ensuring integrity in a business-computing environment. They could have had back-ups; they could have had a change-tracking system; they could have been monitoring audit trails; they could have had access controls on the document to prevent unauthorized change; they could have had business controls on dealing with fired employees; the list goes on and on.

But the truth is that most companies and groups do not have decent protections from this integrity threat. Most organizations rarely back up anything but the most critical information. How often does the typical computer user, for instance, back up the routine files on their PC? Once a day? Once a week? Ever? Furthermore, unlike the disclosure threat, which received considerable attention in the early years of computer security, the integrity threat has been largely ignored by researchers and funding authorities.

Back in the 1970's, a Mitre researcher named Ken Biba was studying the integrity problem, largely from the perspective of protecting military systems. He came to the conclusion that integrity, unlike disclosure, was really just a measure of one's expectation. A person of high integrity, for example, is someone you can trust, someone who lives up to a high expectation. Similarly, a high integrity document is one that is correct, has value, and has not been tampered with.

Biba also observed that people with high integrity routinely avoided documents of low integrity. This is why we prevent children from viewing low integrity materials, like certain magazines and Web sites. If we did not take this preventive measure, then our children would be presumably corrupted and their integrity would be irrevocably reduced. Some people joke that exposure to low integrity materials causes us all to start

life with the highest level of integrity – and then throughout our life, we embark on a constant process of ever-dropping integrity.

Low integrity individuals are also routinely prevented from contributing to high integrity documents. It's sort of like stopping a profane, vulgar person from changing passages in an important religious document. The information entered by the low integrity individual would have the effect of lowering the integrity of the document. A much better approach, of course, is to prevent this from occurring in the first place.

Biba tried to apply these observations to computer systems and interesting results emerged. One interesting Unix system developed at Bell Labs in the 1980's used Biba's approach to protect itself miraculously from worms.[3] It kept low integrity programs connected to networks from ever writing anything into the high integrity systems files. Bell-La Padula controls were then imposed upside-down to enforce the separation. The system gave you a bit of vertigo, but it worked like a charm.

You'd think that such functionality would be useful today. Unfortunately, systems like this didn't sell, because information technology managers deemed them too inconvenient. I wonder if these managers have since bothered to measure the inconvenience of responding to an endless stream of network viruses on their systems. Perhaps the inconvenience of using a more secure system might not seem so bad in comparison.

In the 1980's, another research project had some influence on our collective thinking about integrity in the cyber security community. The project was led by David Clark, a computer scientist from MIT, and David Wilson, from the accounting firm of Ernst and Whinney. Their work resulted in what we now know as the Clark Wilson Model. Several working groups were created in the late 1980's and early 1990's to determine how this model could be used to improve integrity protection on computer systems.

The model is based on the observation that the integrity of computing environments could benefit most from the types of things that businesses do to make sure their financial books remain in order. They explained that performing tasks such as ensuring valid transactions, logging all activity, ensuring good back-ups, and allowing only certain people to access certain important assets, would prove useful to engineers trying to ensure integrity.

The basis for the model is similar to how your checking account works. Every transaction you log in your checking account starts with all entries in a valid state (you hope). Once you complete a transaction, such as writing a check or making a deposit, you perform the associated log entry to make sure everything remains in a valid state.

Clark and Wilson reasoned that computer systems could be designed in the same way. Only valid transactions could be allowed to occur on systems that were already in a valid state. Mathematicians cleared things up for the masses by explaining that this part of the model produced something called "inductive closure."

Unfortunately, this concept turned out to be much easier said than done. How, for example, would you demonstrate validity for a PC running the Windows operating system and the usual set of popular applications? Or how could one ever state, for instance, that such a system is in a valid state if it must be patched every month? Or how could one ensure that only valid transactions are allowed to occur when viruses and other malware find their way onto our systems so easily?

In the end, the Clark-Wilson model was excellent theory, but too difficult to implement in practice. Most security experts are ignorant of the model, and almost no real systems have been built using the basic tenets of

[3] By the way, disclosure issues, in a personal context, are referred to collectively as privacy.

the model. This is a shame.

So how do we maintain integrity in computer systems? For the most part, we don't. People buy a home computer at Best Buy, plug it into the Internet and then use it to browse and send email. Over time, the system becomes increasingly muddled with viruses and Trojan horses. The anti-virus license expires, and soon the whole system becomes unusable. The result is that person goes out and buys a new system - and the cycle begins again. As you would guess, the computer industry has no problem with this approach.

Mind you, security tools do exist for detecting changes to a system. These tools often scan the target system periodically looking for anything that might have changed. A couple of decades ago, Fred Grampp from Bell Labs invented the first such program - one that scanned a Unix system for vulnerabilities. It checked for unused accounts, programs with too much system privilege, bad passwords, and so on. Computer system administrators do this routinely now, but the whole process traces it lineage to this early work at Bell Labs.

Now that I've said such nice things about Fred's scanning program, let me offer a sobering reality: a professional cyber terrorist can attack systems without breaking a sweat at scanners. Computer scanners are designed to test for known problems. If some previously unknown or unreported problem happens on your system, then a scanner will not be able to detect this in any way. [4]

You may not know this, but the software you buy for your home computer might be embedded with intentional Trojan horses before you even unwrap and install the software. These gems, referred to as Easter eggs by software developers, are inserted quietly into code and represent an artistic means for the authors to sign their work. For example, recent versions of Microsoft's Excel program could be turned into a flight program where you fly over bumpy terrain in search of an engraved stone. Engraved on this stone were the names of the developers.

Similarly, an earlier version of Microsoft's Word program could be turned into a pinball machine by a simple sequence of points, clicks, and simple text entry. I've demonstrated this frequently, and people are consistently floored at how little they understand about the software on their computers. Here is something I think we all agree on:

No justification exists for intentional Easter Eggs or Trojan horses, however innocent, to be placed in software by developers.

Unfortunately, no evidence exists that the integrity of critical infrastructure systems is protected more effectively than in home settings. This could be obvious, such as when a power plant or emergency service environment includes the types of virus-prone PCs you might find in the home. But it could also be more subtle, such as when custom developed software contains integrity problems due to insufficient levels of assurance and verification performed during development.

This does not mean that the most recent virus to hit your PC could also take out the computers in your local nuclear power plant. But you never know.

Denying Service

The concept of denying service is easy for most people to grasp. See if any of the following analogous scenarios are familiar to you:

- You're in a rush to get to work, but the traffic is so thick you can barely move ten feet.
- You're trying to get onto an important conference call, but the signal on your cell phone is too weak to connect.
- You're watching the World Series and it's the ninth inning of a tie game during a crucial at-bat, and your satellite coverage suddenly goes out.

When these scenarios occur, we generally just resign

[4] Fred Grampp receives little credit for his pioneering work in scanning. Industries are based on concepts he invented - and people don't know his name.

ourselves to the fact that stuff happens. And we deal with it.

But imagine if, in addition to your inconvenience, you also knew that someone was *deliberately* causing this situation. Imagine if that traffic jam was being caused intentionally to make you late. Or if your cell signal was being degraded for the sole purpose of keeping you off your call. Or if television coverage was shut down to keep you from watching your game. Such infuriating situations correspond to the denial of service threat.

Stated explicitly, denial of service in cyber security involves a malicious intruder intentionally blocking an important computer or network service from its authorized users. Note that denial of service does not correspond to accidental or unintentional outages. Rather, the threat involves someone causing the problem deliberately.

Examples of this abound. Perhaps you are a war fighter and need some on-line tactical information, only to find that the enemy is actively blocking your access. Or perhaps you run an emergency service, and during a serious life-threatening situation, you are blocked from accessing some important system by some hacker. Or maybe your shipping business allows customers to check package delivery on-line. If a virus or worm floods your site and makes it unavailable, then you are the victim of a denial of service attack.

In a crude sense, repeatedly calling someone on the telephone is a type of denial of service. By calling your victim over and over, you are rendering their phone essentially useless. Methods for dealing with this problem include pleading with the caller to stop, contacting the phone company, or notifying the police. Most of the time, these methods will work for basic telephony because it's relatively easy to detect the source of crank phone calls.

Unfortunately, this threat is more difficult to defend against on the Internet. Linking IP address information associated with an attack to the true attack source is extremely difficult due to the ease with which intruders can weave a pattern across the Internet. Furthermore, there is the basic physical principle that if a system can only handle so much capacity, then attackers can simply initiate malicious activity that will exceed that capacity.

How Serious is Cyber Terrorism?

I already know what you're thinking. Cyber security threats don't seem anywhere near as bad as hijacking, truck bombs, and biological weapons. While this may be true, there are two issues that must be considered:

1. All forms of terror can include a cyber component - in fact, some can be directly controlled using computers.
2. Serious inconvenience, disruption, and even misery can be created via cyber attacks.

Most people tend to ignore these issues, perhaps because the effects of cyber security attacks are sometimes less obvious. Here's a story to illustrate: Just after 9/11, I watched live panel discussion on how to prevent future airplane hijacking. One of the experts on the panel endorsed the concept of ground flight control of airplanes to deal with an on-going hijacking. The idea would be that if a plane were hijacked, air traffic control would somehow take over the flight controls and render the hijackers unable to fly the plane from the cockpit.

To my amazement, everyone thought the idea was marvelous, but beyond our technical capacity. I could hardly believe that they were completely ignoring the hacking potential here! Can you imagine the security threats that would emerge if terrorists didn't have to actually get onto planes, but could rather break into

ground flight control networks and remotely control the planes from a network? The very idea makes me dizzy.

Calculating Security Risk

With these frightening threats to systems, you might find yourself wondering how suitable protections are identified. You might also recognize the difficulty of countering threats on the inevitable limited budget that organizations and individuals have for cyber security.

For critical infrastructure systems, this is handled through an engineering practice known as risk management. In particular, security professionals measure and manage risk to computer and network infrastructure using a simple equation: They multiply an estimate of the likelihood of an attack by an estimate of the consequences of such attack.

Obviously, this requires some sort of numeric measures to be used as estimates. Perhaps after some consideration, the security engineer might decide that likelihood of attack and consequence of attack would each be given a rating of 3 for high, 2 for medium, and 1 for low. These numbers might seem arbitrary, but when put in use, they help to demonstrate important relationships.

For example, a system with high likelihood and high consequence of attack would have a risk equal to 3 times 3, or 9. If some step is taken to reduce the likelihood of attack from high to medium, then the risk is lowered to 2 times 3, which is 6. Similarly, if the consequences of the attack are lowered, then the risk is lowered as well, and so on.[5]

This notion of risk being proportional to both the likelihood and consequences of attack is fundamental to how we create security defenses. Think about seat belts, for instance: We would never dream of putting a baby into a car seat without buckling, simply because the consequences of an accident are too high for that baby. When adults get into our car, however, we might be more ambivalent about whether they buckle. This is because we measure the consequences as being lower.

I have a friend who was a jeweler in a strip mall in New Jersey. After a long career, he closed his shop, but decided to re-open on a smaller scale in the basement of his home. This introduced some risk problems in his home. First of all, the consequences of a break-in increased dramatically since he was now storing valuables in his home. And second, the likelihood of an attack increased simply because people were now coming into and out of his home, knowing that valuables were present.

In order to better understand the consequences of cyber attack on national infrastructure, let's take a brief look at how cyber terrorism could affect several of major critical system components.

Are the Phones Working?

Many people around the world continue to rely on circuit-switched telephones - the ones that provide only a keypad and receiver. They are connected to copper lines that run out to traditional public switched telephone network lines. You probably do most of your talking on a traditional circuit switched phone in the kitchen of your home.

Perhaps more importantly, these phones are typically powered via the trickle of current coming over the phone line. This is critical, because when there is a power outage in an area, it is often the case that people with feature-rich phones requiring power are unable to make calls. Many are forced to use their cell phone, perhaps plugging it into the car for power. In contrast, those with the less feature-rich circuit switched phones are typically unaffected.

I'm not saying that modern telephones are undependable. What I am saying, however, is that we

[5] Jon Weiss, now at Lucent, led a group at AT&T in the mid-1980's that invented the use of threat trees to calculate risk based on these equations.

have traded a bit of resiliency in our telephones for the added flexibility that comes with powered devices. Obviously, voice services over the Internet – the familiar VOIP capability so aggressively marketing today – carry this notion to an extreme.

The telecommunications infrastructure in the United States can be grouped specifically into a few basic components: First there are the large transport carrier groups who own miles of underground fiber. These networks support long haul transport of phone calls, data, video, and Internet browsing sessions. Such transport systems are like the super highways in our freeway system – they let you go fast, and they are generally well maintained. But you also need a system of off-ramp highways.

The second component in the American telecommunications infrastructure includes the local phone, cable, and satellite providers, who own the wires connected to buildings and the sides of everyone's garage. These local companies also support voice, data, video, and Internet for customers. They correspond to the local roads and off-ramps in our highway system analogy – they are close to home, tougher to maintain, and don't let you go as fast. Many of these companies are now deploying fiber to the home to increase their ability to sell bundled services.

The third component in our telecommunications infrastructure includes wireless companies. These companies make use of the infrastructure provided by long haul and local providers, but they also operate towers to which you can connect with your cell phone and other wireless devices. The integrity of the connection path between your phone and the nearest tower obviously varies across regions – as you recognize whenever your signal is dying during an important call.

So what are the cyber security risks to telecommunications in the United States? In considering this question, one must recognize that telecommunication networks provide the means over which most cyber attacks are likely to occur. For this reason, many experts posit that a massive cyber attack on any nation would not involve any tampering with basic communications backbones. This would be like destroying the roads before a ground attack.

Keep in mind, however, that if the purpose of a cyber attack is to deny access to landlines, cable television, mobile telephony, pagers, email, Internet access, or even instant messaging, then telecommunications could easily be targeted. For hackers, this could be attractive, if only for the attention such an attack would be given. From the perspective of massive cyber attack to infrastructure, if basic communications are obliterated, the effects on a target nation could be more effective than conventional weapons.

Denial of service is not the only type of threat to national telecommunications systems. We all know that citizens, corporations, and government organizations regularly send and receive valuable information over telephones and computer networks. Such information is obviously much more at risk if someone has managed to infiltrate the telecommunications provider's systems for the purpose of listening. This is certainly unlikely, but must be considered.

During the majority of the past half century, proprietary circuit-switched technology was used for telephone and data connections. This approach proved to be highly reliable in supporting national telecommunications needs, as you probably observed. Furthermore, the limited exposure to the basics of proprietary telecommunications did have a throttling effect on the number and type of attacks that were present.[6]

With the advent of the Internet and its open, non-proprietary services and protocols, however, interesting new opportunities have arisen for hackers. This results in a Catch-22 situation in which our open technology prevents hidden catastrophic vulnerabilities, while at the same time allowing any known

[6] Be careful with this point. Security experts refer to this type of protection as "security through obscurity," and it has obvious drawbacks when adversaries do obtain information about a target system or technology.

vulnerabilities to be known by *everyone*. Think of Internet technology as being in a glass house.

Perhaps more worrisome is the threat that arises when shared telecommunications services are operated across the Internet through collective agreements. The Domain Name System (DNS) and the Border Gateway Protocol (BGP) are two examples of Internet utilities that many experts view as being almost trivial to disrupt. In both cases, individual groups can inject bogus changes to the Internet infrastructure, with no centralized (or even distributed) police force to stop them.

As you might guess, this produces enormous risk to any telecommunications service that relies on the integrity of the Internet. Email, web services, and any types of electronic commerce rely directly on jointly operated services such as DNS and BGP. The cyber security risk here is considerable, and is poorly understood by policy makers in most countries.

What Happened to the Power?

Human beings are dependent on power – period. Except in the most remote and extreme areas, extended losses of power bring great hardship onto residents and businesses. As such, we must presume that cyber terrorists already understand the target-rich environment that exists in any nation's power systems.

Power generation systems are, for the most part, either conventional or nuclear. Both involve complex systems that heat water to produce steam. This steam is used to drive turbines that generate electrons onto a massive transport network of power lines. The high voltage electric power carried on these lines is gradually reduced to levels that are safe for distribution into your home and business.

Power systems generate waste, employ large numbers of human beings, include huge physical plants, rely on massive electromechanical systems, and include many, many computers and networks. Such computers and networks are of obvious interest to the cyber attacker, especially where nuclear power and waste products are being generated. Of course, attackers fully understand that you don't just break into a core reactor. A better approach is to target the computer systems that might be connected to, or contain critical information about, a core reactor.

Now, cyber terrorists with a broadband connection cannot cause a Chernobyl-like disaster at your local nuclear power plant. But this does not imply that cyber terrorism is a non-issue for power plants and systems, especially in the United States. In fact, serious national consequences can occur as a result of the dependence of this industry on computer and network systems.

The software, for example, that is embedded in power plants appears to be no more reliable or secure than any other software developed for less critical applications. Recall the scenario mentioned in our first chapter in which the Nuclear Regulatory Commission discovered a safety monitoring computer program with a serious bug. The likelihood that additional bugs might be present in similar software would seem pretty high.

The major power system-related question for most readers is this: Can cyber terrorists shut off the lights in my home? The answer is maybe, but the likelihood improves greatly if cyber terrorism is combined with more conventional terrorist measures. For example, if the objective is to remove power service from a specific region, perhaps by dropping a bomb onto a physical power distribution point, then cyber terrorists might use electronic means to obtain maps of how the distribution is designed.

Terrorists might also try to obtain sensitive information about power system vulnerabilities in a

given system, especially if they can place insiders into a target power company. The insider problem is certainly not unique to the power industry, but the consequences of malicious insiders in this industry are obviously considerable.

Where's the Money?

During the morning of 9/11, I stood with so many others on the streets of Washington, DC, watching in horror as a black plume of smoke rose up from the Pentagon. Almost instinctively, I went to an ATM and drew out as much cash as it would give me. Some readers might argue that such action is inappropriate, because it contributes to public panic, and they may be right.

But this does illustrate the importance of financial soundness in times of national stress. If the ATM in Washington had not given me cash on that morning, it would have just made an already horrific day much worse. The story also illustrates the responsibility that the owners and operators of financial services infrastructure have to maintain soundness in their systems and to avoid any types of cyber security catastrophes.

The good news is that considerable emphasis has been directed toward reducing security risks in the financial services industry. This includes the massive investments made by businesses to reduce fraud over the past decades; but it also includes the substantive initiatives being worked across most banks today to protect their computers and networks from hackers, criminals, and cyber terrorists.

One insider problem that banks have seen is the so-called salami attack. This involves repeated theft of small amounts of money. For example, a dishonest clerk might steal a few cents from the travel reimbursements of employees over a large period of time. No single transaction would raise an eyebrow, but in aggregate, the theft can be significant. In the United States, Sarbanes-Oxley controls have reduced the risk of this attack somewhat. But the potential remains.

Banks must also address phishing attacks in which account-related information is stolen from their customers. The theft is done via a familiar, but bogus request that victims supply personal information to avoid some unpleasant or annoying action. Unfortunately, there are no good solutions to the problem currently – and it's only a matter of time before banks begin to retreat from their Internet strategies to avoid the risk.

In the mid 1980's, a group of security consultants from AT&T met with system managers from a large investment bank in New York City. The bank apparently was running applications that transferred sizable payments to creditors every Friday afternoon at 3:45 PM. This transfer had to be reliable because late payments carried penalties.

Things worked fine for years, but they suddenly began to notice unexplainable problems with their network just before 3:45 PM every Friday. Everyone suspected insider financial sabotage because the source of the trouble jumped around in a random manner, almost as if to avoid detection. The team tried hard to pinpoint what was going on, but could not obtain accurate evidence.

Ironically, the problem stopped once the consulting group began establishing a more visible presence at the bank. Everyone presumed that the malicious insider probably noticed the ragged-looking security engineers wandering around the trading floor, and just figured that the heat was getting a bit too close. So in the end, the attack stopped.

But this incident left me with an uneasy feeling. The attack, if indeed it really was one, could have targeted great sums of money. Furthermore, the fact that a team of trained forensic security experts could

not locate this problem illustrates, in a small way, the potential for a scenario that might have more serious consequences for the financial sector.

Citizens of most companies are totally reliant on computer and network systems for their personal financial needs. Many view access to their money using an ATM machine, for instance, as a basic human right. In addition, businesses obviously rely on the availability of financial systems to support their day-to-day operational needs. Their supply chain management, their point of sale systems, and their advertising and marketing methods are all heavily dependent on computing.

Another point, made resoundingly clear on 9/11, is that the software, computing, and networking infrastructure supporting financial firms are as vital (if not more) to operations as the structural integrity of buildings. Anyone who believes that such cyber infrastructure will not be targeted more aggressively by a future cyber terrorist attack is simply not being realistic.

Furthermore, the customized software powering the financial infrastructure is increasingly developed in non-traditional ways. Much of this software development, for example, is performed in countries for which the link between government and industry is somewhat blurred. This may be fine, but the result is that these countries now have a direct pipeline to the software powering critical financial systems. The presence of such access certainly must be factored into any estimation of national security risk.

Three Thousand Tooth Brushes to Iraq?

Cyber attacks pose an interesting dilemma for the military. Specifically, if a domestic enemy attacks domestic infrastructure, then most countries view this as a law enforcement issue. This complicates how the military deals with cyber security for two reasons:

- Domestic infrastructure attacks could have strategic military importance.
- The geographic location of some attack source is tough to reliably determine.

The military in most countries includes three components. There is a strategic component tasked with the overall planning, architecture, and methodologies to be used in theater and non-theater engagement (a theater is a place where you fight a war). There is also a tactical component, empowered to perform the steps involved in dealing with a real-time situation. And there is the sustaining base component, which involves the systems that allow military organizations to function. This includes payroll systems, families benefits, food preparation, and on and on.

This distinction is important because so often we hear the phrase "hacking the military," without any information about what specifically is being attacked. We presume immediately when we hear such talk that hackers are using computers to run tanks into walls or to cause airplanes to lose contact with the ground. More likely, such cyber attacks generally focus on military Web sites, part of the non-tactical, non-strategic sustaining base.

The military has tried to assess its level of risk over the years through a series of calculated exercises. Back in the late 1990's, several exercises were run in which good guys broke into military computer and network systems. The good-guy attack team showed that by taking their time and avoiding obviously detectable actions, they were able to get through most of the computer network defenses that the military had established.

This is a useful finding, one that all organizations must consider. Specifically, it showed that the most serious cyber attacks will probably not come barreling into an organization's network with guns blazing and

rockets firing. No, the cyber terrorist will more likely use the techniques demonstrated in this valuable military exercise: They will proceed slowly with the goal of not being noticed. They will patiently build up enough privileged access to perform the attack only when the time is right.

Of course, the military's cyber attack experience is not confined to exercises. Dorothy Denning of the Naval Postgraduate School relates in her excellent book *Information Warfare and Security* the story of five hackers from the Netherlands who penetrated computer systems at 34 military sites on the Internet, many supporting the 1991 U.S. war against Iraq. A program manager at the Air Force Office of Special Investigations explained at the time that these hackers had so much information and control that "instead of sending bullets to the Gulf, they could have sent toothbrushes." This is obviously unacceptable. ■

Silicon Press, Summit, NJ 07901, USA
ISBN 0-929306-38-4
First Edition
Printing 9 8 7 6 5 4 3 2 1 Year 09 08 07 06

Library of Congress Cataloging-in-Publication Data

Amoroso, Edward G.
Cyber security / Edward Amoroso.
p. cm.
Includes index.
ISBN 0-929306-38-4 (alk. paper)
1. Information warfare--United States. 2. Computer networks--Security measures--United States. 3. Cyberspace--Security measures. 4. Cyberterrorism--United States--Prevention. 5. Civil defense--United States. I. Title.

U163.A525 2007
363.325--dc22