THE INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS SECURITY IMPERATIVE: IMPORTANT ISSUES AND DRIVERS

John H. Nugent
Graduate School of Management
University of Dallas
Email: jnugent@gsm.udallas.edu

Mahesh S. Raisinghani
Graduate School of Management
University of Dallas
Email: mraising@gsm.udallas.edu

ABSTRACT

This paper explores the importance and necessity of information technology (IT) and telecommunications security (combined, these activities are referred to as INFOSEC) in an ever more interconnected world. A review of the current state of affairs, some important organizations, privacy, regulatory issues, threats, protections, and tools is undertaken, and a plan for proceeding in this complex arena is presented. A detailed Security Hierarchy Chart is presented at the end of the paper that compiles in a single, easy to use repository threats, attacks, tools and products by segment and layer.

Keywords: E-Commerce security, Security hierarchy overview, Security planning principles.

1. Introduction

The worldwide market for information security services will nearly triple to $21 billion by 2005, up from about $6.7 billion in 2000, according to new research released by International Data Corporation (Costello, 2001). According to the study, the boom in the market will be driven by corporate need for wireless access, extranets, and remote networks because new and greater security services will be needed to secure those technologies. Due to the advancements in technology and the growth of the Internet, more people are interconnected today than in all of prior history. This growth in telecommunications and Internet connectivity is expected to continue at a rapid rate. As can be seen in Table 1 below, only the number of wireless communications users is expected to outgrow in percentages the number of Internet users through 2002.

Table 1. Important Worldwide Trends and Indicators

Category	**1990**	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**	**1999**	**2000**	**2002**
Main Telephone Lines (millions)	520	546	574	606	645	692	740	794	848	906	970	1115
Mobile wireless subscribers (millions)	11	16	23	34	55	91	145	214	319	472	650	1000
International Telephone Traffic (billions minutes)	33	38	43	48	56	62	71	80	90	100	110	130
Personal Computers (millions)	120	130	150	170	190	230	260	320	370	430	500	670

Continued on next page

Internet Users (millions)	2.6	4.4	6.9	9.4	16	34	54	90	149	230	311	500

Source: International Telecommunications Union, 2000 (www.itu.org)

Here, however, in the relatively near term, as wireless mobile broadband communications becomes a reality with the advent of Third (approximately 2 MBPS) and Fourth (2-100 MBPS) Generation mobile broadband networks, such devices will become a leading alternative means of connecting to the Internet spurring overall interconnectivity and access to even greater heights. Additionally, as with cable and DSL connections, these wireless packet based technologies will also be "always on."

Robert Metcalfe, inventor of the Ethernet, has postulated what has become known as Metcalfe's Law (Boyd, 2001). This law puts forward the proposition that the value of the network is proportional to the square of the number of nodes on the network. It is the authors' corollary that the potential for security breaches is also proportional to the number of nodes on the network.

Security Corollary: ***As theoretical network value increases, so does potential risk***.

As can be seen below in Tables 2 and 3, as nodes on the net have increased, so too have attacks and vulnerabilities.

Table 2. Nodes on the Net and Incidents and Vulnerabilities: 1997-2000

Number of computers connected to the Internet (host)/1000 inhabitants[1]	**July 1997**	**July 1998**	**July 1999**	**July 2000**	**Activity** → ↓	**1997**	**1998**	**1999**	**2000**
US	57	88	142	215	Incidents reported to CERT[2]	2000	3900	10,000	15, 400
Europe	314	576	654	1009	Vulnerabilities reported to CERT[3]	320	280	420	790[4]
Canada	30	51	74	113					
Japan	8	13	18	28					
Mexico	0	1	2	4					
US FBI Adj. Computer Crime Estimate[5]						**100,000**	**195,000**	**500,000**	**770,000**
Europe FBI Adj. Estimate						**16,000**	**14,000**	**21,000**	**39,500**

[1] http://www.stat.fi/tk/yr/tietoyhteiskunta/infrastruktuuri_liittymatv
[2] http://www.execpc.com/~mors/newnug2/sld004.htm
[3] http://www.execpc.com/~mors/newnug2/sld005.htm
[4] Number is for only the first 3 quarters of 2000 versus a full year as shown for 1997-1999.
[5] The above estimates of computer crimes are based on a former FBI official's estimate that only 2% of computer crimes are reported.

Because so many individuals and entities fail to report computer security incidences, an accurate number of such incidences is not possible to calculate. However, the Carnegie Mellon University's CERT Coordination Center reports the following trends in reported hacking incidents per year (Telephony 2001):

Table 3. Reported Hacking Incidents Per Year

Year	1988	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000
Incidents	6	252	406	773	1334	2340	2412	2573	2134	3734	9859	21756

The selected highlights of the joint Computer Security Industry Association/Federal Bureau of Investigation (FBI) survey of computer crime entitled, "2001 Computer Crime and Security Survey" (www.gocsi.com), are listed in table 4.

Table 4. Selected Highlights from 2001 Computer Crime and Security Survey

Category	**Metric**
# Participating Companies & Government Agencies	538
% Reporting Security Breaches	85
% Reporting intrusions to law enforcement (25% in 2000 report)	40
% Reporting the Internet as Source of Attack	70
% Reporting Internal Systems as a Source of Attack	31
% Reporting Financial Losses	64
% Reporting Losses of approximately $380 million ($265 million in 2000 report). Number of entities reporting losses 183.	33
Average Reported Loss (in millions of dollars, rounded –off)	2
% Reporting Computer Virus incidents	94
% Reporting DDOS Attacks	38
% Reporting Not Knowing if there was unauthorized access to their e- commerce sites	44

Source: Computer Security Institute (www.gocsi.com) 2001

Considering the metrics reported to the Computer Security Institute by the 538 participating entities as highlighted in Table 4 above, **and the fact that a former FBI official has estimated that only 2% of computer crime is reported**, computer crime may actually be some 50 times greater than that shown in Table 4, or almost $19 billion for the period reported – the year 2000.

The following key quotes help us get an overview of current state of affairs and the size of the problem:

"The big threat to our security comes from hostile nation states that can muster sufficient resources to make a concerted significant assault on America." U.S. Senator Robert Bennett, (R-Utah), speaking on the potential of adversaries launching an electronic attack on U.S. entities made before an Armed Forces Communications and Electronics Association conference, May 14, 2001.

"Only 2% of the companies that discovered their sites had been compromised reported the incidents to investigators." Charles Neal, Former Federal Bureau of Investigation (FBI) cyber crime unit member, June 4, 2001.

U.S. businesses will "increasingly become the point of attack for enemies of [the] United States" by hackers and national governments using sophisticated weapons such as worms and viruses that can be used for precise attacks. Lawrence Gershwin, Central Intelligence Agency (CIA) National Intelligence Officer, in testimony before the Joint Economic Committee of the U.S. Congress, June 21, 2001.

"The U.S. is losing ground in protecting its systems. The rate of progress has been slower than the growth of the potential threat." Duane Andrews, former Assistant Secretary of Defense in the previous Bush Administration in testimony before the Joint Economic Committee of the U.S. Congress, June 21, 2001.

Other recent indicators meriting mention:

- FBI estimates as many as 1 million credit card numbers have been stolen from e-commerce sites by Eastern European Hacker groups (Gomes and Bridis, 2001 and Verton, 2001a).
- Meridien Research estimates Internet credit card fraud at 10% of all Internet sales (Radcliff, 2001a).

- CIA reported in December 1999 that those having their Y2K software systems remediated offshore in some 15 specified countries were likely, if they had the skills, to find that hidden code had been placed in the remediated code (steganography – literally, “”hidden writing”), (Meek, 1999).
- eWeek cites reports of over 4,000 Distributed Denial of Service (DDOS) attacks per week (Fisher, 2001c)
- Carnegie Mellon University’s Computer Emergency Response Team (CERT) Coordination Center, a federally funded and leading center for security development and research experienced significant delays in response times due to a DDOS attack (Fonseca, 2001).
- Chinese hackers attacked the U.S. Department of Energy’s Web site for its Albuquerque, New Mexico facility (Fisher, 2001a).
- Attrition.org reports at least 30 web site defacements per day (2001).
- Verisign wrongfully issues digital certificates to an imposter (Hulme, 2001a), and
- Microsoft reported to users that an unauthorized party had obtained digital certificates permitting that party to deliver viruses while improperly posing as Microsoft employees (Gawlicki, 2001).

From even a high-level review of the literature, we see a large and growing threat to our ever increasingly interconnected communications environment. For years, governments carrying out two of their legitimate primary functions of protecting against external and internal threats have protected and attacked communications and information networks in order to protect its citizens. More recently, it has been seen that certain governments have used the skills gleaned in carrying out their legitimate national initiatives to also conduct economic espionage for the benefit of their domestic constituents. Moreover, in addition to nation/state attacks on other government or corporate entities, we see, as presented in Table 3 and as cited in “Other Indicators” above, an ever-increasing number of attacks being launched by certain groups or individuals for a host of reasons ranging from mischief and crime, to retribution, to economic gain. Consequently, our review of the literature as presented above indicates that the communication security problem is large, grossly underestimated, and growing even larger at an increasing rate.

United States, Europe, Internationally, and the United Nations: A Current State of Affairs

Clearly, if the authors’ corollary to Metcalfe’s law is valid, the areas most at risk are the country or countries that have the most interconnections (potential access points).

Table 5. High Density Interconnection Environments estimated for year 2000

Area	Number	% Of World
United States Main Telephone lines	192,519,000	19
United States Wireless users	100,286,000	14
United States Internet Users	95,000,000	27
European Main Telephone lines	313,506,000	32
European Wireless users	288,455,000	40
European Internet Users	100,880,300	29
Total World Main Telephone lines	991,769,000*	100
Total World Wireless Users	719,718,000*	100
Total of World Internet Users	352,132,000*	100

Source: International Telecommunications Union (ITU) Telecommunications Indicators, http://www.itu.int/ti/industryoverview/at_glance/KeyTelecom99.htm

*The estimates in this table differ somewhat from the actual numbers cited in Table 2.

As seen in Table 5, the United States and Europe are the most interconnected communication environments in the world, comprising over half of all wireline connections, wireless and Internet users, and are hence, potentially the most vulnerable. Because of the level of communications and interconnectivity, and the concomitant levels of potential risk associated with such high levels of interconnectivity, and hence potential access points, the U.S. and Europe, comprising over half of the world’s communications activity, have numerous organizations ranging from governmental units to industry and education related entities participating in providing information or services designed to assist entities in protecting their communications infrastructures from attack (see Appendix II for a comprehensive list of resources).

1.1 U.S.A.

In the United States, the National Institutes of Science and Technology (NIST) (www.nist.gov) and the National Security Agency (NSA) (www.nsa.gov) have been vanguards in the INFOSEC arena. Most recently, these

organizations have decided upon a new replacement for the Data Encryption Standard (DES). The new replacement is called the Advanced Encryption Standard (AES) (Fisher, 2001b and Smith, 2001), and is theoretically more secure as key lengths have been expanded in addition to other improvements. Additionally, these two organizations have also worked with industry to establish five Certified Cryptographic Testing Laboratories (CCTLs) (Http://www.nsa.gov/isso/bao/cpep.htm) that will test industry computer security solutions and issue U.S. Government (USG) specified security level certifications. NIST additionally has released a detailed guide, "Self-Assessment Guide for Information Technology Systems," found at (www.csrc.nist.gov).

The **average** dollar amount lost per organization in the past year by type of security breach, according to a 2001 survey of 538 U.S. security professionals by Computer Security Institute/FBI released in March 2001 is as follows (www.gocsi.com):

- Financial Fraud: $8 million
- Theft of proprietary information: $2.9 million
- System penetration by outsider: $454,000
- Unauthorized insider access: $276,000
- Viruses: $244,000
- Denial-of-service attack: $122,000
- Laptop theft: $62,000

The Bush Administration in July 2001 also announced it will establish a Cybersecurity and Continuity of Operations Board (Verton, 2001f). This Board will have responsibility for overseeing all USG defensive INFOSEC activities. In the industry/educational arena, Carnegie Mellon's Center for Emergency Response Team's Coordination Center (CERT) (www.cert.org), the Computer Security Institute (www.gocsi.com), and the SANS Institute (www.sans.org) serve the public with alerts, information, and/or seminars so that interested parties might be in a better position to protect themselves from cyber attacks.

Recently, there has also been a significant high level of activity regarding INFOSEC functions. No less than the U.S. National Security Advisor, Condolezza Rice, has stated that every vital service in the U.S., from telecommunications to transportation, banking and energy, relies on computers, networks, and communications. "Corrupt those networks and you disrupt the nation… Today, the cyber economy is the economy," said Rice before a CIO magazine industry forum (Verton, 2001b). In this regard Rice announced her support for a joint government/industry initiative, the Partnership for Critical Infrastructure Security (PCIS). In concluding, Rice stated, "One thing we learned from the Atomic Age is that preparation…is what keeps it from happening in the first place."

The U.S. federal government established in 1998, under Presidential Decision Directive 63, the National Infrastructure Protection Center (NIPC) (Frank, 2001a). This organization's purpose is to investigate computer crimes and protect government agencies against cyber threats, as well as issue industry warnings about such threats. To date, the U.S. Government Accounting Office (GAO) has issued a report highly critical of the NIPC's efforts, principally due to the Center's lack of human resources (Verton, 2001d).

The U.S. Department of Defense (DoD) recently reported that, in addition to its extensive cyber security activities, it is establishing Computer Emergency Response Teams (CERTs) for every service agency in order to buttress its cyber protection efforts (Seffers, 2001). These CERTs will monitor all networks and issue alerts as part of their duties. Pentagon spokeswoman, Susan Hansen stated this policy stems from the DoD's desire to expand and improve the breadth and depth of the DoD's cyber security initiatives.

In January 2000, Congress enacted the Electronic Records and Signatures in Commerce Act. This Act provides the framework for electronic contracts and signatures to have the same legal standing as paper based forms. Including the civilian agencies, Congress has passed other legislation in the INFOSEC area. In October 2000, Congress signed into law "The Government Information Security Reform Act" (GISRA) (Frank, 2001b). This law requires agencies to use appropriate programs, processes, technology, and personnel to provide "adequate security" for the federal government's ever increasing IT dependencies, and report on any shortcoming annually. This law codifies the requirements of the Computer Security Act of 1987 and the guidance provided in Appendix III of the Office of Management and Budget's (OMB) Circular A-130 – the central guidance for IT management and security.

In April 2001 the healthcare arena, Republican congressmen requested and received a delay in the implementation of the "Health Insurance Portability and Accountability Act" (HIPAA) (Dash, 2001). The congressmen's' request for a delay was based upon a call for further definition of the privacy rules regarding personal health related information. This Act, PL- 104-101, authorized the Secretary of Health and Human Services

to develop security standards to prevent intentional or unintentional disclosure of any health information that is maintained or transmitted electronically. The comprehensive nature of this Act's requirements, both administrative and technical, brought about the requested delay. The Secretary has so far released five pilot policies regarding the following areas: Confidentiality and Non-disclosure, Data Classification, E-mail, Information Stewardship, and Information System Access. The next set of polices being released deal with: Security Incident, Contingency Planning, Risk Management, Risk Analysis, Configuration Management, Personnel Security and Termination.

In the financial arena, the "Gramm-Leach-Bliley Financial Services Modernization Act" (GLB) was signed into law in late 1999 (Bryce, 2001). This law became effective July 1, 2001. This law requires all financial entities including banks, credit card companies, insurance companies, mortgage companies, money transmitters, tax preparers, financial planners and others to have policies and infrastructure in place to assure the privacy of consumer related information. As Vinson & Elkins partner, Dean Harvey stated, "…entities that understand GLB are afraid because they're not ready. Those that don't understand it are afraid because they don't know where to begin."

Long standing, but yet not utilized requirements of the Securities and Exchange Commission's (SEC) regulations requiring the Board of Directors and Officers of publicly listed companies to provide adequate protection of an entity's assets (including information assets) will likely result in shareholder lawsuits, if and when, such public entities suffer losses due to cyber attacks. In May 2001in Baltimore, Maryland, at the SANS 2001 conference, Randy Marchany, a member of the Virginia Tech Computing Center's systems management group, stated that, "You can expect to see major liability lawsuits in the next 18 months or so." Echoing Mr. Marchany comments, Margaret Jane Radin, a professor of law, science and technology at Stanford University, stated that companies that fail to show due diligence in minimizing their exposure to such threats will become targets for shareholder lawsuits (Vijayan, 2001).

1.2 Europe

In early 2001 the Parliamentary Assembly of the Council of Europe was set to vote on the final draft of a new convention on cyber crime. Because the Council of Europe is separate from the European Union and includes many other states including numerous member states from the former Communist block, this legislation was deemed important in promulgating widely accepted measures in the fight against computer crime (Nuthall, 2001). However, the measure was hotly contested and amendments were demanded. In June 2001, the European Commission submitted a draft report to the Council and the European Parliament addressing the called for amendments – as of July 2001 there are no less than 25 versions of the draft document (http://conventions.coe.int/treaty/EN/cadreprojects.htm). As of July 9, 2001, the Council, Commission and Parliament have not passed the drafted cyber crime legislation. Consequently, in Europe as of July 2001, there is no overriding, comprehensive legislation regarding cyber crime. Rather, each country as of this latter date is relying on its own national laws in this regard (Radcliff, 2001b).

Although several standardization initiatives in the area of authentication have already been launched by standards bodies and industry forums at national, regional and international levels, it was ascertained that they lacked the necessary consistency and coherence for validity and cross-recognition. To remedy this, the European ICT Standards Board, with the support of the European Commission, has launched an initiative bringing together industry and public authorities, experts and other market players: the European Electronic Signature Standardization Initiative (EESSI).

EESSI seeks to identify under a common approach the needs for standardization activities in support of the Directive's requirements, and to monitor the implementation of the work program by ensuring that three main principles were adhered to:

- effective involvement of all parties concerned with the broad subject area of electronic signatures
- openness and transparency of the mechanisms used and of the initiatives taken
- encouragement of global, internationally accepted solutions whilst avoiding duplication of work (http://www.ict.etsi.org/eessi/EESSI-homepage.htm, June 2001).

1.3 Internationally

The Internet Engineering Task Force (IETF) (www.ietf.org) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF working groups are grouped into areas (e.g., security), and managed by Area Directors, or ADs. The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board, (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes (http://www.ietf.cnri.reston.va.us/, 2001).

The International Telecommunications Union (ITU) (www.itu.org) headquartered in Geneva, Switzerland is an international organization within which governments and the private sector coordinate global telecom networks and services. ITU membership represents a cross-section of the telecommunications and information technology industries, from the world's largest manufacturers and carriers to small, innovative new players working in new fields like IP networking. The ITU, which was founded on the principle of international cooperation between government and the private sector, represents a global forum through which government and industry can work towards consensus on a wide range of issues affecting the future direction of this increasingly vital industry (http://www.itu.int/home/index.html, 2001).

1.4 The United Nations

The United Nations (UN) hosted a "Global InfoSec 2001" conference at its New York headquarters in the last week of March 2001 (Verton, 2001c). One of the sponsors to this conference, the "UN Working Group on Informatics" indicated that this group is limited to making recommendations, not making or implementing policy. Nevertheless, this meeting was seen as an important initiative in raising awareness regarding the seriousness of computer security.

This lack of uniform or meaningful and universally applied legislation hampers the prevention or prosecution of computer crimes in many instances. For example, the Love Bug virus that originated in the Philippines in 2000 and invaded literally hundreds of thousands of computers around the world went unpunished, as the Philippines had no laws at the time making such actions illegal. The Philippines within weeks of this virus being launched enacted very tough computer security legislation.

Overall, however, McConnell International in conjunction with the Virginia based World Information Technology and Services Alliance (www.mcconnellinternational.com) found and reported on 52 countries in "Cyber Crime…and Punishment? Archaic laws threaten Global Information," that only ten; namely: Australia, Canada, Estonia, India, Japan, Mauritius, Peru, Philippines, Turkey, and the United States have fully or substantially updated their laws to address major forms of cyber crime. The report continued in reporting that 9 others (Brazil, Chile, China, the Czech Republic, Denmark, Malaysia, Poland, Spain, and the United Kingdom) have pushed forward legislation addressing some types of computer crimes, while fully 33 other nations analyzed such as: Cuba, Egypt, France, Hungary, Italy, Iran, Lebanon, New Zealand, Norway, Vietnam and others have no restructured laws directed at the forms of cyber crime covered in the report. And of course, even if such legislation is passed in most countries, this will not likely stop or thwart nation-to-nation, terrorist or criminal offensive activities (Armstrong, 2001).

2. Current Regulations and Export Policy

Presently, each country governs the export of communication security devices. In 1995 some 33 countries came together to frame an overall guidance on the export of certain defense items including encryption. The protocol established in 1995 and amended since is known as The Wassenaar Arrangement (www.wassenaar.org). Despite this "arrangement", the U.S. was deemed to be the most restrictive of the leading nations in this regard by limiting the strength of encryption devices that could be commercially exported. During the last years of the Clinton Administration, procedures were amended such that the U.S. Department of Commerce, Bureau of Export Controls may now issue export licenses for most software encryption to most countries, with other organizations such as the U.S. Office of Defense Trade Controls in the Department of State retaining export authority over more advanced encryption technology.

Limits on the strength of exportable encryption in necessitated by the dual requirements of governments to provide a means for their citizens' communications to be protected, but to also be able to read communications of those who would thwart the law and/or violate national tranquility. These juxtaposed requirements create the situation where governments must perform both offensive and defensive functions by balancing the requirements of each against the other. This conundrum has caused much concern for civil libertarians in the U.S. and elsewhere who claim their communications should be completely private. However, unless governments abdicate their legitimate dual, bifurcated responsibilities, such contention will continue.

3. Fundamental Elements of INFOSEC

The fundamental aspects of protecting one's communications may be seen at a high level to be comprised of the following seven basic elements:

1) Threat Analysis – determine the level and types of attacks that are reasonably expected to be experienced and implement appropriate tools to protect against such potential attacks. A cost/benefit analysis is usually a major component of this step.

2) Access Control – establish mechanisms such that only authorized users may access the network. Access controls may have multiple levels of access and employ passwords, biometrics, or other means to determine a user's identity.
3) Authentication – system verification that the users are who they say they are. Authentication may be as simple as a callback function to more advanced digital certificate or biometric implementations.
4) Confidentiality – data remains unintelligible to all but the intended, authorized parties. Confidentiality during communication is usually accomplished via the utilization of encryption.
5) Data Integrity – data may not be improperly changed or altered. This is usually accomplished during communication via a check sum/hash function validation.
6) Non-Repudiation – the receiving party cannot deny having received an authorized communication. This affirmation is usually accomplished via system verification of receipt acknowledgements.
7) System availability and reliability – this function requires constant up-time and authorized access to the network and further requires filters or other protective tools to divert Distributed Denial of Service (DDOS) attacks where protection is not provided by one of the above fundamental elements.

Of course while implementing a communication security analysis and plan, certain other fundamentals should be adhered to depending on the level of threats determined in the planning process. The underlying security planning principles are as follows:

- Least Privilege – the user only has access to a level needed to accomplish their work.
- Defense in Depth – multiple protections are employed simultaneously.
- Diversity of Defense – a variety of tools are used to insure proper, authorized use of the network.
- Fail-safe Stance: Default Deny – if an equivocal situation arises, deny access.
- Security through Obscurity – Make security implementations as obscure as possible.

Source: Shawn Irving, Presentation, April 2001, Graduate School of Management, University of Dallas as adapted by J. Nugent

In addressing the above fundamentals of INFOSEC, other overriding conditions also need to be addressed. For instance, as has been referenced elsewhere in this paper, there will likely be lawsuits filed against U.S. public corporate entities by shareholders should such corporate entities suffer a loss due to a computer security breach under the premise that the Board of Directors and the officers of the corporation did not properly execute their fiduciary duties in using due and reasonable care in protecting corporate assets. Such potential litigation should be a catalyst for prudent management of U.S. public companies to become very proactive in overseeing the entity's INFOSEC plans and implementations. In fact, the possibility of such potential litigation may make using U.S. Government approved CCTLs or other certified INFOSEC tools an imperative in order to show that the entity used tools certified by the U.S. Government – under the theory the government is the highest INFOSEC certification body in the U.S.

4. Types of Typical Attacks

As practice has shown, attack types are only limited to one's imagination (please see the Security Hierarchy Overview Diagram illustrated in Appendix I, figure I). In principal, a number of attack types have been shown to compromise most of the known attacks experienced by corporate entities. The most common types of system attacks are as follows:

- Social engineering – this attack relies on the element of human weaknesses in protecting access information.
- Malicious Code – these types of attacks are often distributed via email attachments and often infects large numbers of users. They may be created such that they self replicate. Such code, once activated, may destroy information, provide future improper access to a network, or lock-up a system.
- Distributed Denial of Service (DDOS) – this type of attack is often used when other protections have provided adequate security to the network. When such protections have denied attackers access, such attackers may resort to denying authorized users access to the network by overloading and hence crippling the network such that its performance significantly degrades or ceases to function altogether.
- Physical perimeter penetration – access to a users facility or network is gained by unauthorized physical access to the network circumventing other security implementations.

- Password cracking – typically lists of the most used passwords are tried as a means of unauthorized access to another's network. Numerous cracker, hacker, phracker, phreaker sites post lists of the most often used passwords.
- Screen emulators – this is where low level access is gained to a network and a screen emulator is placed on the access server that brings up a false screen that emulates the proper login screen. This false screen asks for the users login and password and then brings up a screen that states "login incorrect, please try again." Actually, the login was correct and the false screen emulation program has now captured another user's correct login and password. Via this means, low-level authorized parties may capture higher-level authorized parties logins and passwords.
- Data diddling or destruction – improper access is gained and an entity's information is improperly changed or destroyed.
- Wireless intercepts – intercepting either a wireless communication or signals that emanate from electronic devices (EMI/RFI). For instance, for only several hundred dollars in parts costs computer screens can be read from a half a mile or more away from the oscillations that emanate from the computer thereby thwarting access controls, authentication, encryption and other protections.

From a recent study of 4,500 security professionals concerning the most prevalent reported security breaches, an ordinal ranking can be determined as follows (Hulme, 2001b):

Table 6. Year 2000 Reported Episodes by Approximate Percent of Respondents

Type of Breach	**Percent Reporting Breach**
Computer virus, worms, Trojan horses	68
Denial of Service (DoS and DDoS)	15
Telecom or unauthorized entry	12
Web-scripting language violations	9
Manipulation of Systems Programs	9
Identity Theft	8
Fraud	7
Trafficking in illicit or illegal materials	7
Manipulation of software applications	6
Extortion	1
Mobile wireless applications intrusions	1
Unknown	12
Other	4
None	20

Other attacks that typically require more sophistication are: cryptanalysis, man in the middle attacks, fast factoring, registry or directory reengineering, EMI/RFI intercepts, IP hijacking, IP spoofing, anonymous IP addressing, and steganography to mention a few.

5. Typical Protections

Many tools, processes and procedures have been developed in an attempt to thwart improper access, utilization or destruction of networks, or information assets. No single step will likely result in adequate protection. In fact, as in weapons of destruction, there is an escalation in protection capability that is then matched or surpassed in destructive capability, with this cycle constantly repeating. In practice, professional assistance should be sought in undertaking a threat analysis and designing and implementing concomitant adequate protections. Moreover, this is a process and not an end in and of itself. That is, as technology advances so do attacks that then require newer, usually more comprehensive defenses.

Typical INFOSEC tools seen in the market are as follows:

- Threat Assessment
- Security Plan, Policies, Procedures and Architecture Definition
- Physical Security (fences, locks, surge protectors, etc.)
- Power Filtering and UPS devices to thwart oscillation interception and interpretation of power flows
- Access Controls (Firewalls, Passwords, Biometrics, etc.)
- Intrusion Detection Tools

- Virus Protection Tools
- Encryption (PKI and Private Key Systems)
- Authentication (digital certificates, tokens, digital signatures, etc.)
- EMI/RFI Shielding
- Network Management Tools (Scanners, Sniffers, Profilers, Honeypots, Shunts, etc.)
- Training and Education

New security techniques to protect networks provide companies additional layers of security (above and beyond firewalls and encryption), providing better overall security. This is especially true when they are optimized for a particular application, such as integrity of the web servers and treated as incremental solutions, not replacements to traditional network security measures. These innovative network security solutions include honey pots or decoys, air gaps, exit controls, self-healing tools and denial-of-service defenses.

Honey pots are decoy services that can divert attacks from production systems and let security administrators study or understand what is happening on the network. For example, Mantrap, from Recourse, is an industrial-strength honeypot deployed next to data servers to deflect internal attacks, and located off the firewall in the demilitarized zone (DMZ) to deflect external threats. Factors that impact its success are quality, naming scheme, placement and security policy.

The processes that an organization should have in place in order to ensure that transactions such as wire transfers, electronic investments, etc., proceed securely is to deploy honeypots in quantities equal to or greater than that of the production system. Honeypots can get expensive which is why companies must choose the critical servers they want to protect.

Air gap technology provides a physical gap between trusted and untrusted networks, creating an isolated path for moving files between an external server and a company's internal network and systems. Vendors include RVT Technologies, Spearhead Technology and Whale Communications. Self-healing tools are security and vulnerability assessment tools that can detect and fix weaknesses in an organization's systems before problems occur. For example, Retina 3.0 from eEye scans the range of IP addresses provided by the network administrator for vulnerabilities, software flaws and policy problems, reports it and can repair the vulnerability locally or remotely.

Denial-of-service (DoS) and Distributed Denial-of-Service (DDOS) attacks make computer systems inaccessible by exploiting software bugs or overloading servers or networks so that legitimate users can no longer access those resources. Vendors include Arbor Networks, of Waltham, Mass.; Mazu Networks, of Cambridge, Mass.; and Asta Networks in Seattle. For instance, Mazu Networks' solution to distributed DoS attacks works via intelligent traffic analysis and filtering across the network. A packet sniffer or packet analyzer acts as a monitoring device to evaluate packets on the network at speeds up to 1 G bit/second and determines which traffic needs to be filtered out (Haber, 2001).

As has been seen time and again, even large technically sophisticated enterprises that develop tools that are supposed to be secure are shown in time to have holes in them. In fact, it was reported that yet another severe flaw in the IEEE 802.11 wireless LAN security standard had been uncovered (Sorid, 2001). And in July 2001, even more vulnerabilities were exposed (Verton, 2001e, see also www.isaac.cs.berkeley.edu/isaac/wep.faq.html).

In a report entitled, "Weaknesses in the Key Scheduling Algorithm of RC4," authored by Adi Shamir and Itsik Mantin of the Weitzman Institute, Israel, and Scott Fluhrer of Cisco Systems, it is demonstrated how someone who is capable of capturing less than an hour's network traffic could determine a user's private key (Fisher and Nobel, 2001). However, this is not the only potential problem with Public Key Infrastructure (PKI) systems. Here we simply define PKI as an encryption system with private and public key components for each user. The private key component of each user's pair remains private, with the public key of each party wishing to communicate being exchanged with the party with whom one is to have a "secure" communication. The sender's public key is then paired with the recipient's private key, while the recipient's public key is paired with the sender's private key (the key exchange). Then, through modulo mathematics, a common key is derived for the session. For a tutorial on PKI see ("Components of PKI," www.computerworld.com, 2001). That is, as any party may purchase PKI systems, a single party may purchase several units and send many encrypted messages back and forth to himself/herself. In this manner, such a party would have both the clear and ciphered text versions of the message. The missing third piece of course would be the encrypting key. However, in mathematics it is well established that if two elements of an equation are known, one can solve for the third. Here, dense computational tools may be required to crunch the sheer number of test results in order to determine how the keys are calculated, but the process is well founded and most likely known by most sophisticated governments and possibly others. Such a potential counter to a PKI system would put in jeopardy one of the most widely used tools for protecting information today. For this reason, governments closely control and guard devices used in their applications of public key type encrypted

communications. That is, users are not able to acquire both the clear and ciphered text versions of a message (or many messages). Nevertheless, because of the overhead involved in managing and operating a private key system (key management, key generation, secure key distribution, key destruction, key storage, etc.) most individuals and businesses deem themselves incapable of efficiently and cost effectively implementing a private key infrastructure.

Other issues with PKI systems are as follows:

- Short Message Expansion – some public key systems expand short messages. This provides a great deal of information to knowledgeable cryptanalysts.
- Man in the Middle Attacks - where A thinks he is negotiating a key with B, C stands in the middle and communicates with both A and B instead of A to B. (for reference see www.incrypt.com/mitma.html). The above-cited paper by Shamir et al., is a variant on this theme.
- Non-Prime Number Keys – some PKI tools have been shown to not generate prime number keys thereby leaving them open to factoring attacks.

6. Plan of Action

In the longer term, we can expect more stringent Internet security efforts to result, including greater law enforcement and intelligence community demands for Internet surveillance in every country. In the U.S., this is already being implemented in the form of Carnivore (www.fbi.gov). There will also likely be stringent export controls on strong encryption technologies. The U.S. government will probably propose the imposition of encryption-key escrow schemes that support real-time surveillance, at least at Internet service providers (Gomolski, 2001). A digital seals mechanism (Gritzalis and Gritzalis, 2001), along with PKI services can be used to enable a level of trust in terms of not only the security of e-commerce transactions but also the quality of the exchanged services or products. As Perkowski and Kirkpatrick (2001) aptly state, "Unfortunately, security is like insurance: You never know when you will need it." Although the risk and response vary from one industry to another, Perkowski and Kirkpatrick (2001), found that size of an organization does not impact its security readiness. Their rationale is that although large companies (i.e., those with at least 1000 employees) typically devote larger portions of their IT department's staff and budget to security measures, they are also more likely to have suffered security breaches and experienced more serious security problems. In today's networks that are dynamic and constantly changing, the need to take a proactive approach to security is becoming increasingly mission-critical and the solution for businesses that are serious about e-commerce is to implement a complete e-commerce trust infrastructure.

As a practical matter, it is suggested that at a minimum entities should:

- Undertake a thorough threat assessment tempered by a cost/benefit analysis carried out by competent professionals on an ongoing basis, and develop and implement a plan
- Employ proven, and if prudent, government certified computer security tools and physical protections employing the concepts of "depth of and diversity in defense"
- Continually reexamine and test, your own systems' vulnerabilities
- Implement appropriate back-up functions and redundancies as necessary
- Update your defensive capabilities as determined as necessary from time to time
- Continually train and educate your staff relative to threats and defenses and use outside professional assistance to fill in any gaps
- Participate in educational, institutional or governmental forums that provide education, alerts, and assistance relative to threats
- Obtain adequate insurance.

7. High Level Issues and Drivers

So long as INFOSEC remains at the heart of each country's' national security, virtually no one will have absolute communications security. It can be seen here that all governments have two primary functions: 1) to protect from threats from without, and 2) to protect from threats within. No serious government will abdicate these dual responsibilities.

This requires most governments to protect their communications, while simultaneously being able to read others'. As criminal or foreign illegal actions typically take a group of some number of individuals, and as these individuals typically need to communicate somewhat efficiently, or use a communications network to carry out their acts, all communications will likely come under the purview of most sophisticated governments. As such surveillance raises privacy concerns particularly in democracies such as the United States and other free nations, a balance will have to be achieved between a government's need to know, and a citizen's right to privacy. It is

strongly believed, however, that self-preservation and purpose of duty being what it is, governments will err in favor of their need to know in order to insure domestic tranquility.

As a further evidence of the importance of government's two primary functions, the US government even mandates that a civilian agency, The National Security Agency, within the DoD oversee and manage secure communications, versus the military itself. So even the US government instills checks and balances within its own infrastructure regarding offensive and defensive INFOSEC capabilities because of the nature of communications.

Further, as industrial and economic espionage increase via the use of communications networks, such activities will likely become a major driver in entities more aggressively protecting their information and network assets. For never before have such national assets been used against law-abiding entities for purposes of economic gain as they are today. (Nugent, 1992). As was seen in the CSI/FBI Computer Crime study presented earlier, the dollar amounts of such crimes are increasing. However, often when state enterprises surreptitiously enter a corporate network, their presence goes undetected as the party merely copies information – often in the form of valuable intellectual property – versus destroying information assets themselves. Such activity was highlighted earlier in reviewing the CIA's 1999 warning concerning hidden code in Y2K offshore-re-mediated software.

In jurisdictions where legal liability can be great for officers and directors of public companies with a fiduciary responsibility to protect corporate assets, including information assets, we will likely see INFOSEC become a major driver once a claimant wins a case claiming a lack of INFOSEC protections. It is not believed that more laws will thwart or reduce the incidence of computer crime. Those that illegally penetrate or harm network or information assets will likely only be deterred by sound INFOSEC implementations that are constantly upgraded.

INFOSEC will continue to be a matter of escalating offense and defense with each side employing newer, more cleaver means of achieving their objectives. A major negative driver of course is cost. Most enterprises today are experiencing the effects of the present recession. Hence, budgets are tight, layoffs are occurring in an unprecedented number, and new funding for IT, and hence INFOSEC, is all but muted.

Psychologically, one does not expect bad things to happen to oneself. This is part of the human survival mechanism. And it has been part of the delay in entities accepting the need for INFOSEC protections. However, with the rise in hack attacks as cited in Table 3, more and more enterprises are experiencing the negative affects of not being adequately and continually protected. It is anticipated that these hack attacks may actually help senior management at most enterprises realize first hand the importance of taking action before attacks happen.

8. Conclusion

All good security plans begin with a threat assessment that details the perceived threats to an entity's information assets and networks. Based upon this assessment, a plan may be developed to map appropriate defensive tools to the threats. At this point, proposed solutions should be tempered with a cost/benefit analysis of perceived threats relative to protection costs. Any INFOSEC plan must adhere to sound security fundamentals highlighted in this paper.

As was mentioned previously, prudent actions most likely warrant utilization of INFOSEC tools receiving adequate governmental certification in an attempt to further demonstrate the entity has used prudent judgment in the execution of protecting its assets. Additionally, multiple forms of protection under the concepts of "defense in depth" and "diversity of defense" are prudent.

INFOSEC is a process not an end result. And, as the number of interconnections in the world increases, so too will the number of attacks. INFOSEC remains a relatively straightforward risk-management equation—the more security that is in place, traditionally, the more onerous it is for end-users. This status quo will not change until the technology arrives to make impenetrable security invisible to end-users. Moreover, qualified professional security personnel should be used in defining, implementing and managing an INFOSEC architecture as well as the accompanying policies and procedures that will effectively manage the process. Such personnel should receive constant adequate training to maintain the requisite level of skills needed to adequately protect the entity's information and communication assets.

Further, heeding the CIA's 1999 warning, U.S. enterprises need to be prudent in their selection of software and hardware tools. With the fifteen countries the CIA highlighted as most likely to be inserting "hidden code" into Y2K re-mediated code, there is a likelihood that such countries' intelligence services may also insert such "hidden code" in standard software or hardware products originating in those fifteen countries, and possibly others. This is significantly less of a threat in the U.S. as the SEC requires public companies to disclose all material elements of risk in their public filings. Hence, any U.S. based public company would have to disclose if it embedded such "hidden code" in its software for the benefit of a government, or it would be liable to hostile shareholder lawsuits if in fact it embedded such access without disclosing it. This is a protection that appears almost unique to the U.S.

REFERENCES

Armstrong, I., "Legislators turn up the heat on cybercrime," www.scmagazine.com, April 2001.

Boyd, C., "Metcalfe's Law", www.mgt.smsu.edu/mgt487/mgtissue/newstart/metcalfe.htm

Bryce, R., "Financial companies up against deadline," www.zdnet.com, May 14, 2001.

Costello, S., "IDC reports that security services to hit $21 billion in 2005," *InfoWorld*, www.infoworld.com. Sept. 20, 2001.

Dash, J., "Health Care IT Groups Fight for HIPAA Passage," www.computerworld.com, April 9, 2001.

Fisher, D., "Chinese hackers hit US sites," www.eweek.com, April 30, 2001a.

Fisher, D., "AES is ready to assume crypto lead," www.eweek.com, April 30, 2001b.

Fisher, D., "DDOS Attacks Raising the Bar," www.eweek.com, June 18, 2001c.

Fisher, D. and Nobel, C., "Wireless LANs dealt a new blow," www.eweek.com, August 14, 2001.

Fonseca, B., "Security research center blasted with DOS attack," www.infoworld.com, May 23, 2001.

Frank, D., "NIPC cyberdefense vision blurred," www.fcw.com, May 23, 2001a.

Frank, D., "Security deadline looms," www.fcw.com, June18, 2001b.

Gawlicki, S., "Feeling a bit --- insecure?", www.tetecombusiness.com, May 2001.

Gomolski, B., "E-Business Pulse," www.InfoWorld.com, September 25, 2001.

Gomes, L. and Bridis, T., "FBI warns of Russian Hackers stealing U.S. credit card data," *The Wall Street Journal*, p4, March 9, 2001.

Gritzalis, S. And Gritzalis, D., "A Digital seal solution for deploying trust on commercial transactions," *Information Management and Computer Security*, Vol. 9, No. 2: 71-79, 2001.

Haber, L., 'Shoring Up Security," *Network World*, pp. 53-56, May 28, 2001.

Hulme, G., "Verisign Authenticates Hacker as Microsoft Employee," www.informationweek.com, March 26, 2001a.

Hulme G., "Management Takes Notice," www.informationweek.com, page 32, September 3, 2001b.

Meek, J., "CIA officer warns of foreign Y2K trapdoors," www.abcnews.com/newscenter/internetcrime/1999/10/01/y2k1001_01.html, September 3, 2001.

Nugent, J. H., "Foreign Competitive Intelligence: A Personal View," Proceedings of the Society of Competitive Intelligence Professionals, Washington, DC, Seventh Annual International Conference, March 25-27, 1992.

Nuthall, K., "Council of Europe to vote on Cybercrime Convention," www.totaltel.com, February 5, 2001.

Perkowski, M. and Kirkpatrick, T., "The CIO Insight Research Study: Security," *CIO Insight*, Number 4, pp. 49-52, August, 2001.

Radcliff, D., "E-Merchant Beware," www.computerworld.com, page 42, June 18, 2001a.

Radcliff, D., "Playing by Europe's Rules," www.computerworld.com, July 9, 2001b.

Seffers, G., "DoD eyes more teams to counter cyberthreats," www.fcw.com, May 21, 2001.

Smith, R., "Deciphering the Advanced Encryption Standard," *Network Magazine*, pp. 94-101, March 2001.

Sorid, D., "Popular Wireless Networks Vulnerable," www.totaltele.com, February 6, 2001.

Telephony Magazine, www.internetetelephony.com, , page 28, September 3, 2001.

Verton, D., "FBI Investigating Eastern European Break-ins," www.computerworld.com, March 12, 2001a.

Verton, D., "Bush adviser urges increased cybercrime cooperation," www.computerworld.com, March 23, 2001b.

Verton, D., "UN working group seeks common ground on security," www.computerworld.com, March 23, 2001c.

Verton, D., "FBI's cybersecurity chief speaks out on GAO report," www.computerworld.com, May 23, 2001d.

Verton, D., "Bush Plans National Cyber Security Board," www.computerworld.com, July 16, 2001e.

Verton, D., "Flaws in wireless security detailed," www.computerworld.com, July 16, 2001f.

Vijayan, J., "IT security destined for the courtroom," www.computerworld.com, May 21, 2001.

APPENDIX 1

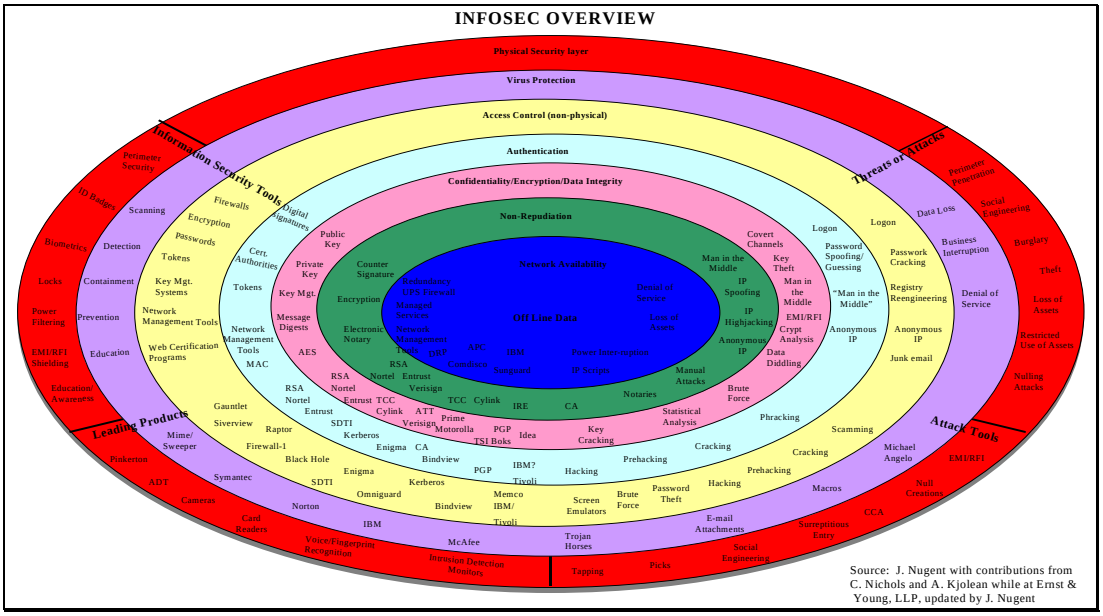

Figure 1. The Security Hierarchy Overview Diagram

The INFOSEC Hierarchy Overview diagram above may be enlarged for easier viewing. Just right-click on the chart, and increase the zoom scale on the tool bar.

Use of the INFOSEC Hierarchy Chart: This chart is the first comprehensive single source document that depicts and arrays by segment: Attack Threats, Attack Tools, Information Security Tools, and Leading Protection Products. Further, the chart bands in color rings threats, attacks, tools and products within the realm of the threat/protection schema. For example, perimeter security (the outer ring) is in the same color band as locks (Tools), theft (Threats), etc. Hence, one can literally walk into the chart beginning at the outer ring (physical security) to the inner ring – off-line operations.

APPENDIX 2

INFOSEC Resources:

www.securitystats.com – computer security statistics
www.cert.org – site provides computer security assistance and warnings
www.nsa.gov – US government site with helpful INFOSEC information
www.nist.gov - US government site with helpful INFOSEC information
www.gocsi.com – Computer Security Institute – commercial training and information source. Undertakes annual security survey with the Federal Bureau of Investigation.
www.attrition.org – site tracks web site defacements
www.dshield.org – site shows what IP addresses are being attacked
www.faisac.com – site is US government sponsored and shares threat data
www.infosecuritymag.com – Information security publication
www.insecure.org – site links to scanning tools and other security sites
http://securityportal.com/research/research.scanners.html – list of commercial scanners
www.securityfocus.com – site lists latest news and updates on viruses and malware
www.sans.org - organization provides seminars, training, and alerts
www.isc2.org – International Information Systems Security Certification Program
www.packetstorm.security.com – hosts vulnerability reports, tools and other useful material
www.ietf.org/html.chapters/ipsec-charter.html – IPSec Protocol for VPN security
www.wedi.org/SNIP – HIPAA information site
www.per-se.com/news/hipaa – HIPAA information site
www.scmagazine.com – computer security magazine
www.fcw.com – magazine that tracks US government computer issues
www.computerweek.com – computer industry publication with many INFOSEC article