Global Information Assurance Certification Paper

Establishing Computer Security in Mid to Large Enterprise Installations

The Human Elements Of Computer Security

By Brennan O'Brien, GIAC LevelOne Candidate

Computers have been involved in modern business for the last 20 years. Networks have been involved in modern business for the last 15 years. Computer Security is only now becoming a major factor in business. As security professionals, we are behind the curve 15-20 years in terms of integrating security into our environments. Retrofitting an environment to support computer security activities can be extremely challenging. Coupling the rapid growth of the Internet with issues associated to legacy computer systems existent in most enterprises requires a significant change in the thinking of the company.

To effectively address these issues, the computer security professional cannot simply rely on technical understanding and ability to address issues. Further, with the heterogeneous nature of many large business computing environments, no single individual can possibly hope to know and track all potential security issues throughout the enterprise. Instead, we must develop security plans and initiatives which change the thinking of executives, corporate staff and our technical peers. These people then become our first line of defense for the enterprise when they see their own role in protecting the company from potential security problems. At the same time, we ourselves must be able to demonstrate our own objectivity within the computer security arena for the company as a whole. Combined, these efforts address the most perplexing of problems of security – how to manage the human elements.

This paper addresses techniques for establishing a more secure environment bearing the attitudes of these groups in mind. We will examine effective techniques for conveying the importance of security, demonstrating how each of these groups impact corporate security, and finally consider tactics for ourselves to use in developing security plans for an environment.

Management Understanding, Acceptance and Encouragement of Computer Security Initiatives

Information Systems, for many non-technical people, largely remain a mystery. Computer security, an even more esoteric specialty within the broad category of Information Systems is so far removed from the average person's experience as to be the functional equivalent of nuclear engineering. Given this, the task of explaining, justifying and implementing security measures can often be extremely difficult. Further, in rapidly growing organizations, activities perceived to be impeding expansion, such as the due diligence associated to

implementing security procedures, can often result in a negative view of the role of computer security.

To address these issues, the security administrator must first gain the trust and understanding of corporate executives. This can be accomplished by placing the role of security in terms of cause/effect relationships to elements management does regularly comprehend. The following bullet items provide examples of phrasing security issues in understandable formats:

- For publicly traded companies, security breaches can lead to economic impact on the company as investors remove themselves from corporate holdings.

- As companies work to improve brand or name recognition, security breaches can lead to a negative public impression of the brand or name.

- As we invest more resources in developing business relationships, breaches of security can damage these relationships and harm business trust.

- In developing products, because of long lead times, information about products can be compromised, allowing imitation products to be placed on market before the company deploys the same product to market.

- Information about personnel, benefits and salaries can be compromised. In a tight labor market, this information can be crucial for other companies to lure away company staff.

- Competitors can learn of marketing and distribution plans, and use this information to actively subvert company sales.

These elements frame concerns over data security into tangible issues which Executive management can understand. Each of the examples demonstrate common computer security issues which we, as technical staff, are required to address. At the same time, each of the examples show a clear relationship between computer security and the financial health company. Breaches of computer security can have a significant, direct impact on the ability of a company to do business, and as executives grow to understand this fact, they will provide increasing ability to address security issues within an environment.

"The Common Man"

By far, the greatest impact on security (both for the positive and the negative) comes from the general staff of an organization. These are the people that have front line duties within the organization, and are often the ones most likely to first recognize a potential security problem.

For the typical employee of a company, computer and information security is viewed as the responsibility of the information systems group, and not by themselves. Nevertheless, according to a joint survey by the Computer Security Institute and the FBI, 71% of all computer security violations occur from within an enterprise. Given this, general staff members represent the best chance of detecting and preventing security breaches. This approach is best voiced by the computer security training company NativeIntelligence:

> *"Security apathy and ignorance are the biggest threat to our computer systems. . . . And the best way to achieve a significant and lasting improvement in computer security is not by throwing more technical solutions at the problem -- it's by **raising awareness** and training and educating all computer users in the basics of computer security."*

Improving computer security awareness is not achieved by using the "stick" approach of negative enforcement. Memos recommending or even ordering increased security in the general population of staff members for any organization does not achieve the desired goal of improved security. Indeed, more often than not these methods achieve very little in terms of actual security improvements for the time and energy invested. Instead, a "carrot" method of positive enforcement must be developed which demonstrates the value of security in terms of the best interests of the user community as a whole.

Consider the average user in your organization. As IS professionals, our key goal is to improve their ability to achieve the missions they have been tasked with. Anything we do counter to that goal (such as implementing stronger security measures) is frequently immediately denounced. Therefore, like management, we must present security in terms the general user community understands.

For many organizations, the "Melissa" and "Iloveyou" viruses decimated the ability of a company to use electronic mail for days at a time. Electronic mail is the key means by which many of our users communicate with one another and with other organizations. These worms exploited trust relationships between individuals in order to "grow". The moral for our user community, then, becomes an issue of trust. Trust is the building block of nearly every form of relationship – both at the business and at the personal level. The misuse of trust is one of the key means by which computer security is violated. We see this in terms of viruses and worms, social engineering, and even in outright lying by members of our own staffs. By framing the trust issue in a manner which the user community can understand, these people can watch their own trust relationships for you. For example, one company I have worked with had an incident where an executive began requesting design information they had never previously been interested in. Shortly after acquiring designs for the product line, they announced their departure. Within two weeks, the same individual was hired by a direct competitor to the first company. Though the activity was

only discovered after the fact, several people involved later said they believed the activity to be a bit strange. Had the company discussed these trust issues with the employees beforehand, the incident would likely have either been caught and halted or questioned, or enough evidence could have been gathered to prosecute the former employee. By involving the user community in security efforts, the security professional can increase their "view" of security a thousand-fold as more people examine the trust relationships between companies and individuals.

The Enemy Within

Arguably the greatest threat to an organization comes not from the user community but from the technical support staff in information systems. We are a threat for three key reasons: First, we have a credible capability to abuse trust relationships. Secondly, we have the technical capability to abuse these relationships in a manner which will do significant damage to the organization. Finally, our jobs are typically moving at a pace which is difficult to maintain a level of due diligence across all systems.

Any time a well-informed member of a company staff decides, with intent, to harm the company in some capacity, the damage can be massive. Consider a company with 1000 employees making $12.00 per hour. Knowing that the burdened cost of an employee is typically ~17% over their salary, these people cost the company ~$14.00 per hour. A single hour of key system downtime can cost this company ~$14,000 in lost wages and benefits. Most IS staff members are completely trustworthy and could not fathom a reason to harm their own company. At the same time all organizations have members who are ethically questionable.

At the same time, the many ethical IS staff members who are overworked, working against impossible deadlines and minimal budgets do experience lapses in their own due diligence. Not one person involved in computer systems deploys and maintains systems which are 100% secure 100% of the time. Systems are installed without being properly secured. Weak passwords are used on critical accounts. Peer relationships are set up between systems to speed operations, maintenance and support issues. Careful reviews of patches and systems releases are skipped because of more pressing issues. These are everyday realities which security professionals are well aware of. Indeed, SANS notes these and many other issues in their analysis, "Mistakes People Make That Lead To Security Breaches".

As security professionals, we walk a delicate line working on security issues among our technical peers. How do we challenge the less trustworthy members of our IS staff without causing a morale issue within the organization? How do we address the overworked nature of many IS staff members who deploy equipment without properly securing the systems without at the same

time challenging these employees ability to do their jobs? How do we

The first key element to establishing effective security within the IS portion of an organization revolves around policy and monitoring.

Change control procedures is an excellent technique for improving security within most IS organizations. Policy based control of who can make changes, what changes can be made, when changes are can be made and a procedure for implementing, testing and reviewing changes can go a long way to improve security. By requiring from the management level a review of change activity on systems three security benefits can be established. First, a general requirement that a wide variety of IS staff members can examine changes to be made on computers systems provides a chance for the "many eyes" principle to be applied towards computer systems. Secondly, with a standardized change control procedure in place it is much easier to determine when unauthorized changes are occurring within the environment. Finally, because the change control system applies to all individuals uniformly, the impact on morale is significantly reduced.

Imagine yourself as a network technician taking on the role of security manager for an organization. You don't know much about UNIX, but you are responsible for security on a UNIX system. How do you achieve your goal with a limited amount of knowledge and a lot of systems to address? You establish a symbiotic relationship between yourself and the UNIX system administrator. They want security, but don't know what all that entails. You know security but don't know how to implement it in UNIX. By capitalizing on your knowledge of network security issues, you can assist the UNIX administrator in securing their own systems. As the enterprise grows, or you need to address multiple systems, you establish these relationships between other individuals. By automating the process of sweeping for system vulnerabilities throughout the environment and reporting to the appropriate personnel, you improve your ability to manage the security issues of multiple systems. As we assist administrators in doing their jobs more effectively, we create a "win" for both ourselves and these staff members.

Who Will Watch The Watchers?

The security professional themselves are potentially the most difficult element in the overall picture of computer security. In order to do our jobs effectively, we must present credible, consist and objective front to all levels of staff within the environment. Credibility comes from several sources. Certification in basic security principles, understanding of the core business mission and integration of best practices from both business and technical sides of the environment all aid in establishing the security manager as a professional, capable person in charge. Consistency comes from the ability of the security manager to develop and apply security measures in a reasonable and regular fashion, not applying

policies and systems which vary between people, groups or divisions of the organization. Finally, objectivity allows the security manager to look at problems from all sides of the organization. Computer security does not exist in a vacuum. It exists to protect a business or asset and allow the protected system to perform its role for the organization. The computer security manager of an organization cannot loose site of the balance between system availability and system security and how this balance applies for each system in a given environment.

A security manager must approach the topic of security with care. While no one wants an environment which is replete with security holes, at the same time no one can address all security issues within an environment in an effective manner in a short period of time. Changing attitudes is a slow and evolutionary process as you bring your peers, your users and your management on board to the long term vision of high quality security in the environment.

Conclusions

Developing security for a company requires more than technical expertise. The security manager must work with all levels of the company to establish understanding, commitment, policies and practices which all contribute to the overall security of an organization. Security is only as strong as the weakest link in the chain, and the weakest links are generally the support by the user community and the ability to view the vast relationships of trust in a large organization. By increasing the awareness of security and the value both to the company and to individuals, more people will assist you in the task of overlooking he environment as a function of their own jobs. This makes the task of managing security in a large environment significantly easier and more likely to catch issues as they arise. By establishing yourself as a credible, consistent and objective voice who champions security, works well with people of all levels and recognizes the mission of the organization, the security manager stands some chance of being able to support the growing mid to large enterprise environment

Reference Material

Schultz, E. Eugene. "Infosec Headlines: Professional Responsibility and Popular Media." September, 1998. URL: http://www.gocsi.com/Infosec.htm (29 Oct. 2000).

Computer Emergency Response Team (CERT). "CERT Advisory CA-1991-04 Social Engineering." 18 September 1997.
URL: http://www.cert.org/advisories/CA-1991-04.html (29 Oct. 2000).

Peltier, Thomas R. "Information Protection Fundamentals." February, 1998.

URL: http://www.gocsi.com/ip.htm (29 Oct 2000).

Morrow, David. "The IT Security Professional as Investigator." March, 1999.
URL: http://www.gocsi.com/sec.pro.htm (29 Oct 2000).

Palumbo, John. "Social Engineering: What is it, why is so little said about it and what can be done about it?" 26 July 2000.
URL: http://www.sans.org/infosecFAQ/social.htm (29 Oct 2000)

Last Updated: July 23rd, 2017

Upcoming Training

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