

Threats Posed by the Internet¹

Abstract

Consider the proverb, “All roads lead to Rome.” With the Roman Empire’s road system spanning over 52,000 miles, this wasn’t too far off base. While the network was essential to the expansive growth of their civilization, it presented a double-edged sword to the Empire. In 213 B.C., Hannibal led a Carthaginian army astride elephants down the very roads the Romans built. Although Hannibal wasn’t victorious, his offensive represented the first attack to utilize the enemy’s critical infrastructure. In essence, the Roman Empire’s network of roads had become its Achilles’ heel.

In our current day, over 2,000 years later, you’ll find modern-day Hannibals in cyberspace. Instead of riding lumbering elephants into Italy, these attackers leverage worms and viruses to swiftly target information on home computers, office systems and mobile devices worldwide. The immediate fallout from a stolen credit card number or patient record may be obvious, but it’s important to note that each data breach brings with it the potential for a significant ripple effect. Because of the interconnectivity afforded by the Internet, as well as by corporate and wireless networks, the initial breach of a low-level computer can open the door to other, more sensitive systems containing data that can fetch a high price on the black market.

U.S. Department of Homeland Security statistics showed that 37,000 attempted breaches of government and private computer systems were reported in fiscal 2007, which ended Sept. 30, marking a dramatic increase from the 24,000 reported in 2006. Cyberattacks against federal agencies rose 152% during the same time period, from 5,143 to 12,986.

The Internet began life without security, and it will never be possible to retrofit any mechanism to effectively eliminate the threat posed by this omission. Those that seek to protect the users of the world's networks are destined to continually respond to the adoption of new techniques and methods by criminals, always reacting and rarely being truly proactive.

Anecdotal and statistical evidence confirms that the threat posed by the Internet has changed completely since the turn of the century. Gone are the days of criminal intrusion to massage egos and cement reputations; instead the Internet is now a profit-generating machine for organized, dedicated and highly skilled teams of criminals. They operate in a truly global environment, largely with impunity and without fear of the law enforcement response that serves as their only deterrent.

We have increased cooperation between law enforcement and industry; we have written more secure software; we have educated users; and we have increased penalties for those convicted of these offenses. Unfortunately, while we have made progress in the field of cybersecurity, due to the persistence and number of attackers our nation’s systems

¹ Produced by the Threat Working Group of the CSIS Commission on Cybersecurity for the 44th Presidency.

continue to be susceptible to a number of cyber threats. Why? Because the Internet underground is now, more than it ever was, about generating maximum revenue with minimal risk, and this combined with the ever increasing of complexity in software, makes for continued success in exploiting targets. Until our combined response meets and exceeds the efforts of the enemy, we will continually face defeat in these battles.

I. Actors

Threat Actor(s): People who intend to exploit vulnerabilities, or an entity (person or group of persons) that would initiate an event, or series of events, that would in turn exploit a vulnerability.

To date, cyber threats have been motivated by criminals and discontented insiders, as well as individual thrill-seekers and cyber-activists. It is also now clear that military adversaries and trans-national threat actors are already considering or developing the use of cyber attacks to strike at nations that possess superior conventional military capabilities.² The capabilities available to the average individual with a computer and an Internet connection are staggering. Many have warned of a gathering storm that could disrupt many of the systems upon which our society relies. Clifford Lau, chair of IEEE-USA's Research and Development Policy Committee, said, "The Country's problem with cyber security is very serious and it is going to get worse in the next five years before it gets any better. I would say the situation not only is alarming, but it is almost out of control."

This becomes more of a concern as the consequences of cyber attacks can now rival the those of physical attacks. In fact, recent research demonstrated that cyber attacks can have physical consequences and, as a result, the Department of Defense is considering an experiment using the application of cyber-force. In the DoD's mind, this question has already been answered. Jeffrey R. Cooper, director of strategic analysis at SRS Technologies, stated, "Although attacks in the cybersphere do not involve the use of physical weapons, their destructive impacts, physical and otherwise, may be no less lethal to society."³

Recent no-warning cyber attacks on Estonian government websites and critical infrastructures demonstrate that targets of technology savvy state enemies can be military forces, government institutions, critical infrastructures or commercial entities.⁴ According

² John A. Serabian, Jr., Information Operations Issue Manager for the Central Intelligence Agency testifying before congress, Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy, 23 February 2000, Washington D.C.

³ Jeffrey R. Cooper, "Another View of Information Warfare," in *The Information Revolution and National Security Strategy*, ed. Stuart J.D. Schwartzstein (Washington, DC: The Center for Strategic and International Studies, 1996), 122.

⁴ Rebecca Grant, Victory in Cyberspace, An Air Force Association Special Report, October 2007.

to McAfee's® annual global cyber trends study, there were more reported cases of cyberattacks on critical national infrastructure (e.g., financial markets, utility providers, air traffic control, etc.) in 2007 than in previous years.⁵

The importance of technology and the proliferation of both cyber threats⁶ and events have turned cybersecurity to an issue of national security. It is critical, before more threats are realized⁷, that we characterize the capabilities and motivations of actors who use cyber attacks to advance their goals.

The Nation State: The traditional threat actor in the national security realm has declared intent and demonstrated capability to use cyber attacks. Other countries have followed the lead of the United States by extending traditional national security capabilities and military operations to cyberspace. We have seen that traditional activities such as intelligence gathering or espionage can be transported to information systems and the Internet. Some instances of cyber attacks as a means of waging war or conducting operations outside of war to influence another nation are becoming more prevalent.

In 2007, the FBI reported that there are 108 countries with dedicated cyber-attack organizations seeking industrial secrets. Databases have been the preferred target of cyber-criminals and nation-states. There is evidence that the underground economy has been proliferating attack tools and techniques to the nation-state community.

Of the state actors, the Russians have exhibited a greater skill due to the organized combination of “tradecraft” and cyber-attack vectors. The Russian state desires to suppress command and control as well as increase capabilities per the interception of data and the improvement of their own electronic countermeasures.

The Chinese have dedicated increased resources to the cyber-infiltration of networks, and their strategy is aligned with the concept of “100 grains of sand”—wherein they infiltrate as many networked systems as possible and lie in wait for sensitive data and/or command and control access. The Chinese are rumored to have begun significant research and development of hardware-based rootkits.

Terrorists: However, it is not only nation-states that pose a cyber threat to our military. As terrorist groups grow in sophistication, they are maturing in their abilities to leverage

⁵ McAfee® Virtual Criminology Report, *Cybercrime: The Next Wave*, Annual Global Cyber Trends Study, 2007.

⁶ Cyber Threat: Any circumstance or event with the potential to intentionally exploit one or more vulnerabilities in a system resulting in a loss of C,I,A. US CERT

⁷ Realization of a Threat: Requires both a “threat actor” and an action to exploit a vulnerability

the cyber attack as a weapon of choice. As well-educated but socially disadvantaged young people are attracted to terrorist causes, the real potential of asymmetric cyber attacks will only grow.

Terrorist groups have been learning from cyber criminals for years on how to hack systems. Some examples of this evolution follow:

- “Muslim Hackers Club” reportedly featured links to U.S. sites that disclose sensitive information such as code names and the radio frequencies used by the U.S. Secret Service. The same website offered tutorials in hacking.
- Irhabi 007, a famous Muslim hacker propelled the jihadists into a 21st-century offensive. He covertly and securely disseminated manuals of weaponry, videos of insurgent feats such as beheadings and other inflammatory material. Irhabi posted a 20-page message titled "Seminar on Hacking Websites," to the Ekhlis forum. It provided detailed information on the art of hacking; listing dozens of vulnerable Web sites to which one could upload shared media. Muntada al-Ansar al-Islami (Islam Supporters Forum) and al-Ekhlis (Sincerity) -- two of the password-protected forums with thousands of members that al-Qaeda had been using for military instructions, propaganda and recruitment. Another fundamentalist hacker was Ibrahim Samudra.
- Ibrahim Samudra organized and financed the atrocious bombing of the Bali resort. During his trial he acknowledged utilizing cyber-crime to finance the attack. Specifically, he hacked credit cards and bank account data from databases of US corporations so as to finance the terrorist attack. While in an Indonesian prison he authored a book depicting the utility of cybercrime in financing global Jihad. The book serves as an instruction manual for those who desire to learn the art of hacking.

Organized Crime: The Internet provides an anonymity and scope that allows cybercriminals to work from anywhere in the world and hide their tracks through a labyrinth of compromised computers. Once the territory of innocuous outcasts seeking bragging rights, cybercrime is now a significant threat with real costs.

Our economy is increasingly reliant on an electronic superhighway containing a number of security holes – where criminals and national enemies possess the ability to turn critical infrastructure against us. Technology is used by the underworld (i.e., both mafia and terrorist organized criminal syndicates) as readily as it is used by professionals and elites. And now, since the end of the Cold War, nation-states no longer have a monopoly over technology, and the playing field has leveled to a point where everyone has access. As a result, not all people using technology are righteous.

There is an entire subculture of highly educated and sophisticated cyber criminals. Much as the Italian Mafia in the U.S. moved into narcotics trafficking in the 1970's, other organized criminal syndicates have realized that identity theft, funds transfer and extortion are the most lucrative business models in the Information Age. The state of play is akin to the Dark Ages. There are a bevy of mercenaries, “hackers for hire” per se, selling their wares online to the highest bidders in Internet chat rooms.

We are also seeing the institutionalization of the hacking phenomenon in certain countries, as well as the realization that the underground economy can feed off the digital e-commerce and e-financial revolution of the late 1990s. The FBI Director, Robert Mueller, declared cybercrime his number-one criminal priority. There are a number of industry estimates which have concluded that there are a large number of compromised computers on the Internet today. According to the Organization for Economic Cooperation and Development, one in three computers is compromised (i.e., remotely controlled by someone other than the intended operator).

It's critically important to understand that threat agents don't necessarily need to know how to hack anymore, much like one doesn't need to know how to build a gun or a tank. It's a question of whether they know how, when and where to use cyber attacks. Today, the Internet has become a huge arms bazaar where anyone can purchase cyber weapons, or download them for free, and use them whenever they choose.

The average cybercriminal is profiting by hacking the average Internet user - 24x7x365, with thousands of new victims per day. One example is the Russian Business Network (RBN). RBN offers a complete infrastructure to achieve malicious activities. It is a cybercrime service provider offering phishing, attack tools and other cybercrime services development (e.g., malware hosting, child pornography, carding and cyber-mercenary services). Some estimate that RBN and its clients were responsible for 60% of cybercrime in 2006⁸. The Internet continues to contain bad neighborhoods, which need to be cleaned. .

While we currently categorize adversaries to include nation-states, terrorists and organized crime, we must consider how cyberspace may allow new coalitions and alliances to form – and ultimately how the United States will maintain network integrity and confidence in the very information upon which we depend. Paradoxically, cyberspace threats range from the human insider to the vendor and supply chain, and ultimately to the remote intrusion – a full spectrum of adversary accesses – each with the potential to devastate the public sector's continuity of operations and the private sector's ability to deliver assured services to the marketplace.

Domestic/Insider: The “insider” falls into the category of the insertion of an operationally introduced vulnerability via a human operation. Normally one thinks of this insider as a person with legitimate access to the system or component. The type of legitimate access and the life-cycle of the component/system are important characteristics of this taxonomy. The person could be a senior manager, software programmer, a secretary, or even a custodian. The person's access could be during the design,

⁸ See http://www.bizeul.org/files/RBN_study.pdf

development, production, testing, packaging, distribution, operation or maintenance of the component.

A classic example of an insider inserting an operationally introduced vulnerability into a target's information technology was the Soviet operation codenamed "Gunman"⁹ and was conducted in the late 70s and early 80s. For this operation, the Soviets designed an implant that was inserted/concealed into IBM Selectric typewriters. The window of opportunity for the insertion occurred while the typewriters were in transit to the US Embassy in Moscow. This was a brilliantly conceived and conducted operation that yielded the Soviets very valuable intelligence for years.

Based upon a "flat world" environment, the life-cycle of US mission critical technology is now routinely offshore. This provides our adversaries greatly increased operational opportunities in exploiting this technology life-line through the use of insiders. While there is a growing understanding and appreciation for this problem, there is not a clear path forwarded in addressing this security challenge.

Motivations and Intentions

Espionage: Computer National Security-Focused Espionage – The collection of vital tactical or strategic information relating to the capabilities, intentions or activities of hostile elements, organizations or persons needed to keep a country or some other organized entity safe or to promote a set of objectives. Recent government system penetrations and large-scale data extractions are most likely the work of foreign nations' intelligence services.

Information Warfare (IW) - Information Operations conducted during a time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (DODD S-3600.1 of 9 Dec 96)[i] The extension of military force into cyber space is becoming more than a concept as several nations begin to organize cyber warfare units and develop capabilities. Modern militaries are dependent on communications and information to operate in accordance with their training. The use of cyber attacks to deny, degrade or manipulate this information could separate winners from losers. In today's interconnected world, the use of force is not limited to military systems. Enemy nations might target civilian infrastructures in order to impact their opponent's military abilities, attack their homelands or disrupt economies. The best military capability in the world has a well exposed "Achilles heel"—the underlying array of computer-based systems that enable virtually all military functions. Even our arsenals of highly lethal weapons systems are increasingly dependent on computers and millions of lines of software for their fundamental operation. The newly-fielded F-22, an airplane capable of delivering

9

James R. Gosler, "The Digital Dimension," in Jennifer E. Sims and Burton Gerber, eds., *Transforming US Intelligence* (Washington, DC: Georgetown University Press, 2005), 96-114.

precision weapons including nuclear bombs, cannot even fly without its computers. This fact was brought home vividly to the F-22's pilots on the aircraft's maiden flight to Japan when the F-22 aircraft had multiple systems failures upon crossing the International Date Line due to a software programming error (Associated Press, 28 February 2007).

Perhaps the most troubling potential exploitation of the cyber threat facing our military is the disruption of military capabilities at the precise time that we are planning to deploy them. A well-placed cyber attack could turn an envisioned "Shock and Awe" attack into fratricide and mass confusion. Targeting coordinates for precision munitions that are changed in random patterns could turn world opinion against the U.S. in a matter of hours.

Moreover, unlike the Greek hero Achilles, our vulnerabilities are not limited to a small area. The systems and software for our military systems are provided by tens of thousands of suppliers from across the globe. Military operations planning, weapons targeting, command and control, as well as support functions such as maintenance and resupply are dependent on computerized systems. These systems are comprised of hundreds of millions of lines of custom and commercially-developed software. It is physically impossible to verify that the software has not been modified to disrupt or deny military US military capabilities.

There have been publically acknowledged attacks on our military capabilities. Analysis of the events referred to as "Moonlight Maze" (CNN.com, 5/10/2001) and "Titan Rain" (Washington Post 8/25/05) showed the signatures of well-organized efforts consistent with those of a nation-state. China has publically acknowledged that cyber attack is a major military strategy (Scientific American, 9/18/2007).

Intellectual Property Theft (State-Sponsored and Corporate)

Intellectual Property Theft and Infringement - the illegal copying, distribution or sale of software, games, movies, music and other intellectual property. This can include plagiarism or theft of products and product plans.

Financial/Economic Benefits—As payment systems move online and credit issuances is granted online, money has become digital. Online bill payment applications were most frequently targeted by cyber thieves according to the FDIC. The Identity Theft Resource Center, put the size of reported privacy losses at more than 127 million records for the year. The data lost or stolen included credit-card information, usernames and passwords, e-mail addresses, and full identity information, such as social-security number, name, address, and date of birth.

Industrial Espionage: Many corporations are targets of industrial espionage. In the 2005 FBI Cybercrime study it was noted that 9 out of 10 businesses were impacted by cybercrime. Many of these attacks were conducted by rival organizations who were attempting to steal intellectual property. Unethical senior managers of rival corporations hire hackers and or hack systems themselves so as to increase competitive advantage and to lower research and development costs.

Mission Destruction: Computer Sabotage - Destruction or disruption of tactical or strategic systems or information via electronic means or by implementation of malicious code.

Ideological/“Political”—Hactivism is a reality of social and political action today. Many groups launch hack attacks for ideological motivation. This has been illustrated by the Palestinian Israel conflict wherein hacking has become a tool of Palestinian and Israelis in order to shut down various websites.

Transiting Through Networks to Attack Others-In 2007- 40% of cyber security incidents originated from third party networks (Ponemon Institute 2007 Survey). Hackers are fully aware that in globalized business world of today that breaching one corporation’s network can allow one to gain access to other proprietary networks which are directly connected. One example was the breach of DHS networks due to a successful cyber intrusion into Unisys last year.

II. Scenarios

A Government Accountability Office report said in September that command-and-control systems that run nearly the entire public infrastructure, including banking and utility systems, face "increasing risks" and "are more vulnerable to cyber attacks than in the past." Cyber intrusions are becoming more sophisticated, more targeted and more prevalent – with the potential to disrupt, degrade or destroy networks or information integral to such critical functions as communications, banking and finance, energy, transportation and human services. U.S. Intelligence confirms that adversaries are actively targeting U.S. Government systems.

A. Financial Sector Threats¹⁰

Over the past few years cyber attacks have grown in complexity and sophistication, and now represent powerful economic weapons that can destroy critical databases and cause serious financial harm in an incredibly short amount of time.

The recent 2007 FDIC Technology Incident Report noted the following troubling trends in the financial sector:

- The number of computer intrusion Suspicious Activity Report (SAR) filings are growing at a fast pace. The estimated mean (average) loss per SAR almost *tripled* the estimated mean loss per SAR identified one year ago.
- Unknown unauthorized access was the most frequently identified type of computer intrusion: meaning the Financial Institutions (FI) could not or did not identify how the intrusion occurred--followed by ID theft/account takeover.
- Online bill payment applications were most frequently targeted by cyber thieves; however, unauthorized access to ACH and wire transfer applications caused the most losses to FIs in the computer intrusion category.
- An increase in websites hosting malicious code was noted by FDIC and anti-virus software vendors.
- Spear phishing (when end users with high computer access levels are targeted) was also sited in several sampled computer intrusion SARs.

The current Financial Sector threat model is overly focused on fraud. The systemic and operational risks (particularly those related to integrity) posed by cyber-related weaknesses are tremendous.

Following are some critical threats to the financial sector:

i. Shared Service Provider Attack

On June 18th, 2001, a computer intrusion into an Internet banking company compromised customer accounts at hundreds of U.S. financial institutions. The attack against S1 Corporation's Community and Regional eFinance Solutions Group gave the hacker

¹⁰ See "Electronic Safety and Soundness: Securing Finance in a New Age". World Bank, 2003.

access to an internal network at the company's Atlanta-based "Data Center," which handles the online banking needs of approximately 300 small banks and federal credit unions across the country. This incident illustrates the systemic risk prevalent in the financial sector, as thousands of domestic financial institutions are dependent upon less than 10 shared service providers' web services and data warehousing. Other critical shared service providers are: *FiServ, Metavante, FDR, and TSYS*.

ii. Integrity Attack on Market Data

Market participants are heavily reliant upon the market data they receive from entities like Bloomberg's and/or Reuters as well as online chat rooms and discussion forums. Hackers have the potential to corrupt the data or insert erroneous data once it leaves the perimeters of financial information disseminators and aggregators such as Bloomberg's and Reuters. The integrity of the data can thus be called into question because it can be digitally manipulated. Since trading positions often are directly related to the interpretation of such data, manipulated data could result in loss of investor confidence or even panic once discovered.

iii. Central Depository Attack

The US Centralized Depository, the DTC, provides clearing and settlement services for equity and debt markets. The DTC provides its services via an online computer system, with participants having direct online access to the system. Transfer of settlement funds occurs through the central bank the same day funds are authorized.

Here is an example of regulation and technology design in supervised arenas not keeping pace with best practice. Since 9-11, a distributed network with significant redundancies is considered best practice. If a consolidated platform is used, these facilities must maintain maximum security – since this is the delta of the settlement and clearance functions. The issues here are design and function, as well as centralizing high value assets. The business continuity movement since 9-11 has opened up once secure dark fiber networks to remote attack. Staged cyber attacks are now feasible against the DTC because of their use of the Internet Protocol (IP) environment. There are therefore significant reputational, operational and systemic risks associated with poor, non-layered security arrangements at the DTC.

iv. Distributed Denial of Service (DDOS) Attack

DDOS attacks could take several forms, such as:

- A hacker could attempt to flood a brokerage company's network (i.e., overwhelm it with vast amounts of data) just before the close of the Market, to prevent it from placing fresh quotes before the end of the day. This could result in penalties and subsequent "reputational risk."
- In a delivery vs. payment scenario, a stock is not transferred to the buyer until payment is received. If payment orders are kept from being delivered, then the stock will not transfer. In a Straight Through Processing (STP), TP, T + 0 environment this scenario carries significantly more risk. This scenario is particularly plausible in the New York Stock Exchange's new wireless trading model. Although the Exchange uses fiber optics as its primary transfer channel, it

has installed a WLAN (wireless local area network) to serve as the redundant backup for those lines in the event of another terrorist strike. Unfortunately, using the WLAN poses a significant vulnerability to the integrity of the stored market data.

- In another example, a hacker could cause a trading system to fail to respond to a time-based transaction(s) or a trade(s). For instance, a system overload/failure could delay the response time and cause a Call Option to be placed after its expiry date. Who is liable for a failed trade in that situation?

v. Currency Trading Scenario

Currency trading is volatile and often dependent on fractions of seconds in trading positions. Suppose that the Euro drops in value relative to the U.S. Dollar effective at 12:00:00 EST on a particular day. The holder of Euros is likely to wish that they had sold Euros before its drop in value. Suppose that the server time tagging the buy/sell orders is being controlled by the reception of GPS positioning and timing signals. A GPS electronic spoofing attack could be launched against the GPS time controlled transaction server. In order to “back-date” the sell order to show that it occurred before the Euro decline, the attacker alters the GPS timing (for example, 11:59:50 EST) thereby causing the system to order the sale and time stamp a time prior to the decline in the Euro’s value. The electronic attacker then turns off the GPS spoofing signal and the GPS timing system once again receives the real GPS signal and returns to the correct time in the server.

vi. ACH/SWIFT/FEDWIRE Attack

U.S. payment systems have migrated to IP-based systems that are susceptible to attack. Past safeguards are now diminished as a result of transactions occurring in real time. Although Straight Through Processing (STP) coupled with XML and T + O appears to provide optimal efficiency, there is no recourse in the settlement window if fraud is committed. Unwinding is impossible in the traditional sense in a T + O environment. Today’s settlement paradigm and its safeguards should be reviewed as the goal to operate in a T + 0 environment redistributes the risk of disputes about settlement to after the fact rather than trying to resolve such prior to settlement.

vii. E-brokerage Compromise

This type of fraud is not new, however the magnitude and speed by it can be committed has grown exponentially in response to the online convergence of networks that were once private. Time is always of the essence to brokers/traders, and competitive positions can be made or lost in seconds. Trading, in particular, is an activity where performance is dependent on being seamlessly connected to the “trading floor” at all times. With the growth in global wireless connectivity, many (if not most) traders and brokers utilize E-PIT (wireless trading on the floor)WIFI or GSM protocols to facilitate remote access. Although this provides real-time access to the trader, it also provides a means for hackers to exploit weaknesses in wireless communication signals to obtain real-time critical intelligence information and/or manipulate trades.

viii. ATM network attacks

On January 25, 2003, the Slammer worm exploited a hole that had been patched 6 months earlier by Microsoft. The worm infected over 75,000 hosts running Microsoft's SQL Server by exploiting a buffer overflow vulnerability and inundated other computers with a copy of itself. Microsoft released a patch for the vulnerability six months prior to the release of the worm. Bank of America's ATMs were unable to dispense cash since they were unable to communicate with the bank's servers. These were taken offline by a worm. The Slammer worm infected 13,000 of Bank of America ATMs. Many reports suggest that Slammer installed a back-door that opened remote access to Bank of America networks. This incident demonstrates the fact that today's ATM networks rely on operating systems that are vulnerable to cyber-attack.

ix. Widespread ID Data Breaches Implication on Credit Issuance

According to the Privacy Rights Clearing House, estimates that since 2005 over 218 millions of data records of U.S. residents have been exposed to theft due to data security breaches. These types of exposures combined with the number of victims of phishing, runs the risk of undermining trust and confidence in the integrity of FICO scores and credit bureau data. The issuance of Credit is the foundation of the American economy and to undermine the integrity of credit scores can and will undermine the US economy. The recent loss of 2 CDs containing records of 25 million people by the UK Tax Authority, also illustrates the nature of this threat.

B. Energy Sector Threats

The reliable supply and delivery of electric power in North America is vital to economic security and quality of life in modern society. Because of the ubiquitous and interconnected nature of the electricity supply and delivery system, absolute protection from malicious acts is both physically and economically infeasible. There is an improbable but credible risk of a debilitating attack on the North American electric grid. Various techniques for reducing the adverse impacts of an attack on the bulk electricity supply and delivery capability are being investigated.

Although the North American electric grid has a good degree of engineered resilience, it remains vulnerable to a myriad of attacks including those targeted against control systems. Current safeguards that reinforce the grid's survivability, such as under-frequency load shedding, islanding schemes and other special protection systems, must be complemented by measures focused on preventing, deterring, detecting and responding to cyber threats.

When one discusses various cyber threats, the most common threats reported seem to be worms, viruses and Denial of Service attacks. While these threats are dangerous they are not equally dangerous to each infrastructure. This is because separate infrastructures can each operate differently from one another. For instance, in the financial and IT sectors, the computer systems and networks comprise the infrastructure. Therefore, any cyber threats that attack the operation of these computer systems (e.g., worms, viruses or DOS) will have a drastic impact on the infrastructure. However, in other critical infrastructures,

the computer systems are auxiliary equipment that is used to control and monitor the actual equipment that comprises the infrastructure. Any cyber threats that attack the operation of these computers may or may not have an impact on the actual operation of the infrastructure depending upon its architecture.

For instance, if a worm was to get into the control system of an electric utility, the most likely impact would be negligible. This is because the infrastructure will likely run quite well based on the previous inputs. The only time a worm could conceivably cause more damage is if the worm attack coincided with a physical event (such as loss of lines due to a storm) then the fact that the computer systems are unavailable or “bogged down” would cause problems that could then lead to a failure. In other infrastructures it would depend on the “failsafe” procedures on whether the worm would have an impact on the infrastructure. For instance, if the infrastructure’s failsafe procedure dictates that the process shuts down when communications are lost with the computer systems, then a DOS against those computer systems could cause the failsafe procedure to execute and the process would shut down. However, if that failsafe procedure does not exist, then the infrastructure would most likely continue operating.

Another aspect of cyber threats against infrastructures is that most individuals believe that the attack is directed at the computers themselves and the loss of those computers would cause harm to the infrastructure. As we discussed above, that is not the case in all infrastructures. Potentially, the most devastating attack is that where the adversary turns the infrastructure control system against the infrastructure itself, causing physical damage to equipment. One fallacy that seems to exist is that it is almost impossible to cause physical damage via cyber means. While that may have been true many years ago, in today’s integrated environment it is much more likely that a clever adversary could cause physical damage. This is because many of the safety systems have become digital and remotely accessible. This means an adversary could modify the safety parameters in such a way to cause harm.

Consider a safety system that is designed to ensure that you perform certain actions in a particular order. In this case, an adversary might attempt to perform those actions in an inappropriate order. For instance, if you have a piece of rotating equipment that must be constantly lubricated, you will usually have a system that ensures this lubrication occurs (e.g., an additional pump). The safety system would be to ensure that this pump is operating every time that the rotating machinery is operating. An adversary might try to cause damage by shutting down (or not starting up) the lubrication pump while running the rotating machinery. This type of thought process applies to many situations that involve safety systems. If the safety systems protect against a situation occurring, the adversary is going to try to make that situation occur.

With today’s heavy reliance on user-friendly Graphical User Interfaces (GUIs), the adversary might not need to be fully versed in the intricacies of the target control system. If the GUI interface has the controls to this lubrication pump readily accessible, all an adversary needs to do is gain access to the control system and then use the interface to impact the device. If there aren’t any integrated safety mechanisms, the odds are that he

would succeed in causing damage. If safety systems do exist, the adversary would need to understand more about the specific control system. The problem is that this is not a difficult task, since more and more of today's industrial control systems are built on common operating systems. In addition, most of these control systems have detailed documentation, and in some cases simulators and test sets, that make it easy for an adversary to become knowledgeable.

The key then to this type of threat is the accessibility of the control system to the outside world. Regrettably, many of the newer components for these systems are coming as fully Internet-capable and utilize standard network protocols and media (e.g., Ethernet, wireless, etc). This dramatically increases the odds of the control system being accessible either directly from the Internet (or the telcom system via dial-up modems) or over the air (wireless). The odds of the control system being indirectly accessible are extremely high, as it is quite common for the control system to be connected to corporate networks that invariably have a connection to the Internet. While an adversary has to find this connectivity and successfully exploit it, anyone with reasonable skills could very well infiltrate this type of critical infrastructure and potentially could cause major damage.

The increasing reliance of the electric power industry on communications and control systems, together with remarkable advances in electronic intrusion technologies and techniques, make the restructured utility industry particularly vulnerable to disruptions resulting from inadequate safeguards and security capabilities. These may include attacks directly on the system, as well as those that use the system or pass through the system.

Following are some critical threats to the electric sector:

i. Attacks Upon the System

The power system is the primary target with ripple effect in terms of outages extending into their customer base. This could be a single component (critical substation breaker) or could have multiple prongs and attack the energy market place itself. Attacks on the system include:

- a. Denial or manipulation of system information necessary for the safe operation of the power grid.
- b. Denial or manipulation of market information to manipulate pricing and market behavior causing rationing of power.
- c. Taking control or sending valid control traffic to open breakers and disrupt power flow.
- d. Disrupting or attacking field devices resulting in system mal-operation
- e. Extortion of a system operator by threat or valid intrusion into electric control systems.

ii. Attacks by the System

The target might be the population at large or customers, and the system is turned into a weapon (e.g., the U.S. transportation system was turned into a weapon on Sept 11th) to cause damage to the target.

- a. Aurora vulnerability: Causing dangerous power conditions that damage connected machines.

Box I: Energy Sector Attack Scenario

Being able to shutdown a portion of the energy sector for a short timeframe might be all that is needed to disrupt the sector. A adversary might also seek a more long-term effect by causing physical damage. The simplest approach for an adversary would be to first understand the safety systems and what events they are designed to prevent, and then develop a means to trigger those events while bypassing the safety system. Shutting off lubrication pumps while rotating equipment is operating maybe enough to cause damage, or shutting down valves could spill hazardous or flammable chemicals that would force the shutdown of that infrastructure while repair/cleanup occurred. The biggest issue is that today's control systems have more remote access than ever before, allowing for powerful modifications to occur. If an adversary can identify an electronic pathway into the control system, then it is likely that he will be able to exploit its vulnerabilities and use it against the infrastructure itself.

iii. Attacks through the System

System assets (e.g., computers, networks, etc.) are leveraged as points of origination or pass-through for normal cyber attacks (e.g., using compromised electric company computers to participate in a DDoS).

- a. Using compromised computers to send spam, participate in DDoS, or use customer billing applications to infect other computers.
- b. Attacking electric control systems to impact interconnected or common gas control systems operated by the same utility.

Aurora Case Study: A critical vulnerability with digital relays was identified by Idaho National Labs who reported it to their sponsors at Homeland Security, Department of Energy, and Defense. This vulnerability could be exploited through remote access points, via network, dial-up, or wireless connectivity depending on architecture. As a result, the Department of Homeland Security established a tiger team consisting of members of government and industry to determine the criticality of the vulnerability, further validate Idaho National Labs findings, and develop a mitigation strategy. Once the validation was completed DHS worked with the Industry, NERC/FERC, NRC, and others to communicate the problem, recommended mitigations, and increased general awareness of the problem.

This specific vulnerability demonstrates that a cyber attack can have physical ramifications and the test validated this by causing significant damage to a 3.4MW Generator, whose configuration was validated by industry officials to mimic how it would be deployed and configured by a utility.

C. Pharmaceutical Sector Threat Scenario

Chemical and pharmaceutical companies consider their products “crown jewels” and closely guard and protect their formulas. These formulations typically involve a tremendous amount of resources in terms of research and development expenditures, testing, and marketing. If they are stored on computers, they are usually highly protected. However, the control systems are often not protected very well. In many instances, the inventory systems that track chemical purchases are accessible. If this inventory system designates what storage tanks the chemicals go to, then an adversary could determine the formulations by gaining access to the control system and reverse-engineering the program (which is not that difficult). Basically, the program for this type of system includes which tanks to mix chemicals from and in what quantities, if heating or cooling is required, and what temperatures the units need to be at and for how long. So knowing which chemicals are in which tanks and then “walking through” the control system program could tell an adversary the formulation. The biggest issue besides the traditional access issue is determining which logical address corresponds to a specific piece of physical equipment (which is true for all of these infrastructures). This can often be found in a computer system in the engineering department (e.g., in a Microsoft Word document or Excel spreadsheet, or even a database). [Note: According to recent DoD attacks, the adversaries downloaded information in the form of Word documents, PowerPoint presentations and Excel spreadsheets.]

Besides determining formulations, an adversary who has gained access to a control system could potentially modify the program. This could result in an adulterated product that severely damages the reputation and bottom line of the company or, in the worst case, results in the death of the products’ users.

III. Vectors

A. Introduction to the Evolution of Attack Vectors

Vectors are the paths that a threat takes to gain access to a resource. Usually the path of attack begins at a point of *exposure* and traverses one or more *vulnerabilities*. Historically, the vectors used by a threat were fairly simple: access was gained via a modem, via a network connection, via an email attachment, or directly from the keyboard. As the threat model changed over the past decade, new vectors emerged. Today's threats gain access via visits to websites, via wireless networks, through embedded software inserted in the supply chain, or via new "converged" technologies such as VoIP. As with all aspects of technology, malware is a rapidly evolving part of the global technology ecosystem. From the early 1980s to 2003, most malware was developed by a niche segment of the ecosystem. It was developed generally as a hobby and, in some extreme examples, as a means to achieve fame or cause significant disruptions in the ecosystem for the sake of disruption itself. 2003 was a landmark year, not only because of the number of computers impacted by malware, but also because it marked a significant change in malware development and deployment trends.

One of the best examples of this sea change is the Zotob virus. Prior to December 2003, most malware was developed to be released weeks or months after a vulnerability was discovered. When Microsoft released a critical security advisor and update for the Windows Plug and Play service, in August 2005, a working exploit was posted on a well known underground web site 3 days later. The Zotob developers used this exploit in their virus and deployed the Zotob virus the following day, which contained a botnet malware payload. Since Zotob, the amount of time between vulnerability announcement and exploit has been continually reduced, and has driven the development of a full-blown underground economy dedicated to the creation, distribution and execution of malware. In fact, it is currently widely accepted among information security professionals that there are vulnerabilities known by the underground, but not known publicly, as they precede any vulnerability announcement.

In addition to this general trend of increasing efficiency in malware development, malware developers are focusing on driving malware to the component level of IT systems. As evidenced by the Broadcom vulnerability announced in 2006 and by subsequent exploits, component-level vulnerabilities provide the opportunity to exploit the vulnerability on any IT system that it contains. For example, the vulnerable Broadcom wireless network chip was built into HP, Dell and Mac computers. The vulnerability was exploitable on all three of those platforms.

Unfortunately, the underground economy has already turned what was the accidental inclusion of vulnerabilities in components into a situation where component factories have been compromised. In these situations, any component manufactured at the facility is compromised from the moment that its production begins. The most significant of

these events was reported in November 2007, when the Seagate¹¹ hard drive factory in Thailand manufactured products with malware already installed – ready for the attacker simply to connect to the system containing the component and execute the exploit.

B. Vulnerabilities

In 2007 the number of vulnerable products was 13,152 and total number of vulnerabilities/exposures was 28645 according to the National Vulnerability database (NVD). On average 14 new vulnerabilities are being reported to the NVD daily. These are the main attack vectors being According to the National Vulnerability Database (NVD) , since 2005 the number exploited for financial gain, espionage, and denial of service attacks.

Typically, once a vulnerability is discovered by a “moral” researcher, the software vendor is given time to fix the bug and issue a patch, so the general public would have an opportunity to patch before the issue is announced. . If a malicious actor wanted to exploit the bug, it could take weeks or months to develop the precise code needed. (Of course, some vulnerabilities were trivial to exploit, such as directory traversal of a web server’s file system or SQL injection attacks.)

Today, the disclosure process has taken a new turn. For instance, some companies offer a significant “bounty” for a reproducible bug in popular software. Likewise, shady criminal organizations offer significantly more for a working exploit against a vulnerability that has not been disclosed, particularly if it permits undetected remote access to large numbers of computers. It is this latter case that has caused a rapid push by cyber criminals in the past two years to acquire “zero day” exploits – tools that take advantage of vulnerabilities in software for which there is no available vendor patch or known workaround. The worst case is when the zero-day exploit is used for criminal or espionage purposes in a manner that is difficult to detect or trace by network defenders. While the number of observed “zero day” events is around 20 to 25 per year, they are especially dangerous since they will be able to compromise systems very rapidly until a vendor releases a patch.

C. Web Application Attacks

Due to the tremendous popularity of the Internet, combined with a general lack of secure coding and the widespread adaptation of website scripting, web applications are increasingly used as vectors by which to attack deep into organizations’ information systems. Below are the OWASP Top Ten Most Critical Web Application Security Vulnerabilities for 2007:

- Cross Site Scripting (XSS)
- Injection Flaws

¹¹ See **Taipei Times** “Bureau Warns of Tainted Disks”, November 11, 2007.

- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forger (CSRF)
- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access

D. Wireless

Wireless computer network access is not new, having its roots in the AlohaNet experiments of the early 1970s. What is new are the standard protocols, widespread coverage, and embedded wireless hardware now common on nearly every new computer system. Wireless is an attractive attack vector due to the relatively easy methods available for sniffing sessions, stealing user credentials, and gaining unauthorized access to private wireless networks. Many private wireless networks are directly connected to internal wired networks, and unfortunately in many cases that connection is behind the firewall protecting the private network from the Internet. Recently new attack methods have targeted wireless hardware drivers, making remote exploitation of a computer system possible as long as the wireless hardware is powered on (no affiliation with an access point is required).

E. Voice over Internet Protocol (VoIP)

Voice over Internet Protocol is gaining widespread popularity due mainly to cost savings (normally no telephone toll charges are levied for a call to or from anywhere in the world), and also because of the flexibility it brings with number portability. Unfortunately, since most VoIP calls are unencrypted and can be intercepted via simple sniffing tools, they can be recorded and played back by an adversary. While VoIP is not a primary attack vector for remote access to a computer network, it does represent a credible problem for capturing confidential information via sniffing or social engineering attacks.

F. Rootkits and Automated Attack Tools

A rootkit is a special type of malicious software (malware) that conceals itself from detection and allows an attacker to gain privileged or root level (system administrator) access to a victim computer. Typically, an attacker installs a rootkit on a computer by exploiting a known vulnerability. Rootkits generally use a variety of techniques to alter a computer's Kernel or User mode software, such as the Task manager or kernel structures/ code. An example would be replacing the original system level code or utilities with malicious code or utilities (i.e. replacing cmd.exe). This process is called "hooking" a system call. These alternations enable the root kit to "hook" or virtually replace any code in the system and remain unnoticed by standard anti-virus programs.

By using stealth technologies, a rootkit has the ability to remain persistently on an infected computer. A rootkit typically contains a number of malicious capabilities, including the ability to install a backdoor for subsequent access to the infected computer, the ability to hide other malware programs, the facility to attack other computers on the same network and the capacity to log keystrokes.

It is significant to note that malware is not the only domain to deploy stealth technologies. Many legitimate software applications contain the technology to protect from unintentional removal or removal without consent. For example, in 2005 Sony's digital rights management software came under fire because it was bundled with stealth technologies to prevent removal of the DRM software, and because it also made computers vulnerable to attack.

Due to their ability to cloak their presence on a computer, rootkits present an especially dangerous and nefarious threat to both private industry and the U.S. Government. Like much malware used today by attackers, many rootkits are shared on the Internet and are the product of online collaboration. This enables attackers to quickly adapt rootkits to avoid detection and add new capabilities. Rootkits, like a lot of malware, can be packaged up to quickly proliferate across a network once it gains control of a computer within a domain.

The cloaking ability of rootkits and the use of stealth technologies by legitimate software makes it difficult to estimate the prevalence of rootkits. According to Microsoft, which runs its Malicious Software Removal Tool on over 350 million unique computers per month, the number of rootkits removed is significantly lower than the removal numbers for backdoors, droppers, viruses, trojans and mass mailers. A number of trends have been recently observed in rootkits, including: spreading beyond trojan viruses to other forms of malware, increased sophistication, attack vectors found in both illegitimate and legitimate software, the increased ease of embedding stealth technologies and the increased number of malicious web sites installing rootkits. Recently, a number of security vendors have released products that specifically identify and remove rootkits. These products continue to evolve to meet the serious threat presented by rootkits.

Automated Attack Tools

An automated attack tool is a program that performs all of the steps needed to attack and compromise a computer, rather than an attacker performing the steps manually. These types of tools automatically scan to identify vulnerable systems, exploit the identified vulnerability to gain access to the system, install a payload, typically malware containing a backdoor and then use the infected system to propagate the attack across a network. This speeds up the attack process and makes it easier for attackers to mount successful attacks. Automated attack tools also have the ability to use a number of attack combinations, in order to identify potential vulnerabilities that can be exploited. These tools enable cyber criminals to quickly adopt new attack methods once a new vulnerability is identified.

Automated attack tools are not solely used by attackers. Like many security tools, automated attack tools can be used for both legitimate and unauthorized activities. Often system administrators will use these tools in order to better understand their own network and system vulnerabilities. For example, the Metasploit project is an online collaborative automated attack tool that is used both by system administrators and attackers. This

tool contains over 200 different exploits for various systems. The challenge is that these automated tools enable attackers to quickly adapt their methods, therefore requiring system administrators to also quickly patch their systems once new vulnerabilities have been identified. The Zotob worm is a good example of this problem. On August 9, 2005, Microsoft released a critical security advisory and update for a vulnerability in the plug and play component of Windows 2000. Four days later, on August 13, 2005, the Zotob worm emerged and began infected unpatched Windows 2000 computers, using an automated process.

The latest trends in automated attack tools are to increase the level of automation and to include the ability to fuzz systems for new vulnerabilities. Due to the increased use of automated attack tools, the vigilance of system administrators to quickly updating systems becomes even more important.

G. Supply Chains

In today's interconnected global community, the world has embraced the Internet as the primary method for voice and data communications. It has enabled global companies to rapidly share data for managing inventory, parts delivery, and "just in time" ordering via electronic data interchange. The Internet has allowed companies to reduce cost through offshoring and reaching many parts of the globe that supplies parts for their products. Today's global corporations have become so dependent on the availability of the Internet that it is essential to them maintaining business continuity. Their ability to deliver services and products therefore depends on the Internet.

If the Internet were to become unavailable, whether regional or globally, there would be significant impacts to the supply chain that public and private sectors depend on for products and services. This is a result of many of the products being built on a global basis. You only have to look at the computer sitting on your desk and the components that make up that computer to realize the dependence on the Internet for goods and services. Your video card might be made in Japan, your hard-drive manufactured in Singapore, and your computer assembled in China before delivery to the United States.

As a result of supply chain globalization, there are many attack vectors in supply chains that an adversary could use for the purposes of espionage, denial of service attacks, and the ability to disrupt products or services necessary for companies to conduct business or a country's ability to respond to a national emergency.

IV. Contributing Factors: Constructs

Externalities are those areas of concern outside of the typical technical and human/social areas that are the normal focus for computer security efforts. Many external factors can bear on the nations's cyber security posture, including globalization, outsourcing, lack of trained expertise due to a general slowdown in the nation's development of science and technology students, lack of proper auditing tools, and a lack of licensing or liability requirements for those who practice information security and software engineering.

A. Globalization/Outsourcing

Globalization and competitive pressures are forcing businesses to outsource information technology (IT) services and functions, as well as many other business processing functions that are IT-enabled. Increasingly, this work, known as ITO/BPO (IT Outsourcing/Business Process Outsourcing), is going offshore. Irrespective of whether the vendor is located in the U.S. or in a developing country, the privacy, security, and cybercrime risk considerations – from both the service provider and client perspectives – are similar. The GAO, for example, noted in a 2005 report that “Concerns that offshoring could pose added risks to the privacy of personal information have led to a variety of proposals to enhance protections.” The Government Accountability Office (GAO), at the request of Congress, investigated several aspects of outsourcing and released a report in September 2006 regarding privacy considerations associated with the domestic and offshore outsourcing of personally identifiable information (PII) in Medicare, Medicaid, and TRICARE transactions. The GAO surveyed 378 federal contractors and all state Medicare agencies and found that 90 percent of them engaged in some outsourcing, and 47-39% of them (varies whether Medicare, Medicaid, TRICARE, or state Medicaid) had experienced a privacy breach within the past two years. In addition, the GAO found that security breach notification procedures differed among the entities. The GAO recommended that the Centers for Medicare and Medicaid Services (CMS) require that all contractors handling PII notify CMS of security breaches. CMS and the U.S. Department of Defense (DoD) concurred with the GAO’s recommendation. In its comments and evaluation of the report, CMS drew attention to a June 9, 2006 memorandum requiring security breach notification and stated that it is developing specific instructions for responding to such notifications. CMS also said it was adding provisions to its vendor contracts that would require written approval from CMS before any work involving PII could be performed offshore.¹² These decisions will impact numerous private sector contractors.

There are, however, additional considerations that must be taken into account if the work is being performed offshore. From the policy and managerial/operational perspectives, outsourcing of information technology and business processes requires companies to ensure that their compliance and governance obligations are being met through their service provider’s operations. For example, all public companies must consider the integrity of their financial information and compliance with Sarbanes-Oxley (SOX), whether their data is maintained and processed internally or by an external provider. Financial institutions must also take into account regulatory guidance on managing outsourcing risks. From the legal side, there is a myriad of considerations regarding privacy and cybercrime laws, cooperation with law enforcement, search and seizure of electronic evidence, evidentiary and jurisdictional issues, and, of course, the underlying Master Service Agreement (MSA) and Service Level Agreements (SLAs). From the technical perspective, it also depends upon establishing effective controls and metrics and

¹² See *Privacy: Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE*, U.S. Government Accountability Office, GAO-06-676, Sept. 2006, <http://www.gao.gov/new.items/d06676.pdf#search=%22gao%20outsourcing%22>.

implementing a thorough incident response program. Effective risk management in the outsourced environment also requires knowledge about best practices, standards, and technical solutions and an understanding of the risks associated with software assurance.

Another notable globalization issue surrounds the lack of manufacturing of critical components within the U.S. For many infrastructures, critical components typically require long lead times of 9-18 months and are very costly. Regrettably many of these components are no longer manufactured in the U.S. That means if an adversary was to preposition themselves in several infrastructure companies and then execute an attack that simultaneously damages equipment, the possibility exist that there would be insufficient spare parts for repairs. This would extend the impact of the outage for a much longer timeframe (for attacks against Finance and IT sectors, recovery is typically discussed in terms of hours) for successful attacks against the equipment in the other infrastructures recovery may be in terms of weeks to months. In addition, since these items are only manufactured overseas, the U.S. might have very little leverage to raise the priority of our orders, which would add additional delay to the recovery.

B. Shift Away from Technical Expertise/Human Capital

A recent report by the National Academies¹³ highlighted that American competitiveness is being threatened now and will continue to be threatened into the future based on, among other things, existing trends in worldwide human capital development in science and engineering. By most current measures of science and engineering capability, the United States enjoys a global leadership position today. However, that position is in serious jeopardy: we are losing ground to industrialized nations around the world.

We face a similar threat in cybersecurity, and the trends are disturbing. Throughout the educational pipeline in recent years, interest in computer science has been waning. For example, at the collegiate level, undergraduate degrees in computer science and computer engineering declined 34% between 2002 and 2006; and at the high school level, the number of students who have taken the AP Computer Science exam has been flat or declining in recent years.

We are seeing related disturbing trends from an international perspective. The ACM (Association for Computing Machinery) hosts an annual international computer programming competition. Talented young students from around the globe compete in the so-called “Battle of the Brains,” a multi-tiered, collegiate competition. To give a sense for the scope of the contest, in 2007 the competition included over 6,000 teams from 1,765 universities representing 82 different countries. The United States used to dominate the competition, but not any more. Here are the winners of the competition since 2000:

- 2007 – Poland (Warsaw University)
- 2006 – Russia (Saratov State University)

¹³ Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future, The National Academies Press, 2007

- 2005 – China (Shanghai Jiatong University)
- 2004 – Russia (St. Petersburg Institute of Fine Mechanics and Optics)
- 2003 – Poland (Warsaw University)
- 2002 – China (Shanghai Jiatong University)
- 2001 – Russia (St. Petersburg State University)
- 2000 – Russia (St. Petersburg State University)

Extremely talented U.S. student teams from some of the top U.S. universities have participated in the competition, but the U.S. teams have simply not fared well in recent years. The last time a U.S. school won the competition was in 1997.

So who will be the future workforce to defend U.S. critical infrastructure and information from the adversaries around the globe described earlier in this paper? The trends suggest that we have much work to do and that we must act quickly and with urgency. What is needed for all of the infrastructures are personnel who are very well versed in control systems and cybersecurity. The problem is that this is currently a very small, shallow pool of candidates and therefore the infrastructures are all fighting for this small group of people. We need to drastically increase the number of personnel in these disciplines in order to ensure that infrastructure modifications will be developed with security as an integral part of the system, rather than as an add-on after the fact.

C. Lack of Certification/Liability and Training

Software engineering and information security continue to be two of the most critical career fields for the new information age, yet both professions lack any formal requirements for licensing, liability or training. For example, the medical, legal, engineering, real estate, financial planning, and truck driving professions all require a license to work in those fields. Practicing without a license can send a person to jail or, at a minimum, subject them to fines and penalties. Likewise, these professions all carry some form of legal liability should one not follow practices and standards agreed to by the profession. The lack of licensing and liability in the software engineering and information security professions are an externality that puts our nation at extreme risk of cyber attacks.

Software engineering and information security continue to be two of the most critical career fields for the new information age, yet both professions lack widely accepted training and education concerning secure coding and proper systems configuration. Today, secure development training is not required by most academic institutions, training institutes or certification programs. This lack of training is an externality that puts our nation's ability to secure its critical information systems at risk. Establishing secure development training programs as an essential skill set to be learned by new software engineers and information security professionals, is an important step to increasing the security of our nation.

D. Risk Management

For too long, technology risk has been considered independent of operational and reputational risk management. In 2006, the Congressional Research Service estimated that NYSE Company suffered shareholder losses of \$50-\$200 million (approximately a 10% devaluation) following a cybersecurity event. Risk managers have not been sufficiently trained to manage and mitigate the risks associated with IP based systems. This reality is a consequence of insufficient governance of information technology assets within corporations and organizations. Governance, compliance and operational (legal) risks of cyber crimes within publicly traded companies include multiple and interrelated vulnerabilities that are interconnected with a corporation's global business model. Vulnerabilities include lacks of accountability, independent risk verification and metrics at the Board of Director level to identify negligence and breach of fiduciary obligations for safeguarding assets due to ...

- (1) self-assessment by management of internal controls on safeguarding of information assets (COSO) and related risk frameworks (e.g., Sarbanes-Oxley 404, FDICIA, GLBA, FTC ACT, Basel, Camels);
- (2) a lack of verification, effective metrics and accountability on compliance with laws and regulations in (1); and
- (3) Board approval of faulty risk management frameworks for GLBA and Basel. Non-compliance with laws and regulations in (1) represent violations of safe and sound banking practices required for maintaining federal deposit insurance.

Failure to safeguard assets is a central operational risk that radiates out with multiple interconnections in a corporation's global business model. COSO's integrated framework identified three interrelated risks in 1992 for internal controls: effectiveness and efficiency of operations, compliance with laws and regulations, and reliability of financial reporting. Strong, effective internal controls are designed per COSO, Sarbanes-Oxley 404 and the newly proposed FDICIA to safeguard assets against unauthorized acquisition, use or disposition as part of a process, effected by an entity's board of directors, management and other personnel, to provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the entity's assets that could have a material effect on the financial statements. Failure to safeguard information assets, in this digital world, with strong information security governance internal controls per COSO's three-faceted model create operational (legal) risks that include loss of federal deposit insurance, litigation by shareholders and/or consumers for negligence, breach of fiduciary duties, and breach of contract. Loss of federal deposit insurance and/or settlements, such as in the TJX case, poses significant harm to business and the economy.

Ultimately, Boards of Directors are accountable and need to step forward and verify and manage their operational risk profile in this digital age and interconnected global economy.

Conclusion

While the nature of cyber attacks may differ in terms of targeting, tactics and results, the one constant in our threat assessment is the “human factor.” Ultimately, cyberspace provides for more agility and easier access to affect the desired outcome of those who intend harm (in whatever form it may take). As society becomes more dependent on technology, every aspect of human convenience and international markets will depend on cyberspace and all that goes with it. As the seeds of a virtual epidemic spread into the smallest crevice of our networks, the solution space must consider risk management and living with the infections that come with global interconnectivity. Unfortunately, on average, organizations are spending less than 6% of their overall information security budgets on security, and consequently neither public nor private sector defenses are adequate.

Appendix I: Relevant Definitions

Asset

Anything of value (e.g., people, information, hardware, software, facilities, reputation, activities or operations). Assets are what an organization needs to get the job done—to carry out the mission.

Attack Profile

A characterization of all attack goals that an adversary has for a system.

Broad Attack Types

Critical Infrastructure

Those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matter (USA Patriot Act, 2001).

Groups & Causes

Organized bands or individuals, who espouse a particular criminal, political, religious or other cause, that attack publicly accessible web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into websites to send their espoused ideological or political message

Incident Analysis

A retrospective analysis of incidents at a particular site, among assets within a particular site, or assets with a category in a particular area, which indicates patterns of potential adversary activities or intentions. Incident analyses should include an assessment of countermeasures sufficiency based on the ability to asses and respond to the suspicious activity in such a way as to have reduced the likelihood of success if it had been an actual incident.

Intrusion

Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource [ii].

Malicious Code

Hardware, software or firmware that is intentionally included in a system for an unauthorized purpose (e.g., viruses, Trojan horses, worms) [iii].

Risk Management

A continuous systematic and analytical process made up of several phases by which an organization identifies, reduces and controls its potential risks and losses.

Risk Perception

The manner and extent to which a decision-maker comprehends risk.

Residual Risk

The amount of risk remaining after the net effect of risk reducing actions

Risk Tolerance

The degree of risk associated with normal activities that people tolerate, usually without making a conscious decision.

Threat

The capability and intention of an adversary to undertake actions detrimental to an organization's interests. Threat is a function of the adversary only; it cannot typically be controlled by the owner or user of the asset. However, the adversary's intention to exploit his capability may be encouraged by a vulnerability, with levels driven by the inherent or perceived qualities of the asset or discouraged by an owner's countermeasures.

Vulnerability

A flaw or weakness in the design or implementation of hardware, software, networks, or computer-based systems including security procedures and controls associated with the systems (U.S. Strategy to Secure Cyber Space).