COMPUTING INDUSTRY CERTIFICATIONS AND SECURITY

Mr. Kurt Jensen MCSE+I

January 30 2002AD

GIAC GSEC Certification Version 1.2f

Introduction

Here comes a statement that may astonish you: Day-to-day operation of today's highly interconnected networks, network services, client desktops and network-ready appliances simply cannot be consistently and effectively secured! "Really" you ask? "That certainly is a radical statement! We have a number of firewalls, antivirus software, security audits, and other security techniques for our network. Certainly all this technology provides a secure network. "You are just trying to sell another expensive network security product!" Actually, my response is a solid "not really." However, what we can do through this study is consider just how highly insecure today's complex network systems can be when vendors do not incorporate at least minimum industry standard *information security* training for their IT Professional certification tracks, and release many products without full consideration of security vulnerabilities.

The Problem

Since the early days of computing and IT product certification training tracks, vendor training has not focused on information or network security. This approach has left a society of information technology professionals ill prepared for the overall network and information security needs present today. Curriculum to train candidates on information or overall network security has simply not been included. Due to this training shortfall, most current networks and information technology products cannot be secure when created or deployed to a modern network. Hackers and freeware tools, an abundance of built-in product security flaws, and constant streams of virus and hacker code simply overwhelm IT departments of today.

The Psychology of Security and Self-Defense

- **Global attitudes towards information security became very lax over time**

The decisions we make as freedom-loving people oftentimes come from a more relaxed mentality in regards to security, coupled with financial pressures of maintaining profit margins, making a living and taking whatever time we can to enjoy our freedom and pursue our desires. In reality, the world we live in is not a completely secure or peaceful place. For a moment consider the tragic terrorist events of September 11th, 2001AD. How many of us would have seriously considered that such disastrous events would really be carried out against the World Trade Center Towers and the Pentagon, using four occupied civil airliners? We may have considered a similar accident possible, but would we have changed our lifestyles to prepare for such a tragedy if someone told us they thought it would happen? Prior to these events most of us would not have changed much. Who wants to live in fear? Certainly most people do not. On the contrary, today we actually pride ourselves in not being afraid, and living out our apparent freedoms. And we certainly should enjoy our freedoms. However, let's take a look at attitudes and lifestyles of ancient history for a moment and see what they thought about security.

In comparison, consider the lifestyles of many ancient peoples. They were *accustomed to the idea of being attacked*. Over time many of their cities, towns, and villages were built with protective mounds, brick or stone walls, fortifications, moats, cannons, tunnels, caves, and the like. Weapons and defensive strategies were part of daily life for many of these peoples, just to help them feel safe if nothing else. Even more importantly, keeping important information hidden from would-be attackers was often one key to survival. Secret hiding places, supply depots, weapons, countermeasures, escape routes, and the like, account for many of the things used to bring victory in times of conflict. People knew that secrets had to be kept if safety or the hope of victory was to be maintained.

In ancient history, lofty ideas like openness and collaboration were either unknown or looked upon with suspicion and disdain. A distant neighbor was someone to be feared, not embraced, and oftentimes for some very good reasons. Most of these societies used defensive measures as a *plan for their safety*, even if it meant designing a way of escape. However, witty attackers eventually learned that fast moving armored vehicles coupled with swift airpower operated under a concept of war called *Blitzkrieg* made such walls and defenses useless. Rapid successes in conquest of nations astonished the modern world, and made nations captive practically overnight! In the more modern space age, trends of defensiveness, isolation, and suspicion still prevailed in people's minds around the world. Risks of nuclear war frightened the world. Cold wars raged.

- **An Isolationist world suddenly became a very open world**

As world wars ended and nations began to heal, world travel eventually increased, and nations cooperated under huge joint economic and military programs never possible before. The United Nations (UN) was born. Nations opened arms and hands wide for trade, cooperation and support even from other nations that were once dreaded enemies. Governments once at odds with each other jointly created and built military systems and space programs. An atmosphere of trust and cooperation was fostered. The notorious Berlin Wall even fell as nations watched in astonished gazes on TV and the idea of Glasnost took over Soviet policy. Attitudes of openness and cooperation had begun to overtake societies worldwide. Mindsets began to change.

Similarly, in computing the concept of "open systems" appeared where network system, communications, and software design standards became agreed upon by nations and the world. What were once "standalone" or isolated systems were quickly being replaced by systems increasingly interconnected to directories, domains, the Internet, and eventually the World Wide Web, as we know it today. Unique non-routable or custom network protocols and hardware that once kept systems unique and separate were tossed aside to make way for the cooperative world of TCP/IP and the Internet. In an ever growing rush to *get connected*, router production and Internet savvy software sales made prosperous giants out of many technology firms, with some exceeding revenues of entire industries from past generations. A desktop PC revolution, coupled with low cost modems, steadily falling prices, World Wide Web browsers, application software, and eventually faster broadband access for homes moved the world toward standardization and higher link speeds, causing a new world of *open communications* to be available to the public practically overnight. Computer systems influenced every part of society. Information security practices, (also known as INFOSEC), remained unknown to most users.

All the while, lessons of world history and such ancient mythological stories as Achilles' heel were simply ignored. In the past, if a Kingdom had some weakness or vulnerability, eventually someone took advantage of it and attacked. Potential attackers knew there was something about that target that remained vulnerable. In the biblical story of King David and Goliath, a tiny stone was used to slay the huge opponent. This seemingly impossible attack defeated Goliath in a way he *did not expect!* The same it was with mythological Achilles and his vulnerable heel. It was a type of *attack that was not expected*! The now famous ancient story of the Trojan horse carries the same tune. An attack that was not expected was most successful. These ancient stories and mythological concepts became ironically applicable to the new modern giant known as the Internet. A terribly sensitive and unprotected heel became exposed. A host of vulnerabilities, security flaws, hackers, and attack opportunities were created by vendors unwittingly, and eventually led to a nearly complete downfall of this new giant in the late 90's and the year 2000. Why?

Ironically this modern day "*Achilles Heel"* was created, exposed, and even flaunted by the most wonderful benefit of the Internet: Powerful new Internet based communications and standardized information exchange over *open systems*. The very *open systems* we so readily accepted, along with volumes of publicly distributed code and data on these newly standardized communications technologies, flagrantly posted an open invitation to those unseemly elements of society who would leap at the chance to defeat the new giant, or take advantage of anyone using it. A mindset of security was left behind in exchange for a mindset of opportunity. Born was the age of faceless attackers hidden behind a remote computer screen. Also born was the age of electronic funds no longer safely protected within a vault. Key business trade secrets, government information, or personal data was now unintentionally but readily available for the reaping via the latest open source technologies, where no daring physical break-ins were required. No longer did an attacker or thief have to muster the courage to face angry dogs, fences, alarms, guards, or weapons. Highly visited or prominent (but unsecured) web sites created an excellent and most tempting venue for hackers to vent their creative anger or mischief, as they trashed victims web sites and pages, or shut down their servers and networks while proving their supposed hacking prowess to their competitors in the hacker community. Truly, the brave new world of open systems and communications became a wounded giant ready to fall.

- **Hackers provided the computing world a harsh “wake-up-call.”**

This downfall or near collapse of the Internet was manifested in several ways during the late 1990s and beginning of the latest decade. Consumer confidence soon plummeted in regards to industries such as telecommunications, Internet Service Providers, software and technology firms and stock values slid down or fell by hundreds of points. Unlike other price drops in the past, these losses persisted. All kinds of firms that had previously hopped onto the Internet bandwagon were affected counting online bookstores to network implementers and PC builders. Technology firms who once held high the banners of free enterprise and profitability through technology began to go bankrupt in rapid succession. Investors saw once attractive technology portfolios bring huge losses in revenues. Thousands of workers were losing once promising jobs and careers. Surprisingly, even the leading Internet router production giants such as Cisco were affected. Layoffs seemed to sound death tolls for the future of Internet based profitability. Even innovative high-speed Internet access providers such as Sprint Broadband and @Home.com found it too costly to operate and shut down, either turning away new customers or just filing for bankruptcy. [http://@home.com/; http://www.sprintbroadband.com/]

- **Pacifist attitudes toward INFOSEC have caused great loss**

Could it be the constant high profile exploits of hackers, continuous news of Internet based security failures and intrusions, the constant onslaught of more and more advanced viruses, practices of Internet con artists, investment scams, and stolen credit card numbers frightened away once excited and frequent investors? Could it be these very security problems that brought the confidence of the Internet connected public and enterprises down to a disastrous low, putting countless billions of dollars invested in Internet technologies to the bit-bucket and causing so many lost jobs around the world? History always speaks for itself. Consumer and investor overconfidence followed by very rapidly collapsing consumer confidence, and the panicked rush on banks and investment funds that followed, were the leading contributors to conditions that brought on the infamous Stock Market crash of 1929, or “Black Thursday,” and the terrible Great Depression that came with it. Similarly, in 1999, 2000 and 2001, investors saw large continuing reductions in the value of their technology shares. However, a more secure Internet without a tarnished reputation of prominent security breaches, high volume credit card theft, hacker exploits, and availability problems from DDOS attacks could have maintained higher levels of consumer and investor confidence. Such confidence could have kept a stronger flow of necessary capital pouring into the industry, not away from it. Strong investments keep investor confidence, bringing in and keeping plenty of investors, even when profits may wane a little from time to time. It is when something scares investors away that values fall, money dries up, and investments fail.

State of the Computing Industry and Security

For years many of these *collaboration technology* product vendors created and marketed new systems with unintended but serious security vulnerabilities built right in. Of course, in a completely peaceful and trustworthy society without aggressors, cheaters, hackers, snoopers, spies, crime, or wars, that oversight would have been perfectly acceptable.

Vendors continue to market products supplied with numerous or substantial security vulnerabilities such as backdoors, insecure password handling techniques and clear text password files, and unchecked memory buffer space. All these vulnerabilities require plenty of skilled attention from knowledgeable IT Professionals while on the job. This problem continues to make overall security of network services even more difficult to achieve. Adequate testing against security standards is obviously not being completed prior to release of these products.

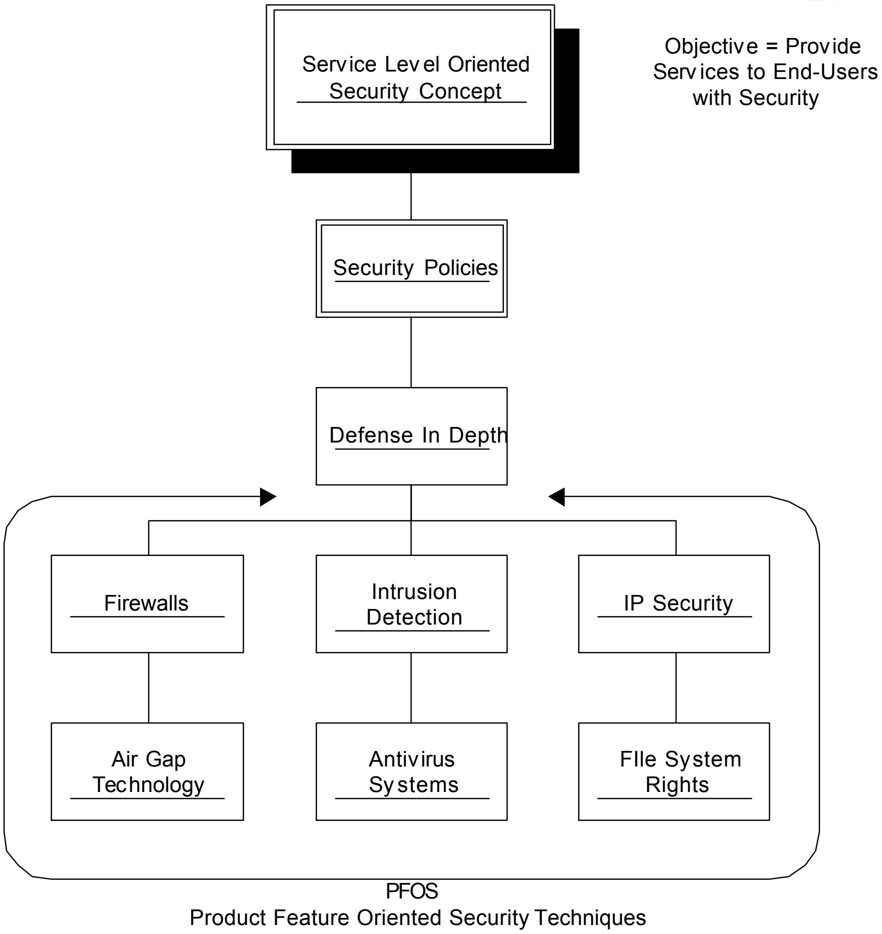
Most vendors do train IT Professionals in use of very specific granular security features such as access control rights, file system security, object access rights and permissions, user accounts, and other highly localized security features. Security of this type can be identified as PFOS or *Product Feature Oriented Security.* This security concept would provide the most detailed guidance on use of server file system security features and firewall access control lists. Granular security controls like these typically satisfy the requirements of SANS *Least Privilege* concept and *Know Your System* guidelines. This is where an administrator grants the smallest set of access rights possible for any given user or role and still provide the services users require. Based on expert knowledge of systems or products, such feature related security is more possible to achieve.

However training in PFOS security practices alone is simply not adequate. This level of training does not achieve the important Defense In Depth security concepts or discipline published by SANS, where it is understood that no one product or service is adequate to secure information or networks by itself. The Defense In Depth concept is used to help determine the specific security products and methods incorporated into a network in order to assure that information security is accomplished and maintained.

Another concept is called *Service Level Oriented Security* or SLOS. This concept focuses on the high level objective of a network system; *providing service but with security.* This can include web hosting for example, while also providing the desired level of security for the network. Security alone is certainly not the objective of building networks. If that were the case then we could simply disconnect everything and be more secure. The objective of course is to provide services over a network, not to just construct something more that needs protection. Therefore, use the SLOS concept to define the specific services your systems should provide, the level of availability needed, and what risks are created up-front by providing the services. Once the risks have been determined, both known and unknown, use Defense In Depth design principles to reduce and eliminate the levels of risk to your services and systems. These security concepts, regardless of what anyone might call them, must be understood, practiced, and accepted industry wide if network systems, information, and services are to be properly secured. Figure 1 provides a high level view of how these security concepts all fit together.

However, because many vendors still do not train their IT professionals in disciplines of writing or implementing information security policies, prevent common hack attacks, or retrace intrusive actions attackers may carry out against their systems, the systems they install and support are simply not as secure as they should be. Daily news in technology and business show just how vulnerable many systems are today.

Figure 1 - Security Concept Tree


Service Level Oriented Security Concept
Objective = Provide Services to End-Users with Security
Security Policies
Defense In Depth
Firewalls
Intrusion Detection
IP Security
Air Gap Technology
Antivirus Systems
FIle System Rights
PFOS
Product Feature Oriented Security Techniques

Now that we have seen the concepts and how they fit together theoretically, remember that multiple layers of information or network security products must usually be added and administered in the typical Internet oriented network. These requirements make modern networks far more complex and time consuming to properly administer. Guidance for use secure use of any product or technology in any network is required if successful levels of information security is the desired outcome. Even the best security products require well-guided decision making during both deployment and operations if the benefits of the product are to be received. As a baseline or starting point, INFOSEC practices or disciplines like those described in ISO 17799 or similar security policy standards can be modified to fit most organizations. Such standards are rapidly becoming globally accepted INFOSEC policy guidelines, and this will probably continue into the future. The ISO site can be looked at for information at: http://www.iso17799-web.com/ In order to understand how these concepts apply to the real world components of an organization or network, Table 1 includes purpose statements for each concept.

Table 1 – Security Concepts and Purposes

Concept	Purpose
Service Level Oriented Security - SLOS	Provide Services to users while limiting vulnerabilities and risks to smallest number possible. This concept acknowledges that networks are built to provide service.
Security Policies	Defines information security goals and practices. Provides guidance on secure use of resources and products as well as policy expectations regarding personnel activities regarding information security.
Defense In Depth	Layered security architecture or design concept. No single product alone such as firewalls can assure information security.
Product Feature Oriented Security - PFOS	Concept including all security features and options provided by a given product. Use of such security tools, options, or features supports information security but cannot provide overall security assurance alone.

- **Other causes for a lack of information security training**

Some significant causes for a lack of security training regarding information security can be the constant rush needed just to keep up with computing technology and the market. This is the ongoing problem of numerous technically advanced products and so little time to know them in detail. Updates regarding important *information security* topics are often missed for the same reasons. IT professionals should understand this concept as applied to security, and be able to help plan for the unknown. Separate tracks in security training can be quite costly to attend, and not as interesting to many technical personnel, resulting in limited access and demand for in-depth classes in security. Information security is also relatively new as a career path to many organizations, and standards have been few and not well known. Over time, these trends have been changing and more organizations see the need for better security.

What a Lack of Adequate Security Training Has Caused

Due to the past and current lack of emphasis on information security in training tracks, many current software developers were taught to get code written quickly, make it work, and get it packaged on time. Again, the emphasis has been focused primarily upon features and capabilities. This problem is made evident by the tremendous number of software-based vulnerabilities hackers find pleasure in exploiting regularly today.

As a testimonial to this fact, many of today's common *buffer overflow* and *unchecked buffer space* vulnerabilities result in terrible risks and backdoors that provide unintended access into network platforms. Many of these vulnerabilities have frequently been used to gain root or system level access to computers and networks. Any hackers code that runs in "unchecked buffer space" left open by software or programs usually runs at the root level of user access on a target system! The overflowing of system buffers through use of malicious code usually accomplishes the same thing. And worse yet, today numerous free tools are readily available for download from the Internet that can easily take advantage of such vulnerabilities using the average modern PC and modem connection. Many of these tools have become popular with teens that have now become hackers as a way to impress friends and exercise their curiosity.

- **A heavy burden was placed on information technology users**

As a result of inadequate security in coding practices, the necessary task of keeping up with numerous layers of software patching or code updates for systems seems to be an endless task for systems support staff and administrators. Often change management processes and budgets are strained with the overhead related to tracking continually updated configurations, documentation, and managing system reboots. Managing layers of different vendors computing products to defend against ever-growing Internet or internally based threats consumes numerous hours of precious IT department time and resources. Duplicating efforts for each workstation and server is a frequent task and concern. Putting out security fires eats up more and more resources, limiting the availability of time for security training and adequate security planning. On the other hand, with adequate security planning in advance, use of INFOSEC policies, and tested security practices, much vulnerability and the related attacks would rarely if ever affect properly secured networks.

To demonstrate this problem further, think about the following facts. In the last several years, many product or service vendors such as Yahoo and Microsoft have been badly compromised or humiliated by hackers through break-ins or denial of service attacks. Even high profile government web sites related to security or law enforcement such as those belonging to the US Senate and FBI were compromised. Hackers have often succeeded by using freeware tools coupled with vulnerability information and scanners posted to the Internet for free download by anyone. Ironically these hackers usually have little if any understanding or education regarding the operating systems or software they attack, while targeted network systems and services are typically staffed with some of the most educated and highly trained computing professionals available. Exponential growth in such hack attacks and intrusions has boomed right alongside the dynamic and astounding growth in network services and technology.

- **Marketing practices have undermined information security**

Historically, new services and technologies or "bells and whistles" have been the leading motivation for marketing new computing products. The development and release of hot new services and technologies has always taken top priority with many vendors simply to maintain a competitive edge. Getting the most advanced products to market quickly has often increased sales and revenues, while security concerns have been largely dealt with after release of the product, if at all. Products that are simply more secure have not been considered to have much “upgrade appeal” in the past.

- **Cost vs. benefit decisions have often undermined security**

Common and necessary business procedures for evaluating products prior to purchase or implementation have also expanded the problem. “Cost-Benefit” analysis efforts have historically been focused on the cost or timesavings benefits of new products without fully considering the security concerns behind it. While many new IT products may indeed result in time, productivity, and cost savings, these same products may also shorten the future or success of an organization when information security is not a priority. For many Internet oriented businesses consumer confidence means everything. Just one high profile incident regarding loss of information security could result in lost trade, customer traffic, sales, investors, and the eventual collapse of the business.

- **Insufficient application of common security technologies**

Innovative and proven security technologies such as RSA, PKI, PGP, MD-5, S/MIME have been available for several years. Many of these security technologies are free to the end user. Yet without this technology the Internet would not be secure for doing business at all. While most of these security methods, technologies, or products were not invented or originated by operating system or major software vendors, currently these vendors do implement these solutions into their own products in an effort to make the products more marketable and secure. As that is the case, vendors that incorporate such technologies should provide much more security awareness and in-depth training along with exam requirements on use of these security systems for their certification candidates. In the past many of these specific security technology topics have been simply glossed over.

Default configurations of most products, when installed, are certainly far from secure today, even when such security technologies are readily available. Each IT department must research and enable it’s own minimum-security configurations or risk immediate attack by anxious hacking opportunists. This duplication of effort made necessary by inadequate security of default product configurations costs the industry and end-users plenty of cash every year. Default configurations that lock systems down much better should be the standard today. Then users would disable the security features they do not wish to use as compared to the current mode of trying to make systems secure instead.

- **Legal ramifications exist but have been taken too lightly**

Important legal topics such as the protection of Privacy Act related data or HIPPA protected medical patient records and documents are simply not discussed in any of the curriculum or exam objectives I reviewed either. Yet the law requires all such medical data to be secured by the service provider that holds it, such as medical agency. Security compromises related to such data can result in substantial legal penalties to organizations involved. Therefore, leading Network Engineers, Systems Administrators, and Analysts should be able to demonstrate understanding of such legal topics and how they may affect information security disciplines during systems design, maintenance, and administration.

As the desire to protect privacy and security of information increases in America and around the globe, organizations that run messaging systems hosting e-mail accounts for numerous end users across the Internet and large corporations may be required by law in the future to install protective systems for their networks such as IP Security, antivirus software, mail filtering firewalls, and possibly even intrusion detection systems. At the present time however, law does not currently require these measures except in the most secure environments, such as where sensitive government information may be located. Internally based attacks and security violations have become a trend as well creating more internal legal concerns for businesses, governments, and employers. Host based intrusion detection systems can monitor unauthorized access attempts, and possibly prevent violations. Logs of such activities can be created and possibly used later for the purposes of investigation and prosecution, possibly making networks more secure from internal attacks that would go unnoticed by firewalls and perimeter security systems.

- **Why INFOSEC must be improved through training now**

The overall availability and integrity of the Internet and data stored there is too important to ignore. When hackers compromise one system it is very likely that many more systems and other networks will be seriously compromised also. Internet Service Providers (ISPs) have not been doing enough to curb the flow of malicious code and viruses. The majority of computer end-users cannot be counted on to prevent denial of service attacks, remote control of victim's computers, and the spread of viruses. However, ISPs have left it up to end-users and to protect their systems. Most end-users are not prepared to do so, even with the popular antivirus software packages out today. There is much more to security than installing a software package and forgetting about it. ISPs are in a much better position to identify problem hosts, traffic types, behavior, and DDOS attacks. Traffic identified as illegal could be logged, and reported to authorities by ISPs if warnings sent to end-users or organizations that put out such traffic go unheeded.

Personal data, medical records, financial records, trade secrets, and the like should be well protected at all points, especially during transfer to other systems. Security methods from the past such as locked doors and file cabinets are simply no longer adequate to protect important files, records, and finances, since most of this data is now digitized.

Vendors have released too many computing products to market with numerous security flaws. It is time that computing product vendors take more responsibility for the levels of security their products achieve in a default installation. Messaging systems and e-mail software provides a classic example of products highly vulnerable to attack. Network E-mail systems alone can easily justify the addition of corporate antivirus software systems and software for workstations and servers. Running without antivirus software today will likely mean mass infections of your network through e-mail infections, followed with large losses in productivity and compromise of the system, regardless of the presence of network firewalls.

Recommended Solutions

Engineering level certification tracks should agree upon and teach standard levels of information security. Defense In Depth, SLOS, and security policy in the workplace should become topics taught as standard practice. A much more security-oriented workforce in the computing industry could be created. For a baseline curriculum, upcoming and recent global security standards such as ISO 177799 could be used.

An independent governing agency should be formed with the authority to accredit engineering level certification track curriculums especially in regards to information security. This agency could oversee the content and objectives of each certification track submitted to it for accreditation by vendors. Such an independent accreditation could lend more validity to levels of training and knowledge achieved by students. Accreditation of important certification tracks could also bring more interest to the IT security career field.

Companies and organizations must place much greater value and emphasis upon training for information security. All personnel that handle sensitive information must be aware of major risks to information and networks, and how they should help protect it. Privacy and/or confidentiality agreements help but cannot adequately protect organizations today when information can be so easily accessed, copied, and transferred between systems. All personnel should receive basic training related to the risks they manage or may be part of. IT professionals in lead positions in the engineering and/or support roles should become certified in security. All other personnel should attend brief but regular hands-on security awareness training sessions where information security can be specifically related to the tasks these personnel perform day-to-day when using networks and information.

Internet Service Providers and Application Service Providers should arise to the task and take the lead in providing better security. For example the current practice of sending clear text usernames and passwords over the Internet for access to Post Office Protocol (POP) or Web based e-mail accounts and services should be eliminated. Secure logins to remote services should become the standard. Messages, content, and web sites known to contain viruses, or malicious code should never be relayed by ISPs. Legal agreements with end-users and service providers have simply not been enough.

In the long run, the best way to obtain more secure computing products such as server operating systems, routers, messaging software, network applications, and outsourced services is to qualify them against independent security standards and evaluations. An independent body of product security experts sponsored by industry could evaluate computing products or technologies against a proven set of criteria and certify the product against globally recognized security criteria. Through use of such independent evaluations, vendors from all segments of the computing industry could incorporate helpful feedback from independent security teams and evaluators up front during the engineering process, allowing more secure products to be created, without the burden of reinventing the entire security evaluation process on their own.

Conclusion:

Looking at the number of successful hack attacks reported over the past several years it has become obvious that information security surrounding the Internet, and today's computing model of collaboration or *open systems* is simply not adequate. With the evidence of so many security vulnerabilities in computing systems and software now receiving media attention, and in so many urgent security flashes, coupled with the extensive vulnerability information databases and tools readily available to the hacking community, computing professionals that understand all the requirements of information security are now needed more than ever. Core training should include INFOSEC.

There will always be a need for personnel that specialize in careers surrounding network or information security practices and design, and that evaluate networks from the ground up with security disciplines in mind. However, with the numbers of Internet-based and internal hacking attempts seen historically, coupled with rapidly increasing levels of hacker activity expected in the future, it is now essential that our computing world obtains security certified computing professionals industry-wide. IT Professionals should gain practical knowledge in all the major factors surrounding secure networking and computing, including how to protect Information Systems and data throughout the life of the system. Many more personnel are needed that could specialize in skills such as secure design practices, technical consulting, or others in administration and management. Practical knowledge on how to write and apply security policies for network systems is essential and should be taught across the industry. Vendors providing engineering level IT certification training programs and the computing industry now have a dynamic opportunity to agree upon a set of proven information security standards, in a manner similar to how they have collaborated in the past to create, and agree upon, new Internet technologies. Then, enhanced IT training programs can create a much larger base of security proficient personnel and users. Information Security could then take its rightful place in computing around the world and in the products we deploy; providing the levels of privacy and security that are so important in our open computing planet.

References: (January 27, 2002)

"Achilles," Microsoft® Encarta® Online Encyclopedia 2001
http://encarta.msn.com © 1997-2000 Microsoft Corporation. All Rights Reserved.
http://encarta.msn.com/find/Concise.asp?ti=03EAB000

"Fortification and Siege Warfare," Microsoft® Encarta® Online Encyclopedia 2001
http://encarta.msn.com © 1997-2000 Microsoft Corporation. All Rights Reserved.
http://encarta.msn.com/find/Concise.asp?z=1&pg=2&ti=761579203&cid=13#p13

"Internet," Microsoft® Encarta® Online Encyclopedia 2001
http://encarta.msn.com © 1997-2000 Microsoft Corporation. All Rights Reserved.
http://encarta.msn.com/find/concise.asp?ti=761579729&sid=12#s12

Black Thursday and the Great Depression
http://www.geocities.com/Athens/Olympus/1545/

Significance of security problem and government or private sector responses:
http://www.gocsi.com/ (Computer Security Institute)

http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.03/index.html
http://www.cnn.com/TECH/specials/hackers/primer/
http://www.newscientist.com/news/news.jsp?id=ns99991804
http://www.eff.org/

Statistics on reported hacker activity. History of hackers and downfalls of the Internet:
http://www.incidents.org/
http://zdnet.com.com/2001-11-0.html?legacy=zdnn
http://www.gulker.com/ra/hack/
http://www.washtech.com/news/software/4769-1.html
http://www.cnn.com/TECH/computing/9906/11/senate.hackers.02/
http://www.thebee.com/bweb/iinfo101.htm

SANS Reading Room has many helpful articles on topics mentioned in this paper and many more:
http://rr.sans.org/index.php

Security Policy related articles and links, ISO17799:
http://rr.sans.org/policy/standardization.php
http://www.information-security-policies-and-standards.com/
http://www.riskserver.co.uk/iso17799/
http://www.yourgateway.to/iso17799/
http://www.securityauditor.net/
http://www.iso17799-web.com/

Gartner Group http://www4.gartner.com/
Has much research on status of the industry, performance records, and how product vulnerabilities affect network management:
http://www4.gartner.com/1_researchanalysis/mrr/1201mrr.pdf
See following sections of Gartners' December 2001 "Monthly Research Review"
Article: "The Information Security Hype Cycle;" and "Internet Vulnerability Risk Assessment."
Adobe Acrobat Reader required for viewing. Also, more support for building secure products, not just patching systems:
http://www4.gartner.com/1_researchanalysis/mrr/200201mrr.pdf
Article: "Tax Breaks for Internet Security Will Increase Vulnerabilities"

Training Programs and Vendor Certification tracks:
Compaq ASE:
http://www.compaq.com/certification/na/index.html (North America)
http://www.compaq.com/certification/na/ase_proliant_windows.html

Compaq Master ASE Track: (Has lots of security coverage built into this track which is beyond the norm for most certifications)
http://www.compaq.com/certification/na/mase_internet_intranet.html

Microsoft:
MCSE (Microsoft Certified Systems Engineer)
http://www.microsoft.com/traincert/mcp/mcse/requirements.asp
MCSA: (Microsoft Certified Systems Administrator)

http://www.microsoft.com/traincert/mcp/mcsa/new.asp

Reference (Continued)

MCDBA: (Microsoft Certified Database Administrator)
http://www.microsoft.com/traincert/mcp/mcdba/requirements.asp
MCSD: (Microsoft Certified Solutions Developer)
http://www.microsoft.com/traincert/mcp/mcsd/requirements.asp

Oracle Inc.
http://www.oracle.com/education/certification/news/index.html?certlevels.html

Sun Microsystems Inc.
http://suned.sun.com/HQ/certification/
(Sun also has a newer separate security track that offers interesting security training)
http://suned.sun.com/US/catalog/networking.html

Novell Inc.
CNA: (Certified Novell Administrator)
http://www.novell.com/education/certinfo/cna/index.html
CNE: (Certified Novell Engineer)
http://www.novell.com/education/certinfo/cne/index.html
Master CNE:
http://www.novell.com/education/certinfo/mcne/index.html