Global Information Assurance Certification Paper

SANS Security Essentials GSEC Practical Assignment

Version 1.3

John Maxwell

March 28, 2002

Abstract: The perceived complexity of the current electronic security business model is a contrivance for consultants. The security issues can be easily grasped and addressed by comparing the security to be used in cyber-space as that in a sometime hostile foreign country.

Security Complexity – Consultant Myth?

While browsing through a SANS NewsBites I ran across an interesting question from one of the editors. In response to an article on the complexity of the current security environment, editor Eugene Schultz asked:

> "Has security really become more complex, or do consultancies make it appear more complex to the point that demand for their services grows? Perhaps if we began viewing security as not so complex, we would actually make some headway in improving defenses." (Schultz)

I found the question very thought provoking. Various vendor industries, but particularly the anti-virus industry, have been accused of ratcheting up the threat level for their own ends. While every service business is somewhat guilty of this, is the security industry becoming so enamored of the technical end it has lost site of the basics?

In the spirit of a reply to that question, here is a simple comparison of an electronic internet site and a hypothetical overseas branch office. I believe we will find security is much the same as it has always been; only the location has changed. Thinking of cyber business as a branch office in a sometime hostile foreign location (without an embassy) may clarify the issues.

Defining the current local environment

Examine the physical site

Physical security is just as important as cyber security. The fact we have had a long period during which physical security has been very lax does not change the need for it,

In a real sense, nothing has changed in the realm of physical security except many people's awareness of it. The hardware and software in the organization's data center is the real-world part of a cyber-business, a valuable and sometimes sensitive asset. Treat the physical data center the way such assets are always treated in your organization.

All the rules that apply to paper-based file cabinets still apply to the computer and its storage media. This is a good time to review the access rules, locks, and disposal rules that were developed for paper documents, as well as verifying their continued use in their original incarnation, Use this as a base to apply those rules to the digital world. Security policies may transpose with no changes whatsoever, and only minor updates in the processes and procedures.

.

Limit access to those with a need for that access, and insist on a full-week re-assignment or vacation every year for all employees – including the security staff and all managers.

This serves a multitude of purposes – sharing job skills, annual verification that procedures are in use, and an informal audit of the effectiveness of the job instructions that would be used should there be a personnel change. It also lets a 'new pair of eyes' review the job – and can possibly even spot flaws in the arrangement of secure areas.

It is often stated that the only truly secure computer is unplugged; this is only true until it (or an important component of it) is carried off. If a 'villain' can open the cover and take out the screws, many current hard drives are small enough to simply drop in a briefcase, or even be carried in the hand camouflaged by a small book.

Examine the way computers are used

There are some vulnerabilities that exist as soon as the computer is used – not only security vulnerabilities, but copyright issues, licensing issues, and other possible problems escalating to 'the nightmare scenario' - disasters that destroy the machine and all resident data while incapacitating vital staff.

Don't forget the simple things. Some businesses in the World Trade Center building on September 11th, 2001 were unable to recover due to the loss of key personnel. In an article called 'Picking Up the Pieces' by Bob Tedeschi , Todd Gordon, vice president of IBM Business Continuity and Recovery Services is quoted as saying :

> "In many cases, the data itself wasn't really disrupted. What wasn't available were the endpoints: the workstations, the phones, the people. Businesses had forgotten that even if their data was safe, without the ability to use that information, they were in trouble." (Tedeschi)

In the same article Damian Walch, senior VP of professional services at Comdisco, reported some customers could not recover because they could not access a working open phone line

ALL computer processes and connections must be divided into those that are critical to continue the job or mission, and those that are not. Just as some paper memos do not need a filed copy, some data and processes are so unimportant (or so easily re-installed , re-created, or re-entered) that it is not necessary to recover them. Some examples might be a daily price list, or non-critical mail items. Initial desk top loads of software can be reloaded from the original source, so may not need to be backed up at all; however, ensure there is more than just the original copy of the software. Having just the original might prove a problem if the original media is lost or damaged.

A disaster-recovery/business continuity plan should be made; this is not a security item itself, but it will help the organization sort out what is critical to continued operations

Now that we know where we stand in our world, let's look at the cyber location.

Defining the 'foreign' cyber environment

Examine you cyber site

Consider the cyber-world's connectivity to other machines and to the networks that provide those connections. The risk of cyber computer mischief is directly related to how the computers in question are connected and what kind of computers they are. The fewer connections and the simpler the network is, the easier it is to defend – just as a room with two doors and no windows is easier to secure than a room with a long row of non-locking windows and four doors.

Sometimes the network design can be simplified for more effective defense – the equivalent of boarding up the extra doors. Network connections, especially those leaving and entering the local network, are a great place to insist on the KISS (Keep It Simple, Stupid) principle.

Often management will want to focus on external threats, partly because the media hype surrounding a security lapse and partly because many assume their own people are beyond suspicion. While it is true there is a real external threat to the organization, the more dangerous and expensive threat is from internal breaches of security. Unfortunately, traitors and spies have been known in all times and cultures. Even without a malicious purpose, internal staff bypassing security checks may be leaving potentially devastating security openings.

If we make the analogy that cyber thieves are the equivalent of shoplifters, even semi-trusted internal individuals will do more damage over a longer period than an outsider walking in and back out with stolen items. In the Timothy Lloyd case, a trusted sysadmin using just six lines of code, wiped out his former employer's entire production server. The cost is estimated a $10 million and above, and in addition the company has lost market share, its reputation, and nearly failed. (Amurao)

And as in the retail environment, if the alarms are designed primarily for external attacks, internal people may be able to circumvent them entirely. Also beware of the misplaced blame scenario – remember it is possible to spoof addresses just as it is possible to type someone else's name on an insulting memo. Investigate carefully and fully.

Cyber vandalism is also easier from the inside, and user mistakes can be just as devastating as intended vandalism for the same reasons. What would happen if a trusted supervisor opened the shared data files linked to the desktops in the organizations and deleted the entire contents of those files? Whether intended or accidental, even if the total amount of data lost is not crippling, the reconstruction without a current backup is probably impossible.

Know the local troublemakers

In some cultures vandals are tolerated more than others, but in nearly every culture there is some line drawn to recognize ownership or privacy.

In the preceding paragraphs cyber intruders have been alluded to as vandals and thieves. Add trespassers to the list and we have the real-world equivalent of the cyber intruders. Bear in mind, though, that crime involves intent. It would be wrong to condemn those who mistype an IP or discover in a beta-test there is a major flaw in their products. Sometimes people really do just wander in from curiosity, or by mistake.

There are cyber-professionals, who, like trail guides, have inhabited cyber-world so long that they have located the treacherous spots, the snares, and most importantly perhaps, know the habits of the locals, especially hostile ones. Organizations venturing into cyber-world should get help from one of these guides to learn to recognize the locals and the cultural rules.

Here is a very basic primer on 'hacker' culture.

First, understand that cyber intruders do not appear to respect anyone who is not technologically inclined – just as some nationalities or religious groups discriminate against anyone not of their group. At the Hacker's Jargon site author Eric Raymond points out the there is a pervasive attitude of superiority among most of the 'hacker/cracker' community. This is illustrated by their terms for others – 'Stupids', 'Suits', 'Luser(Loser)', 'Muggles', and 'Mundanes'. They, of course, are 'Wizards', 'Samurai', and 'Gurus'. Another 'hacker' not at some undefined level of expertise is referred to disparagingly as a 'larval' or a 'script-kiddie'. (Raymond)

For the most part there is little one can or need to do about the street urchins of cyber-space, the so-called 'script-kiddies'. These intruders are essentially a malware-using group without the ability to actually write exploits. While they can cause damage using the exploits developed by others, after a few weeks their pre-packaged tools and exploits become known and are countered by early victims and the anti-virus industry posting prevention information and software upgrades. Just as juvenile crime is patterned on adult crime, protecting a site from true hacker/crackers will by default lock out 'script kiddies'.

The one real danger from 'script-kiddies' is denial of service attacks – and there are few practical ways to avoid these attacks. Using the firewalls and routers to control the damage may help, but a prolonged and determined denial of service attack cannot be prevented. However, the 'script-kiddies' do not increase the effect of these attacks, only the potential frequency.

There may have been a time when breaking into others' systems uninvited as a prank was an acceptable behavior; frankly that is doubtful. Imagine being told it was OK to break into houses as long as nothing is taken and the intruder 'only looked around'. This is the real-world equivalent to so-called 'benign hacking'. This behavior is not tolerated in any culture, except some segments of cyber-culture. We do not excuse real-world trespassers and should not do so for our cyber colleagues.

Suppose the trespasser decided to deface the walls, break the furniture, or otherwise destroy property. This is vandalism, and is punishable in every culture in the non-cyber world. Cyber vandals are not highly regarded in cyber-world, either, except (as in the physical world) by other vandals. Destroying others' work and possibly their livelihood is the act of the thoughtless and immature, no matter how it is excused.

We now enter the part of 'hacking/cracking' culture nearly everyone agrees is unethical – entering another's site for the purpose of stealing something. We call this theft. Every culture recognizes theft if it recognizes ownership; this seems to be a cultural constant. Whether the cyber-thief is stealing ideas, competitor's information, financial information, passwords to avoid paying at other sites, storage space, or even just bandwith and response time, the act of taking what is not their own without the owner's permission is stealing.

Again, from Hacker's Jargon site, we find that 'hackers' themselves can't decide if there is ever a moral side to hacking. From the second definition of 'hacker ethic':

> "2) The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality . . . Sense 2 is more controversial: some people consider the act of cracking itself to be unethical, like breaking and entering. But the belief that `ethical' cracking excludes destruction at least moderates the behavior of people who see themselves as `benign' crackers . . ." (Raymond)

It is interesting that the so-called 'samurai' hacker excuses thefts as being acceptable if done for money, so-called 'activists' excuse thefts as fighting for the good, and generic 'hackers' excuse themselves as just trying to make knowledge available to the world. In any case, theft is theft. When law enforcement stops treating cyber-crime as something different from other crime, perhaps we will begin to get control of the problem.

There may be a rare breed of hacker who is so professional that their presence is never detected. Like the expert espionage agent who arrives, photographs the secret documents, and leaves after carefully masking his activities, this intrusion may never be discovered, leaving no chance the intruder would be caught. Only tight security practices have a chance of thwarting this offender.

Know the 'Allies'

There are some friendly organizations in cyber-world. Just as having common issues with the native population can cause disparate groups to work together in a foreign country, there are others in the cyber world with an interest in controlling the problems the 'villains' can cause.

Your first allies are the businesses you buy internet solutions from - the anti-virus provider, firewall provider, router/switch provider – who all have a stake in keeping your site up. The organization security team or security vendor is another staunch friend.

Vendors are not altruistic; they want money. Beware the hype they use to influence your purchase, but remember their products perform valuable services. For example, it is in the interest of the anti-virus vendors to keep virus counts high, so they sometimes report a number of viruses that do not exist in the wild and never infect a single computer. This does not mean that anti-virus products aren't needed, but that you need to understand what they do and why they are needed.

There is also a wide range of free help from sites such as CERT or SANS. The help offered by so-called 'white hat' hackers may also be valuable, but it will be tough to discriminate whether the person is helping or setting up a backdoor for themselves Be vigilant when dealing with unknown security people in the real world or in cyber world.

Cyber security

The firewall is the gatekeeper at your authorized front door. Just as a human guard needs to know who to allow through the door, a firewall is only as good as the access lists used. Closing ports is a blanket denial of access for programs that use those ports, just like locking doors that aren't used for regular business. The tighter the firewall, the safer the network installed behind it.

Is the firewall sufficient in size? Does it have the current patches/updates/upgrades? If not, the gatekeeper can be tricked or easily overwhelmed – you want a robust guard, not a scrawny greeter.

Routers can be thought of as the receptionists who direct visitors to the correct office – keeping visitors on the correct path as they travel through your installation and blocking people from sensitive areas.

An Intrusion Detection System (IDS) is an alarm system that can trigger on preset conditions – like a fire alarm or more consistently with our discussion as a burglar alarms. There is a growing trend toward host-based IDS systems – protecting the specific assets rather than monitoring the whole network. The best solution is to use both – the

network IDS functioning as the building alarm while the host IDS is the Halon alarm in the computer room.

Anti-virus products are the metal detectors of cyber world. As traffic passes by they check for known dangerous items and report the carrier. Some can be set to act in conjunction with the firewall or router and deny access to outsiders whose traffic display known violations.

The key for firewalls, routers, IDS, and anti-virus protection is to remember they work almost exclusively on KNOWN threats. Just as a metal detector would not find a plastic knife, so these cyber-world equivalents will not report an attack unless designed to look for. It is critically important to keep these items at current level for total protection, and assign resources to monitor them.

The security team in your cyber organization functions much as the physical security team should. A working security team should have standard protection in place to handle expected intrusion attempts and a few plans for non-routine incursions. They should also be able to respond quickly to limit a break-in and control its effects.

Secret messages

Encryption is not a new idea – but is it needed in a cyber business? The answer here depends on your non-cyber practices.

If mail items are sent in sealed envelope under certain conditions, there should be an examination of what is accomplished by using those conditions. If it is because the Post Office or delivery service requires it, that limitation can be ignored in cyber-world, but if it is to protect sensitive information or financial instruments, for example, that same protection will be needed in cyber world.

Unfortunately, the nature of the internet means if you are sending sensitive items, unless they are encrypted the possibility exists for them to be intercepted and read, or even altered, usually multiple times between the sender and the intended recipient. To counter this the installation may have to install a Virtual Private Network, or use a secure socket installation, or investigate other secure messaging. In any case encrypting the data will be an additional level of protection, and can be done without any additional underlying technology.

The people on your team

The great balancing act is security and usability – users resent password limits and difficulty checks, and locked doors, and people will always look for the 'best' way to finish the job. This does not make them evil or bad, just human!

Realize your staff usually has activities to complete to earn their pay – and being secure has to be drilled into them to make them see the benefits. If security becomes a block or delays their work, people will find ways to circumvent it – just as people will sneak in the closest door if it is not locked.

Security professionals should be aware of the needs of the job – just as the gate guard will have to open the gate to let delivery trucks in, cyber security will have to permit the work of the organization to proceed while making the organization as secure as possible.

It is possible that someone on your team is a traitor – they are working for the other side. Much of the above will serve to mitigate their effectiveness, but as stated above the inside job usually nets the most reward. Be aware of people who become secretive, or suddenly live much better than their means would normally allow. Internal firewalls – between your own servers inside your own network – and software that monitors the servers will help immensely.

Another real danger is users trying to help themselves. Some people will gladly download anything that promises them faster response time. Some users can't resist the promise of a new screensaver; others are fascinated by any new technology and will gladly install it if they can. Just as an organization may require a dress code in the office, there should be standards and rules addressing the use of outside software and hardware,

Internet usage may have to be restricted. Outside connections to services such as Hotmail or IRC need to be controlled as these tend to be passed directly into the system bypassing normal security. Modems can be the equivalent of a trap door into the network - especially if they are left on and unattended. Again, impress on the staff the need to securely use their computers.

Remember the system users are still the best alarm system – be aware of complaints and chase them down quickly. Convince users that security practices are there to protect them and you may have a chance to limit the damage done by intruders.

There it is – a comparison of real-world and cyber world business security. Not so different in scope or policy, there is a profound difference in implementation. Even so, digital security actually only faces the same problems security people have faced for years in the physical world. Often, the solutions to digital security can be found by examining them in the context of a digital reflection of a physical security problem.

Security itself is no more complex than ever – it remains the thoughtful review of policies, processes, and procedure to ensure the agreed security goals are met, just as it has always been.

List of References

AMURAO, George T. "The Dark World of Hacking". July 19, 2001

url: http://www.e-magazineonline.com/spotlight/SPO/SPO0126a.htm

KERSTETTER, Jim. "Beating Back the Biggest Risk -- 'inside job'". January 15, 1999.

url: http://zdnet.com.com/2100-11-500067.html?legacy=zdnn

MCLEARN, Matthew. "Firms wage electronic war on industrial espionage". Calgary Herald. January 18, 1999.
url: http://www.landfield.com/isn/mail-archive/1999/Jan/0084.html

PRIMROSE-SMITH, Elizabeth." Facing the New Corporate Security Rules". ZDNET News. March 8, 2002.

url: http://zdnet.com.com/2100-1107-855323.html

RAYMOND, Eric S. "The on-line hacker Jargon File, version 4.3.1". 29 JUN 2001.

url: http://www.tuxedo.org/~esr/jargon/html/index.html

SCHULTZ, Eugene. Comment on the article "--8 March 2002 New Issues Facing Corporate Security". SANS NewsBites Vol. 4 Num. 12

SHAW, Eric et al. "Managing the Threat from Within". July, 2000.

url: http://www.infosecuritymag.com/articles/july00/features2.shtml

TEDESCHI, Bob. "Picking Up the Pieces". Ziff-Davis Smart Business site. December 1, 2001.
url: http://www.smartbusinessmag.com/print_article/0,3668,a%253D19522,00.asp