Global Information Assurance Certification Paper

Responsibilities of the "small shop" in a post 11 Sept world

"In [today's] climate it's very difficult to convince the best technology experts to divert their time and effort away from making money and advancing technologically to focus on what seems to them to be obscure and theoretical national security issues"[1]. In April '01 Newt Gingrich wrote these words in an article outlining some of his work with a Presidential commission set up to study National Security in the 21st Century. I think this quote summarizes the attitude of many towards computer security at the beginning of the year. While it was agreed security was an important issue, it always seemed to take a back seat to the more important issues of the company's bottom line or the decision of how to allocate resources. A poll taken around the same time as Mr. Gingrich's article showed that 54% of the companies that responded said they have not implemented all their "needed security programs" due to lack of money. The second most popular response was lack of people at 42% (multiple responses were allowed)[2].

Despite general acceptance that there has been a steady increase in the number of computer security incidents (DDoS attacks, virus/worm incidents, etc) over the past couple of years, there is no clear reason to explain why a lack of focus on computer security still exists. One reason offered by Mr. Gingrich is the fact "that the high-tech generation has no frame of reference for any serious threat to national security or sovereignty". All of this changed on 11 September '01 with the terrorist attacks on the United States. While these attacks were not the "cyber pearl harbor" Mr. Gingrich speculated about in his article, they proved we are vulnerable in many ways that were previously dismissed as unthinkable. Now, in the post 11 Sept world, with our new frame of reference, we have to ask ourselves, "What do we need to do now?"

The Small Shop

Before examining the new frame of reference and answering the question, some context should be established. The phrase "small shop" may have different meanings to different people. In order to explain the phrase as used here a couple of examples would be; an at home DSL user with one or more machines, or a group with a limited IT staff, or just contractors, and a full time Internet connection. Even with 30 users, 1 admin and about 300 occupied IPs I consider my own organization a small shop. No matter what type of small shop is used as a reference though, most people would probably agree the issues and problems faced by the small shop are significantly different than those faced by their larger counterparts. The notable exception should be when it comes to computer security. As one reporter phrased it in a 31 October article entitled Protecting Your Computer Now Part of National Security, "You have a weapon sitting on your desk that terrorists could use. It's a good idea to make sure they can't."[3]

While there are some disadvantages to running a small shop it should not be an excuse for letting security lapse. With some careful planning, what would normally be a disadvantage can be turned into an advantage. In my experience, some of the major issues are:

- *Funding and acquisition of security resources:* Since the revenues of the business (or disposable income in the case of the home user) are smaller, the amount of money going

into dedicated security is going to be significantly less. However, in those places with fewer employees it is usually easier to get access to the person who has the final say on whether or not something is implemented. Therefore, the speed of the acquisition process combined with fewer machines to worry about, means a new security paradigm can be rolled out in hours, not days. Small shops are also probably more willing to adopt some methods and programs the larger ones are not (such as freeware security toolkits, beta programs, etc). Of course, without a dedicated person working on security, this could quickly turn into a disadvantage again.

- *Lack of dedicated and knowledgeable personnel:* Speaking of which, with fewer people to draw upon it is harder to have someone whose sole job is running the security function. In most cases this means the person responsible for security is also doing something else for the company. In the worst case, security is an individual responsibility and there is no central identifiable person. Careful selection of the "go to" security person can turn this into an advantage, as the person may be able to draw on experience from their other job duties to enhance the security program. Obviously the network/systems administrator would make a good choice. If your facility has a physical security officer, this person could be another good choice (depending on the person's interest and skill level). In order to have an effective program though, it seems best to have one identifiable person responsible for the overall security, regardless of the responsibilities individual users take on themselves.

- *Lack of user acceptance or training:* No matter what measures or policies are put into place, if the users do not buy into them, or do not understand them, there is a risk of facing an increased threat from insiders. Hopefully most small shops are not facing the generally accepted problem of a greater threat from insiders. However, if the security precautions put into place are considered excessive, people may try to find (or create) ways to get around them. Alternatively, without a clear understanding of what security measures are in place and why, people may unknowingly violate the policies. In a small shop, it should be easier to work with the users to establish a working set of guidelines that everyone can buy into. Also, getting people involved in the process should make it easier to keep them informed of expectations at the user level. Having a single "go to" security person will help when it comes to establishing the policies. It also gives the users a single person to look to for training and for answers to their security questions.

- *"The can't happen here" mindset:* No matter what size shop you are, this may be the hardest disadvantage to overcome, since it will usually be found in the management of the company. In the worst cases the computer administrator and users might be guilty of this mindset as well. In the wake of the September attacks this attitude seems to be changing however. According to Richard Clarke, the President's special adviser for cyberspace security, "high-technology executives are more willing to talk about building and buying more secure technologies"[4]. Now may be a good time for the decision makers to talk about the new frame of reference we are living in and see what changes may need to be made.

The New Frame of Reference

Unfortunately Mr. Gingrich was eventually proven wrong, in that the high-tech generation now knows a credible and serious threat to our national security. To ignore this incident simply because it did not take place online is to run the risk of allowing the "cyber pearl harbor" to eventually happen. The next step in the process of offering recommendations for small shops is to briefly highlight some elements of our new frame of reference. Central to the discussion are, the likelihood and nature of increased attacks, as well as potential targets.

Anyone reading the newspapers these days, or following any of the various security email lists, will see a constant stream of reports seemingly showing there is an increase in cyber attacks. In a recent New York Times article, columnist John Schwartz wrote, "Government officials are warning that cyberattacks are likely as retribution for the United States campaign in Afghanistan"[4]. On 22 Sept the Institute For Security Technology Studies At Dartmouth College published a paper that would seem to confirm this. Entitled Cyber Attacks During the War on Terrorism: A Predictive Analysis, it gives a historical perspective on the increased level of cyber attacks during some of the recent physical conflicts such as the NATO conflict in Kosovo, and the U.S./China spy plane incident. The study concludes by stating, "an examination of historical precedents indicates that major political and military conflicts are increasingly accompanied by significant cyber attack activity"[5]. Given President Bush has been bracing the American public for a war on terrorism that is to last for years, the prudent conclusion would be cyber attacks are not going away anytime soon, and they are likely to get more intense and more sophisticated.

Without the benefit of a crystal ball, it is hard to determine the exact form these attacks will take. Again drawing from the Dartmouth analysis and recent news reports (if the past is an indication of the future) we are likely to see more denial of service attacks, worms, and web defacements to name a few. Distributed denial of service attacks should be of particular concern to the small shop, since the very nature of these attacks requires a number of machines all targeting a specific machine. Those small shops that do not take security seriously will likely find themselves the victim of the sending end in a DDoS attack. Machines getting infected by worms can be the initial stage of a DDoS attack, which is one the reasons why worms should also be of concern. Some other problems with worms (as recent variants have shown) are the accidental dissemination of information, destruction of systems, and the embarrassment factor that results from having to clean up when people on the receiving side complain about infection. Some times web defacement is similar, in that it is only a slight embarrassment and a matter of restoring from a backup file. However, those small shops involved in some sort of "critical infrastructure", news and information, or some sort of life safety field may find a web defacement not only embarrassing, but having serious consequences as a result of disinformation on the site, or general lack of access to the site. [According to the Dartmouth study "critical infrastructure" involve banking, voice communication, or anything related to essential resources such as electrical, water, oil or gas.]

Even before the incidents of 11 Sept, those shops (large or small) that fit the profile of "critical infrastructure" were considered likely targets of cyber attacks. Since that day, not only

are these possible targets of cyber attack, but physical attack should a valid concern as well. Even if a specific small shop does not fit into one of these categories directly, one just has to look at the unfortunate side effect of what the collapse of the World Trade Center towers did to the buildings surrounding them to realize the intended target of an attack is usually not the only one affected. As of the date of this paper, an illustration of this can be found on the CNN website: http://www.cnn.com/SPECIALS/2001/trade.center/damage.map.html.

Recommendations

> "System administrators and government officials in the U.S. and allied countries should be on high alert for the warning signs of impending hostile cyber activity, particularly during periods immediately following military strikes or covert operations. Reconnaissance by potential attackers is a fact of life in network operations, but changes in 'normal' scanning activity should be considered highly suspicious… As an additional precaution, logging levels should be temporarily raised to trap as many events as possible to increase the fidelity of subsequent law enforcement and/or counterintelligence investigation, and enable the issuance of specific warnings by the NIPC [National Infrastructure Protection Center] and other appropriate entities to other potential victims." - Cyber Attacks During The War On Terrorism: A Predictive Analysis [5]

The question of "What do we need to do now?" remains unanswered. Below are several recommendations based on some of the things I am going to be implementing in my own "small shop". It should be noted that these are not all strictly computer related and not all of them will apply to everyone's situation. However, they draw upon a cross-disciplinary range of skills and offer some suggestions that might otherwise be overlooked by those running a small shop.

1. Write/Reexamine company policies – First and foremost, if some sort of policy statement related to computer security does not exist, now is a great time to write one. Even in the case of an at home DSL user (especially one in a home office, accessing a company LAN) having a written document will force the thought process of "how am I going to do what". There are many resources available to help in generating such a document (a few starting websites are given in the Resources section at the end of the paper). I would recommend all aspects of security, both physical and cyber, should be taken into consideration when writing the document. As mentioned previously, getting input from the users who will be subjected to it may help avoid creating problems down the road.

   If a policy statement already exists, now is a good time to read through it again to see what is still applicable and what may need to be adjusted, such as the logging levels as recommended by Dartmouth. However, as stated succinctly by the editor of Security Management magazine, "it makes sense for companies to look at their policies and procedures critically in light of the changing threat environment, but the yardstick against which they measure their programs – the best practices that have been recommended in the past – still generally stand"[6]. Therefore, even in today's climate over-engineering the solution should be avoided.

2. Test/Train employees – As part of the reexamination process employees should be tested to see if they are following the existing procedures. The nature of the test will depend upon the layout of the shop. Many may find it easier to have a refresher course on security, or simply using an email reminder. Training is especially important if there are any changes being made to the policies or if it is the first time policy is being introduced to the employees.

3. Increase interaction between department heads – The main thrust behind this recommendation is to get people talking and thinking outside of their own field. Those responsible for computer security should talk to those responsible for physical security. Initially this may seem to have limited applicability depending upon the size and nature of the shop (if there are not separate physical and computer security functions or people, for instance). However, the people in charge of computer security should take it upon themselves to think of things from the physical security side occasionally. While the majority of threats of concern to computer security people are from the online side, the most secure firewall in the world will not stand up to someone physically rewiring the network around it or simply turning the power off.

4. Get to know the neighbors – Again this recommendation draws more from the physical security discipline, and may not be applicable in all situations. While there may not be much that can be done to protect directly against physical attacks, considering what is in the neighborhood can help when drawing up policies, especially when deciding how far to go with them. For example, those in a remote rural area will probably want to consider a different security plan than those in a high-rise office building. Further, getting to know the neighbors may create opportunities to draw upon other information resources both with respect to the design of security policies and the implementation of them. For example, those in a building that already has a strong physical security process in place may not find it worth installing something of their own. In some locations, going as far as establishing a neighborhood watch type program may be an option.

5. Start to think like a large company – There are two main aspects to this. First, no company is too small or remotely located to incorporate what Michael Dell, of Dell Computer Corp., calls "geographic diversity in disaster recovery"[7]. While it may not make sense for most small shops to have an entire alternate data center ready to spin up at a moments notice, something as simple as maintaining an offsite copy of a recent backup tape could go a long way towards effective disaster recovery.

   Secondly, it seems increased interaction with Government agencies may be inevitable. One of the recommendations Mr. Gingrich outlined in his article was a stronger interaction between the public and private sectors. Recently President Bush has put this into policy with Executive Order #13231, which created the National Infrastructure Advisory Council. One of the council's tasks is to "enhance the partnership of the public and private sectors in protecting information systems for critical infrastructures"[8]. It is still too early to tell exactly what nature this partnership is going to take. As outlined in the Dartmouth paper though, voluntary submission of incidents is already being strongly encouraged. On the other extreme, this interaction could be in the

form of "[confiscation of] computer equipment for nothing more than a suspicion that it was used for a computer crime"[9] as one unnamed privacy advocate speculated in a news article discussing some of the recent legislation debated by the U.S. Congress. Either way, it is probably best to have these considerations thought out and committed to policy before an incident happens.

Conclusion

Before the attacks on 11 Sept, security was an issue that should have been taken seriously by everyone on the Internet. However, this was not always the case, as some thought it unimportant when compared to other issues faced by a company, and others may have considered themselves to be too small to be concerned with such matters. These attitudes allowed certain mindsets take hold, and unfortunately, it sometimes takes an incident like what happened on that morning in Sept to force people to change their frame of reference. Now that the U.S. has been proven vulnerable, the question on everyone's mind should be "What do we need to do now". Hopefully, the previous suggestions provided some direction for crafting an improved security program. It would be unfortunate if everyone, no matter what size "shop" they have, did not treat computer security as an issue of national importance. If the predicted "digital pearl harbor" is allowed to happen, it could be devastating.

Resources for writing a security policy

This is by no means meant to be a complete list. It is really just a quick list of starting points on some of the better security sites.
http://www.sans.org/infosecFAQ/policy/policy_list.htm
http://www.usenix.org/sage/publications/policies/policies.html
http://csrc.nist.gov/isptg/
http://www.cert.org/security-improvement/practices/p065.html - Actually doing a search on "policy" will turn up a significant number of pages that address all aspects of developing an effective policy.

References used

[1] Gingrich, Newt. "Threats of Mass Disruption." Information Security. April 2001 (2001): 36-38.

[2] Prince, Frank. "Translating Security for Managers." Information Security. May 2001 (2001): 44-46.

[3] Husted, Bill. "Protecting You Computer Now Part of National Security." Newsfactor Network. 31 October 2001. URL: http://www.newsfactor.com/perl/story/14492.html (27 November 2001).

[4] Schwartz, John. "Cyberspace Seen as Potential Battleground." New York Times (online). 23 November 2001. URL: http://www.nytimes.com/2001/11/23/technology/23CYBE.html?searchpv=past7days (27 November 2001). [NOTE: Paid subscription required after 1 week of publication.]

[5] Institute For Security Technology Studies, Dartmouth College. "Cyber Attacks During The War On Terrorism: A Predictive Analysis." 22 September 2001. URL: http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm (27 November 2001).

[6] Marowitz, Sherry. "Rebuilding on Security's Solid Foundation." Security Management. November 2001 (2001): 42-43.

[7] Daga, Anshuman and Humer, Caroline. "Sept. 11 Boosts World Market in Disaster Recovery." Reuters. 13 November 2001. URL: http://biz.yahoo.com/rf/011113/n09346798_1.html (27 November 2001).

[8] Bush, George. "Executive Order on Critical Infrastructure Protection." Whitehouse, Washington DC. 16 October 2001. URL: http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html (27 November 2001).

[9] Middleton, James. "Hacking could become an act of terrorism." Vnunet. 26 September 2001. URL: http://www.vnunet.com/News/1125668 (27 November 2001).

Last Updated: July 27th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
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
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 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
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