Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Need for Information Security in Today's Economy

Information is the primary commodity in world of E-Commerce. As technology advances and access to markets expand, the need to protect information to ensure its confidentiality, integrity, and availability to those whom need it for making critical personal, business, or government decisions becomes more important. With nearly than half of the U.S. economy estimated to be producers or intense users of Information Technology by the year 2006, the need for Information Security is crucial. Without protection, the success of...

Copyright SANS Institute

Author Retains Full Rights

AD

The Need for Information Security in Today's Economy

Dated: 1/5/2003
Author: Jeff Tarte
Version: GSEC Practical Assignment v1.4b
****

Introduction:

The 1990's can be characterized as the *decade of Information Technology*. Advancements in computer and telecommunication technologies helped to drive the U.S. and world economies to staggering growth through the year 2000. The technological advancements and their impact on the economy and society have had a revolutionary effect around the world, similar to that of the Industrial Revolution of the 18th and 19th centuries. This growth was also driven by the acceptance of the Internet as a medium for communication among consumers, businesses, and governments. The Internet provided a cost-effective and efficient medium to share information that the world had not seen prior to the 1990's. In 1995, the U.S. had approximately 18 million users on the Internet, and as of April 2002, there were more than 165 million users.[1]

The advancement of technology, the Internet, and information sharing has had both positive and negative impacts. One of the negative impacts was the large increase in new "information" threats. The number of threats and reported computer related incidents increased at a tremendous rate by the end of the 1990's, and into the 2000's. Many of the computer incidents exploited confidential information being stored by companies in a variety of different industries. The ability to carry out threats against information systems has been made easier due to the sharp increase in system vulnerabilities. Unauthorized access to confidential information was also the result of weak or non-existent information security practices. Not identifying and mitigating risks is a leading cause of unauthorized access and the exploitation of vulnerabilities.

These computer incidents have raised a number of concerns about how information is secured and maintained. With such a critical dependency on information, a threat to the security and trustworthiness of information was also a threat to the U.S. and world economies. The cost to protect against information threats has increased as the number of threats and vulnerabilities also increase. However, the cost of a security breach to an organization can be considerably higher in many cases.

Many businesses have been slow to adopt sound Information Security practices to protect company and customer information. The components that make up Information Security are designed to address and mitigate the risks to information. The inclusion of Information Security into corporate IT

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

infrastructures, budgets, and strategies is critical to the survival of most companies and the economy overall.

One of the biggest concerns to consumers in the late 1990's and into the 2000's has been *consumer privacy*. There has been a growing concern about the increase of reported fraud and identify theft. The increase can be directly related to the advancement and impact of the Internet around the world. Consumers need to be aware of the threats that could result in these crimes, and what their role is against them. Consumers must also be cautious about giving their information to companies that do not appear to follow standard security practices to protect information.

For Information Security to be successful in today's new economy, it will require the involvement of all of its players to work together. Because many organizations and governments have been slow to adopt the concepts of Information Security, the need for standards and regulations is required to provide the proper direction for successfully protecting information.

As with the Industrial Revolution, the need to identify and manage the negative effects of technological advancements is crucial. By not addressing these issues, the success of the technological advancements may be short-lived. It is critical that Information Security play a major role in the new age of Information Technology.

e-Commerce - The New Economy:

The Internet has changed the landscape of commerce around the world. Not since the Industrial Revolution of the 18th and 19th century has the world seen such a comprehensive advancement in technology and commerce.

During the Industrial revolution, the advancement of machinery for the production and distribution of goods was the catalyst for commerce and society. The Industrial Revolution can be characterized as the time when businesses migrated from the utilization of hand tools and handmade goods to that of machinery and mass-produced goods. The timeliness, cost, and availability of goods helped to spur population growth and urban centers to employ in the new commercial society. This revolution sparked more than 200 years of advancement and the development of a world economy.

Like the Industrial Revolution, the *Information Technology Boom*, which started in the 1990's and is still present today, has dramatically changed commerce around the world. This is mostly due to the advancement of technology in computers, telecommunications equipment, and networking standards, leading to the development and widespread use of the Internet. The Internet was originally developed in 1969 and was called ARPANET. The Internet was merely a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

communication tool used for the military, its contractors, and universities as a way to easily communicate with each other.[2] It has undergone a natural transition from private, restricted usage, to widespread public commercial and consumer usage by the 1990's.

There are more than 500 million Internet users worldwide as of the year 2002. Of that amount, 165 million users are from the U.S.[3] The Internet has provided businesses with the ability to market their products anywhere in the world without incurring the costs of the normal brick and mortar commerce model, which requires you to have a physical presence to be successful. The Internet broke these physical barriers, and allowed commerce to flow freely throughout the world where the Internet was available.

In addition to accessing new markets, businesses have benefited from the free-flow of information that is facilitated by Information Technology and the Internet. It is the availability and sharing of timely information that allows businesses to strive in the new economy. This information allows businesses to make better decisions and bring to market products and services that are more tailored to meet the needs of individual consumers. As stated by James Chessen, a chief economist for the American Bankers Association, "Information Technology has radically changed how business is done today. With greater access to information, businesses have better control of inputs, better control of inventories, and lower advertising and marketing costs."[4]

Better decision making in turn, allows businesses to become more efficient with the production of goods or services. In theory, the business model's cost per transaction or goods produced, should be reduced, and therefore resulting in additional profit for the business. This results in the expansion of business models to newer markets, products, and services, and allows for the reinvestment of capital for new ventures.

The free flow of information has become a major commodity in the U.S. and world economy, and the catalyst for Information Technology. It is estimated that "by 2006, nearly half of the U.S. workforce will be employed by industries that are either major producers or intense users of Information Technology products and services."[4] The *Information Technology Boom* of the 1990's has also spawned a major boom in the Information Technology industry. As a result, spending on information and telecommunications technology rose from nearly $1.3 trillion in 1993, to $2.4 trillion by 2001, while online purchases totaled nearly $600 billion."[4]

The falling out of the "dot.com" businesses and the downturn of the U.S. and world economy has had an impact on e-Commerce, but the slowdown is only seen as temporary. The economy will be back on track as advancements in Information Technology continue. The next frontier of technology appears to be in Wireless networks and devices. Wireless communication, still in its early stages, is known for its weak implementation of encryption and security controls.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Currently, nearly 85 million Internet users worldwide access the Internet via Wireless technologies. This number is estimated to grow to 387 million users by the end of 2004.[5] These numbers are a clear indication that information technology is still a major economic commodity and a way of life.

Information Technology Threats:

With the advancements in Technology also come problems. While the industrial revolution had a number of innovations and spurred the development of a commerce-rich society, it also had its share of problems. These problems ranged from unsafe working conditions, child labor, and low wages, to pollution and overpopulation. While there were occurrences of these problems before the Industrial Revolution, the amount was minimal. The occurrence of these problems greatly increased as the Industrial Revolution continued.

The *Information Technology Boom* also experienced its own problems. Most of these problems were a direct result of the advancement of technology, the Internet, and the free flow of information throughout the world. A majority of the Information Technology problems involved the gathering, storing, availability, and sharing of information. There are now new threats to businesses, consumers, and governments, and a sharp escalation of existing threats that have taken advantage of technological advancements. New technology also provides those who are exploiting these threats, with additional methods of hiding their actual identity making it more difficult to stop such activities.

There are a number threats to information and information systems that impact a majority of the world's population. Most businesses, consumers, and governments now maintain or transmit their information using some type of information system designed since the 1990's. Most of these information systems are also directly or indirectly connected to the Internet through the use of a Local Area Network (LAN) or Wide Area Network (WAN). For those systems that are not connected to the Internet, many still share information with remote computer systems utilizing a dedicated private data connection point (using frame relay, ISDN, ATM, or other intranet connection method) or in some cases a modem connection over the public phone system. Each of these scenarios depicts a method of sharing information electronically.

Threats to information systems that do not share information with any other system are fairly minimal. In most cases, security is accomplished by restricting physical access to the computer system and then restricting users physically and electronically. Without physical access to the system or its output, unauthorized use is not possible. Protecting information systems in this scenario are very much the same as protecting any physical asset. Most physical security safeguards are adequate to protect this environment, including the backup of information to physical media in case the system encounters problems. The

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

principles of physical security have been around for a very long time and most are implemented in all businesses.

While physical security controls are still required for the protection for information systems that do connect with other systems electronically, the need for *physical access* to the system is now *not required* to access information. This problem now opens the floodgate for a multitude of possible threats to information and information systems that did not exist before. Combined with the fact that more than 500 million people can now potentially gain access to your information systems, you have a problem. Here is where information security becomes a necessity.

While there are a number of different internal and external threats to information, not all information systems are at risk because of their design, or the information that they maintain. The number of vulnerabilities can impact the associated risk of a threat. The following is a list of common threats to most information systems:

1) Unauthorized access, alteration, or destruction of information.
2) Misuse of authorized access to information.
3) Accidental alteration or destruction of information.
4) Malicious software programs (viruses/worms/trojans).
5) Misconfigured or poorly designed information systems allowing too much access.
6) Social engineering.
7) System or communications disruptions (denial of service, hardware failure).
8) Improper handling of information. *
9) Physical theft of information or information systems. *
10) Environmental hazards (flood, fire, earthquake, snow, etc.). *
11) Utility failure (power, water, heat, etc.). *

* *Indicates a relation to physical security practices.*

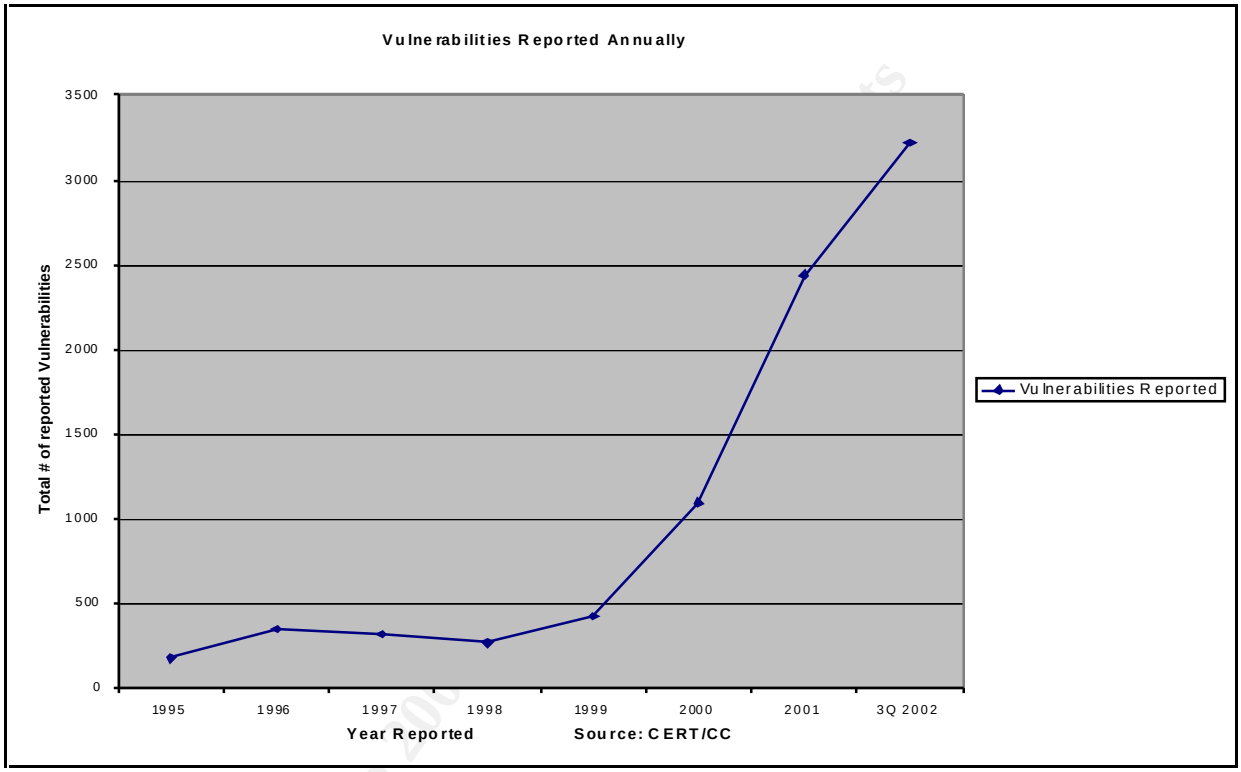
Information Security Vulnerabilities:

Vulnerabilities can be defined as identified weaknesses in information systems, policies, and procedures that can facilitate a successful exploitation of a threat. A threat cannot be carried out without a vulnerability that can be exploited. The fact that a threat and vulnerability exists in turn creates risk. The likelihood of the threat and vulnerability being exploited determines the overall risk probability or score. Not all vulnerabilities are relevant to every organization.

Many of the vulnerabilities that exist in today's economy are directly related to the advancement of technology. Most vulnerabilities tend to be found in the operating systems and applications on computer systems and devices that are

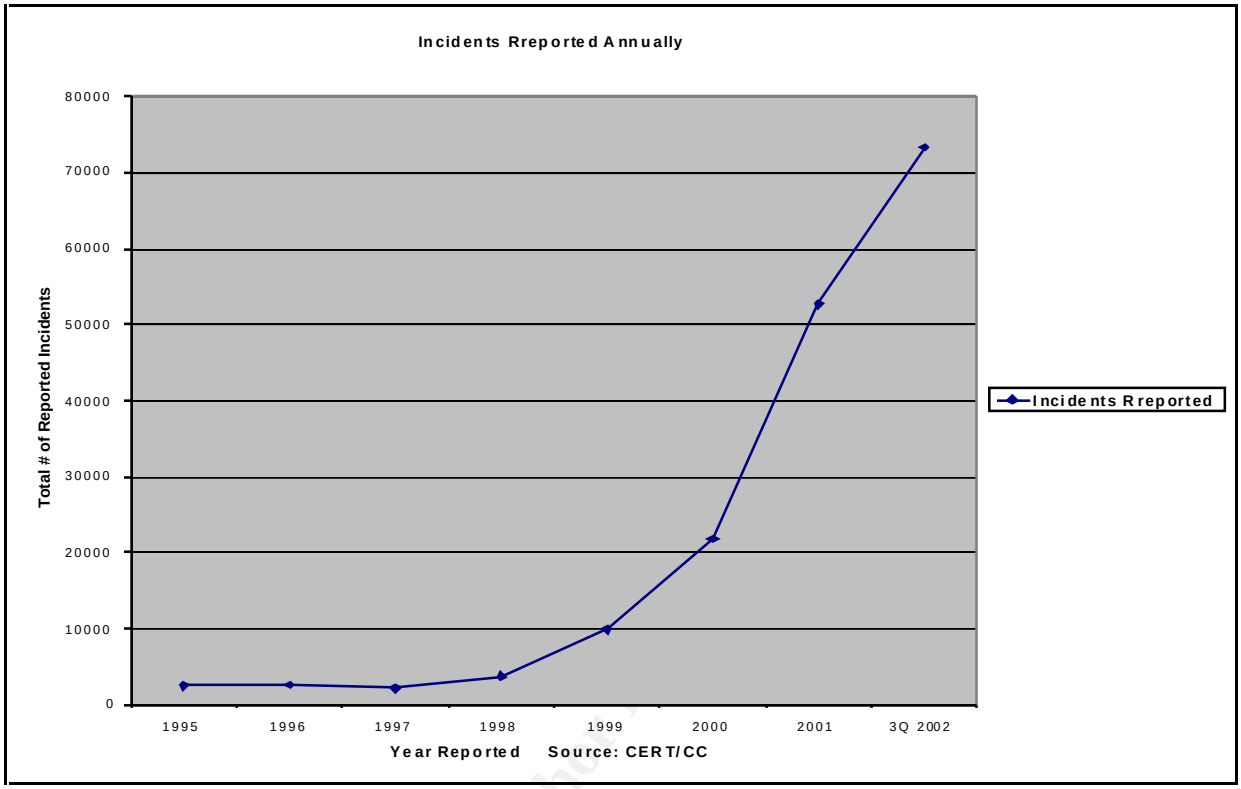
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

used to maintain the information in the first place. The total number of annual reported system vulnerabilities has skyrocketed from 171 in 1995, to over 2,437 in 2001. The total number of reported vulnerabilities since 1995 through the 3rd quarter of 2002 is 8,255.[6] The total increase in reported vulnerabilities since 1995 was more than 4800%. The chart below shows the true scale of the increase in vulnerabilities.



With the low cost of technology and the worldwide availability of the Internet, the possibility of exploiting vulnerabilities and turning threats into reality is a major concern. The increase in reported incidents of exploitation is staggering. In 1988, the reported number of incidents was 8. In 1995 the number was 2,412, and in 2001 the number was up to 52,658. The total number of incidents reported from 1995 to the 3rd quarter of 2002 is 168,485.[6] The total increase in reported incidents since 1995 was more than 6900%. The chart below shows the true scale of the increase in reported incidents.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Information Technology Risks:

Like in the Industrial Revolution, advancements seem to create problems. Without machinery that mass-produces goods, there would be less pollution. Likewise, without the advancement of information technology and the Internet, there would be fewer vulnerabilities and security incidents. It is, however, a reality that must be dealt with for e-Commerce to survive and prove it to be a positive business model in the future. To deal with this reality, addressing information risk is crucial.

Having a process in place that identifies both threats and vulnerabilities is only one step in managing risk. Many other steps also need to be taken:

1. Identifying and classifying critical assets.
2. Analyzing the possibility of vulnerabilities being exploited.
3. Associating a level of risk to vulnerabilities and threats.
4. Measuring the potential cost of a successful exploitation of a threat.
5. Implementing the appropriate controls to manage risk.
6. Periodically reviewing and updating the risk management strategy.

These steps are essential to a successful risk management strategy. The purpose of risk management is to identify and mitigate risk to an acceptable level. The goal of risk management is to protect critical assets. A critical asset

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

could be defined as physical assets, information, reputation, financial strength, relationships, business strategy, or any other component that is critical to the viability of a person, business, or government.

The Role of Information Security:

With the structure of the world and U.S. economies becoming so dependent on the ability to share information and information technology resources, it presses the issue of the security and validity of the information. Has the information being shared been legitimately obtained? Is the information accurate? Is the information secure? Who has access to the information? These are all questions that should be asked by all users of information technology and by those that have provided information to others. Information Security's role in this economy is to ask and answer these questions.

The goal of Information Security is to ensure the confidentiality, integrity, and availability of information. The integration of Information Security practices with E-Commerce and all other entities that use information should be a logical process. In reality, this is not necessarily the case. The integration of Information Security into personal, commercial, and government information technology resources is still a long way from where it should be. This, in turn, puts a majority of the information currently being shared at risk for unauthorized access, use, alteration, and destruction. This presents a problem to sustaining an economy that depends heavily on information.

The implementation of Information Security is generally perceived to be a negative impact on a person, business, or government, when in fact it can provide just the opposite. While controls generally do have a monetary or procedural impact in many instances, it also can provide a major improvement to relationships in the form of *trust*. There are many ways in which Information Security can provide not only the protection of information and reputation, but also a competitive advantage, enhanced processing capabilities, and better decision making.

The Cost of Poor Information Security Practices:

The primary reason behind the slow adoption of integrating Information Security into many homes, businesses, and governments is the reluctance to understand and acknowledge that the threat to information is real. It is usually too late before it is acknowledged. In most cases, it is a successful hacking attempt or identity theft that finally gets someone's attention.

One of the reasons for not acknowledging that the threat is real is because you rarely hear about it. Of the 168,485 incidents reported since 1995, how many

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

have you heard of? If management doesn't feel that they need to be concerned with Information Security, then why should they allocate more capital for its cause? This is especially true, because showing a Return-On-Investment (ROI) of Information Security is difficult to calculate. Unfortunately, there is no global Information Security ROI calculation that can be applied to measure the impact of Information Security. It is still in the company's best interest to budget security spending based on the results and prioritization of their risk assessment. According to survey conducted by KPMG in 2002, "the average direct loss of all breaches suffered by each organization is USD$108,000."[7]

Most incidents do not get any press because of the obvious drawback: *bad publicity*. A story released to the public acknowledging a successful penetration of a company or government agency's information systems, or of extortion due to stolen information, can have a negative impact. In addition to the embarrassment, it could also affect the vitality of the organization.

For most organizations, the release of such a story would have a damaging impact on its image and reputation. This is especially true for industries that rely on trust, such as banking, insurance, healthcare, and government agencies. Over the past few years, there have been a number of e-Commerce firms that experienced a serious downturn in business after a public release of a serious security breach.

Another major consideration is the impact of the theft of intellectual property. A competitor that knows your business or product secrets can potentially drive you out of business. A government agency that loses critical military information to the enemy can cause injury or death to its citizens. Even worse, a hacker that penetrates a system providing access to medical or military information can alter the information with deadly results.

The impact on individuals can also be devastating. One of the biggest concerns for individuals is the loss of privacy. The release of sensitive medical, family, or financial information to unauthorized parties can have unwanted results. Worst yet, is identity theft. The effects of Identity theft, the use of personally identifying information, such as a person's name, address, social security number, etc., for the purposes of committing fraudulent acts under another person's identity, can be costly, emotional, and hard to live with. The Identity Theft Resource Center estimates that there were between 700,000 to 1.1 million victims of identity theft that occurred in 2001. The financial loss for these victims is estimated at nearly $12 billion.[8] The increase in identity theft claims can be directly related to the growth of the Internet.

These incidents have a negative effect on the economy, which relies on information for its critical business decisions and relationships with its business partners and customers. If consumers are not confident that their privacy is being protected, it may force them to find alternate methods for doing business,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

or refrain from conducting business altogether. Analysts have estimated that privacy concerns by individuals have resulted in lost Internet sales for businesses in the amount of $18 billion.[9]

Information Security Components:

There are a number of major components that make up Information Security. Some of the major components of Information Security are:

- Risk Management Programs
- Policies, Procedures, and Standards
- Intrusion Detection Systems
- Incident Response Programs
- System Monitoring
- Access Controls
- Management Sponsorship
- Continuous Assessment and re-alignment of the above components on a regular basis to make sure that they are still relevant to the organization or information that is being protected.

In most cases, there is an enormous amount of information available on each of the topics above. White papers, software programs, training classes, case studies, books, magazines, and a myriad of other resources are available to help the Information Security professional to understand, formulate and implement an Information Security program that is right for his or her organization. Because companies maintain different information and must address different threats and vulnerabilities, there is no one Information Security model that can be applied to all organizations. It is accurate to state however, that the core components that comprise Information Security are valid in most scenarios.

It is also important to realize that Information Security is not just a technology issue, but also a people and business issue. This helps to emphasize that the role of Information Security does not begin and end with Information Technology, but is a reflection of the overall management, reputation, and culture within an organization. The products and services offered by an organization will also reflect the commitment an organization has to protecting information.

Information Security Players:

Implementing security controls is not solely up to one individual, one company, one information system, or one government. It is a combination of all of them. The following are some of the major players in Information Security:

- Individuals

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Businesses
- Manufacturers
- Governments
- Auditors (internal and/or external)
- Standards Bodies

Each of the above players must do their part to ensure that Information Security does what it is supposed to-- protect information.

Individuals must be more aware of what information is given out and to whom. Sensitive information should only be given to those that can be trusted, and require it to provide goods or services. The only way individuals should transmit or share information is when it is being done securely (e.g. using SSL). Individuals must also do their part to ensure they are installing and updating security controls (e.g. patches, virus updates) that protect their information systems.

Businesses must ensure that they have the proper Information Security Programs in place to analyze and mitigate risks, implement appropriate security and access controls, educate and train its employees on how to protect information, monitor and assess program compliance, and review and update their program on a regular basis. Businesses have a greater responsibility when it comes to protecting sensitive information, since they maintain information for many people and are trusted to protect it properly. Businesses may face criminal and/or legal problems if they do not adequately protect sensitive information. It is imperative that Executive and Senior Management members be involved in the overall direction and integration of Information Security into the culture and business environment of all companies.

Manufacturers play a major role in Information Security by providing the hardware, software, and operating systems that make up an information system. Vulnerabilities are generally linked to a flaw in manufacturer system programming or design. It is critical that manufacturers are security conscious and build their systems in a manner to protect the information that they will process. The lack of secure information systems has been a major roadblock to the success of Information Security. Too many Information Security resources are forced to monitor, test, and correct flaws that are found in applications and operating systems.

Governments have a number of roles to play in the success of Information Security. Governments (or certain agencies) generally maintain the most sensitive information of all players. The protection of classified information, military secrets, agency investigations, foreign relations, citizen information, and other sensitive government controlled information is of the utmost importance. The government needs to be the leader in the Information Security field, and set the groundwork for others to follow. This, unfortunately, is not the case. While

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

strides are made protecting military information, the same practices are not followed in other federal and state government agencies.

The *Government* also plays a role in the development of laws and regulations to promote Information Security. The recently passed Cybercrime Act amends the Criminal Code Act 1995, by adding additional penalties for people who commit computer crimes. The recently approved USA Patriot Act of 2001 also provides the basis for an expanded investigated reach of the government for investigating Internet related crimes and cyber-terrorism. While this can be considered by some as an invasion of privacy, it also encourages the advancement of security controls and the penalties against those that commit electronic crimes. The UK also enacted regulations, the Data Protection Act, to encourage better protection of information.

Other major regulatory measures passed in the U.S. include the updated Fair Credit Reporting Act (FCRA), Health Insurance Portability & Accountability Act (HIPPA), and the Gramm-Leach-Bliley Act (GLBA). All of these regulations contain consumer privacy and information security components that are geared towards protecting information in the Banking, Insurance, Lending, and Healthcare industries. The positive effects of regulations appear to be working, as testified to the Senate Banking Committee. "As a result of the GLB Act, financial institution customers are far more privacy and security-protected than they were three years ago, and far more protected than the customers of companies in other industries."[10]

While *Auditors* are not always the most liked of the players, they are important. It is their role to review the practices of businesses, governments, and manufacturers to ensure that they are following best practices for Information Security, and are addressing the risks associated with their respective industry. They also play a major role in bringing attention to management and politicians about the real dangers of poor Information Security Practices. Unfortunately, not all industries are regulated, so many companies may not use them since it is not mandatory.

Standards Bodies are responsible for developing Information Security Standards based on input and research by some or all of the players mentioned above. It is the sharing of ideas, challenges, experiences, and solutions that results in the development of security standards that can be used by most players in Information Security. Examples of these standards bodies, include those developed under the National Security Association (NSA), National Institute of Standards and Technology (NIST), Organization for Economic Cooperation and Development (OECD), International Organization for Standardization Standard 17799 (ISO 17799), and the IT Governance Institute. The standards developed under these bodies are key resources for Information Security and IT professionals around the world.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion:

Information is the primary commodity in world of E-Commerce. As technology advances and access to markets expand, the need to protect information to ensure its confidentiality, integrity, and availability to those whom need it for making critical personal, business, or government decisions becomes more important. With nearly than half of the U.S. economy estimated to be producers or intense users of Information Technology by the year 2006, the need for Information Security is crucial. Without protection, the success of an E-Commerce marketplace may be short-lived.

The world economy has changed over the past decade; mostly by the positive impacts of a technology revolution, or *Information Technology Boom* of the 1990's, which spurred by the advancements in computers, networking, and application development. This, coupled with the lower cost to produce these items, has helped to facilitate the creation of the Internet as a global telecommunications media where people can share information and access products and services electronically. Changes to the global economy and its positive impact on society resulting from the technological advancements from the *Infomation Technology Boom* can be compared to the impact of machinery advancements made during the Industrial Revolution in the 18th and 19th century.

There have also been problems that were introduced by the advancement of technology and the free flow of information globally. As seen with during Industrial Revolution, rapid changes in technology, commerce, and society also bring with it unexpected negative consequences that must be dealt with. The primary problem involves the new threats and vulnerabilities to information that were not considered serious risks as we entered the *Information Technology Boom*. Many of the threats became reality as the growth of the Internet around the world and the role of Information in most major areas of business, government, and society began to shape the new electronic world economy.

The number of reported information system vulnerabilities and security incidents have increased dramatically during the late 1990's and into the present day. The need to assess and mitigate the risks to information is major step in protecting information from the new threats and vulnerabilities. This sparks the necessity for Information Security in all areas of business and government to manage the protection of information assets. Without Information Security, the fate of the new economy so dependent on information may be short lived.

It is the role of Information Security to provide the basic requirements to successfully integrate security into Information Technology in a manner that properly addresses real threats. It is the goal of Information Security to ensure the confidentiality, integrity, and availability of information. Implementing weak Information Security controls can result in the loss of trust, reputation, and money

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

for consumers, businesses, and governments. The sharp increase in the number of fraud, extortion, and identity theft crimes is a primary result of weak Information Security controls. The cost of implementing basic controls to protect information is generally much less expensive than a security breach.

Weak Information Security controls can generally be contributed to the lack of understanding and acknowledgment of the real threat to information. The need for business and government leaders to realize the benefits of security controls and integrate them into existing and new IT environments is key to the success of Information Technology and the economy that is driven by the sharing and availability information.

There are a number of resources available for consumers, businesses, and governments to assist them in creating an Information Security Program that works for their environment. Industry Regulations and Information Security Standards documents have been developed for the purpose of offering practical guidelines for the implementation of Information Security controls for many different environments. The development of regulations and standards is a direct result of the need for better protection of all information systems.

The role of Information Security is essential for the protection of consumers, businesses, governments, and the U.S. and World economy from the threats caused by the natural advancement of Information Technology and society as we know it.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

List of References:

[1] "NUA Internet How Many Online." *NUA*. URL: http://www.nua.ie/surveys/how_many_online/n_america.html (29 Dec. 2002).

[2] "The Internet Economy Indicators." URL: http://www.internetindicators.com/factfigure.html (30 Dec. 2002).

[3] "Cybercrime Law: How do we Deal with Infosecurity?" *SC Magazine*. October 2002. URL: http://www.scmagazine.com/scmagazine/2002_10/feature_1/ (22 Dec. 2002).

[4] Chessen, James. "Information and Privacy." *American Bankers Association*. February 2000. URL: http://www.aba.com/aba/PDF/iandp.pdf (29 Dec. 2002).

[5] Greenspan, Robyn. "Wireless Surfer Numbers Grow." *Jupitermedia Corporation*. 6 Sep. 2002. URL: http://cyberatlas.internet.com/markets/wireless/article/0,,10094_1457671,00.html (29 Dec. 2002).

[6] "CERT/CC Statistics 1988-2002." *Carnegie Mellon University*. 4 Oct. 2002. URL: http://www.cert.org/stats/cert_stats.html (22 Dec. 2002).

[7] "2002 Global Information Security Survey." *KPMG*. URL: http://www.kpmg.com/Rut2000_prod/Documents/9/giss.pdf (29 Dec. 2002).

[8] "Facts and Statistics: Find out more about the Nation's Fastest Growing Crime." *Identity Theft Resource Center*. 28 Oct. 2002. URL: http://www.idtheftcenter.org/html/facts_and_statistics.htm (31 Dec. 2002).

[9] Gellman, Robert. "How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomlpete." *Privacy, Consumers, and Costs*. Mar. 2002. URL: http://www.epic.org/reports/dmfprivacy.html (30 Dec. 2002).

[10] Pitts, Jim. "FSCC Testifies Before Senate Banking Committee on Privacy Legislation." *Financial Services Coordinating Council*. Sep. 2002. URL: http://www.fsccnews.com/articals/20020919.html (22 Dec. 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**