Cyber Security Threat Statement

June 6, 2007

1.0 INTRODUCTION 2
1.1 Purpose 2
1.2 Background 3
1.3 Office of Science Environment 3
2.0 TYPES OF THREATS 5
2.1 Environmental Threats 5
2.2 Natural Disasters 6
2.3 Human Threats 6
3.0 HUMAN THREATS UNIQUE TO SCIENCE 8
3.1 General Description of Attackers 8
3.1.1 Nation States – Foreign Intelligence Services 9
3.1.2 Foreign National Visitors – short term 9
3.1.3 Foreign National Visitors – long term 9
3.1.4 Arrogant User 10
3.1.5 Remote User – CONUS 10
3.1.6 Remote User – OCONUS 10
3.2 Specific Vulnerabilities 11
3.2.1 Failure to Patch Workstations and Laptops 11
3.2.2 Voice Over IP (VOIP) and Peer to Peer (P2P) Networking 11
3.2.3 Grid Computing 12
3.2.4 Mobile Devices – Laptops/PDA/Cell Phone 12
3.2.5 Loss of PII 13
3.2.6 Extensive Use of System Administrator Rights 13
3.2.7 Legacy Systems 13
3.2.8 Rootkits 14
3.2.9 Social Engineering 14

1.0 INTRODUCTION

The Department of Energy (DOE) Office of the Chief Information Officer (OCIO) recently released an updated Threat Statement (4-09-07) describing the actors (those entities that seek to harm the agency), vulnerabilities in the DOE infrastructure that can be targeted, and an assessment matrix describing the probabilities that a specific actor would target a specific vulnerability. The OCIO document, while explaining the overall threat landscape of actors and vulnerabilities does not address specific threats to Office of Science (SC) missions which constantly balance information security concerns with open collaboration research needs. This Cyber Security Threat and Vulnerability Assessment document has been developed to address this gap.

SC is the single largest Federal government supporter of basic research in the physical sciences in the United States, providing more than 40 percent of total Federal funding for this vital area of National importance. It oversees, and is the principal Federal funding agency of, the Nation's research programs in high-energy physics, nuclear physics, and fusion energy sciences. Such a diverse research portfolio supports tens of thousands of principal investigators, post-doctoral students, and graduate students who are tackling some of the most challenging scientific questions of our era.[1] Tom Malec, Director – Information & Special Technologies Program for DOE stated that "[the] DOE unclassified network infrastructure is a potentially lucrative target for foreign collection because of its vast holding of information essential to the competitiveness of critical segments of the US economy."

The threat to the SC information systems and data is significant and growing, as in all organizations. This document discusses the common threats and vulnerabilities across the SC's Laboratories and Site Offices. Cyber resources and its supporting infrastructure are the primary focus of the documents, moreover since most cyber assets rely on a secure physical infrastructure; this report includes environmental, natural, and human threats.

1.1 PURPOSE

This document identifies the threats, foreign and domestic, to the SC Laboratories and Site Offices information and information systems. As discussed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems, and other related documents, the following definitions apply:

- Threat: Any individual, organization, or activity that potentially could damage the confidentiality, integrity, or availability of information or information systems.
- Vulnerability: Any flaw or weakness in people, processes, technology, system security procedures, design, implementation or internal controls that could be exploited and result in a security breach or violation of the system's security policy.
- Risk: The net impact on mission, considering the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system's susceptibilities and the resulting impact if this should occur.

[1] http://www.energy.gov/sciencetech/index.htm "about Science and Technology"

Information technology-related risks arise from legal liability or mission loss due to:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information;
- Unintentional errors and omissions;
- IT disruptions from natural phenomena or human disasters; and,
- Lack of care and diligence in implementing and operating the IT system.

1.2 BACKGROUND

Information systems and the supporting infrastructure are attractive targets for malicious individuals and organizations. SC constitutes a very attractive "target of opportunity" for exploitation because:

- The interconnected network can provide pathways among systems to gain unauthorized access to DOE (SC) data and operations from external locations.
- Feature-rich, commercial software products are enormously complex and replete with flaws and vulnerabilities requiring frequent corrective patches.
- Sophisticated tools for knowledge management, data mining, and analysis offer trusted insiders the ability to misuse significant amounts of information (facilitates aggregation).
- The infrastructure of high bandwidth telecommunications provides a powerful tool for international and domestic organizations seeking to identify potential targets. The science networks that facilitate the transfer of peta-bytes of information if compromised may be used to initiate Denial of Service (DOS) attacks on other sector specific assets (e.g. banking or healthcare).

1.3 OFFICE OF SCIENCE ENVIRONMENT

Ten SC Laboratories are situated in a campus environment. There are generally two main roads onto the campus which are protected by guards in a gatehouse. The guards check badge identification or a pre-screened list of visitors for the day before allowing vehicles to pass through the gate. SC Site Offices are located on these campus environments either in a dedicated building or a shared facility. Some SC Laboratories have no gatehouse as they are situated within an "office park." These Laboratories have guards at the main entrance. Two facilities (ORO and SC-HQ) have physically restricted facilities.

International cooperation and openness in nuclear sciences as high-energy physics, particle physics, and high performance computing have drawn DOE Laboratories into an interconnectedness that facilitates research but at the same time presents unique security challenges. Following are some of the communications systems at many of the SC Laboratories.[2]

[2] Threat Statement – DOE Unclassified Information Systems – June 21, 2005

- The InterAction Collaboration: The interaction collaboration organized in December 2001 is a worldwide collaborative endeavor for the advancement of particle physics. Experiments at the world's accelerator laboratories are carried out primary through CERN[3] . SC participants include Argonne, Brookhaven, Fermi, Lawrence Berkeley and Thomas Jefferson Laboratories.
- ESnet: ESnet is an unclassified backbone network that provides network and Grid services to support international collaboration. ESnet connects SC Laboratories to major universities and other scientific institutions. ESnet does not assume or accept responsibility for site security, privacy or data integrity across the network.
- TeraGrid: TeraGrid is a multi-year effort to build the world largest distributed infrastructure of open science research. TeraGrid is expected to connect to ESnet. Argonne and Oak Ridge Laboratories are TeraGrid sites.
- GLORIAD: the Global Ring Network for Advanced Application Development (initiated in 2004) is a secure high speed network linking scientists in the United States, Russia and China. The US node is located at the StarLight facility in Chicago.

These networks present a unique threat to SC because while we are interconnected, SC does not control access nor are these networks centrally managed. It is also reasonable to conclude that NIST controls are not applied to these networks because these multi-national networks are not covered by Federal Information Security Management Act (FISMA).

Locally each Laboratory has a number of local networks/servers to support mission requirements and run the business of the Laboratories. Many sites have taken the initiative to segment the business systems from the rest of the infrastructure and implement moderate controls for the protection of these systems and their information. Many sites also have legacy devices (workstations, servers, etc) that run custom applications needed for scientific research. Sites that provide wireless access to visitors have this capability outside of the wired infrastructure. Wireless access at these facilities requires registration and "acceptance" of privacy and code of conduct restrictions.

[3] CERN is the European Organization for Nuclear Research.

2.0 TYPES OF THREATS

This document describes environmental, natural, and human threats. These include:

- Environmental threats such as fires, air conditioning- and power-outages, and other events, like biological-, chemical-, or nuclear-attacks that may limit access to facilities and/or the information systems they hold.
- Natural threats or phenomena, i.e., weather-related events, such as flooding, severe storms, and earthquakes.
- Human threats are generally separated into two main categories; intentional and unintentional. The former cover individuals or groups who actively attack an organization to cause disruption, obtain information, or deny access to others. Unintentional threats result from authorized individuals gaining accidental access to, or distributing information from other systems.

This document discusses the environmental, natural and human threat categories. Environmental and natural threats are discussed only as they pertain to compromise or destruction of the physical environment of the information and information systems. The reader is directed to review the Safeguard and Security Threat Statement for full discussion of physical threats.

2.1 Environmental Threats

Environmental threats are frequently related to physical security because their occurrence often denies access to or degrades the functionality of the facility. These threats range from loss of air conditioning or electrical power to a Hazardous Material (HAZMAT) incident that may render the facility unusable for a considerable time. Environmental threats range in impact from very low (e.g., limited power failure) to very high (e.g., destruction or contamination of a building). The likelihood of most of these incidents is often relatively low due to the controls already in place. For example, most large laboratories have a fire station on site; laboratories within office parks rely on the capabilities of the municipality. Most buildings have fire-alarm systems that notify the fire department if a fire is sensed. Many also have sprinkler systems to further reduce a fire's impact. Newer buildings are constructed with fire retardant materials.

Environmental threats are often a general threat to the facility as opposed to an IT threat *per se*. For example, a fire may result in damage to an entire building or it may only damage a data center. Environmental threats are primarily the responsibility of the Safeguards and Security Office, except where they may have a direct IT impact. In most cases, the site office piggybacks on the capabilities of the National Laboratory.

Some potential areas that will be assessed under environmental threats include the following:

a. Transportation Infrastructure – Generally the Laboratories are reliant upon the transportation infrastructure to carry supplies, vendors and workers. Some of these supplies are explosive or hazardous materials. An accident involving these vehicles could have a major impact if the incident happened close to the site.
b. Fire (electrical origin) – The primary threat to the information and information systems from fire would be in the data centers. Alarms and automated fire suppression systems are located in all data centers to reduce this threat.

c. Heating, Ventilation Air-Conditioning (HVAC) failure – Cooling and humidification of the data centers is critical in environments where computing devices are closely mounted to conserve space and maximize computing resource availability.
d. Power outage/failure – Computers rely upon clean power for sustained operations. Sudden power disruption could cause system to fail in an unsecured mode or lose data.
e. Loss of water – Loss of water or low water situations can result in cooling failures, which could affect the accelerators, or some of the high speed processors that rely on water cooling for heat dissipation.

2.2 NATURAL DISASTERS

Threats in this category are natural events or phenomena that can destroy, interrupt, or alter the normal functioning of the facilities, personnel, or equipment devoted to the information system. They usually are associated with, but not limited to, fire, windstorm, lightning, flood, tornado, earthquake, or snow and ice storms. The threat posed by these events must be considered in combination with their corresponding effects. Examples include the evacuation and loss of access to a facility, or inaccessibility by personnel because of hazardous conditions.

An often-overlooked source of threats to technology controlling or processing information is the physical features of a building or facility. Potential vulnerabilities can be associated with interrupted, damaged or inadequately secured water mains, tunnels, passageways, windows, and insubstantial walls.

Some potential natural threats that were considered include the following:

a. Earthquake
b. Floods (flash or tsunami)
c. Extreme temperatures
d. Hurricanes or tornadoes
e. Drought
f. Lightning
g. Wildfires
h. Severe storms

After careful consideration it was determined that the Natural Threats are a threat to the entire facility as opposed to a cyber threat. Natural Threats, except where they may directly impact on information systems, are primarily the responsibility of the Safeguards and Security Office and will not be further considered in this threat analysis. It should be noted that hurricane / tornado season appears to be starting earlier in the year and the severity of these storms has increased in recent years Katrina (New Orleans, LA.), Rita (Sabine Pass, TX), Wilma (Cape Romano, FL) and most recently the tornado that leveled Greensburg Kansas on May 7, 2007, prove that entire cities – not just campuses can be crippled in minutes, therefore contingency plans, and offsite storage plans should be reviewed with an eye to increasing the physical separation distance.

2.3 HUMAN THREATS

Individuals may focus on an organization's physical or information infrastructure when seeking to disrupt, destroy or acquire information. People inside an organization, pose a threat to the SC mission due to carelessness or ignorance, "serendipitous opportunity" in which they believe they

can gain financial benefit for the information they have or because they specifically try (with the concurrence of their government) to exploit their relationship with the scientific community.

Physical security includes security guards, cameras in data centers, locking mechanisms that provide access controls to sensitive locations, and keycards or keys on doors all help prevent the compromise of a trusted device. Multiple levels of physical security is important and can help prevent some of the more serious breaches of facility security and associated high-visibility actions, such as bombings, shootings, and other acts of violence. In addition, threats to human life and cyber systems from disgruntled employees must be taken into account.

Human cyber threats include items such as viruses, worms, Trojan horses, logic bombs, and other types of code written to destroy or limit access to information and information systems. Intentional cyber threats also covers spoofing, masquerading, phishing (sending email purportedly from a legitimate enterprise to gain personal data), social engineering (manipulating people to disclose authentication information), and other activities to gain access to information that the perpetrator does not have official approval to view. A joint survey by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) indicates the top four security incidents were 1) virus contamination, 2) unauthorized access to information, 3) theft or loss of laptops or mobile devices, and 4) theft of proprietary information[4]. These intentional activities are usually initiated to either provide or deny overt access to information and information systems. Unintentional threats usually occur because management has not implemented appropriate controls to prevent the prohibited activity, as follows:

- Failing to segment networks and servers to limit the accounts that have access to specific information.
- Allowing personnel to retain access to IT systems access after they have moved to a new group and no longer require access.
- Allowing personnel to install non-standard tools and applications from on their workstations.
- Failing to address/raise awareness of social-engineering vulnerabilities.
- Failing to adequately train personnel on maintaining equipment properly.

Unintentional human threats can be a significant risk to information as individuals have access to powerful tools that can have devastating impact if the user does not understand the impact of their actions. This area includes the impact of launching an unintentional malware attack by opening a SPAM email or any other infected media on a DOE computer.

[4] CSI/FBI Computer Crime and Security Survey -2006 by Gordon, Loeb, Lucyshyn, and Richardson.

3.0 HUMAN THREATS UNIQUE TO SCIENCE

The SC Workforce Development for Teachers and Scientists Program continues the Department's long-standing role of training young scientists, engineers and technicians in the scientifically and technically advanced environment of our National Laboratories. The Program supports three science, technology and workforce development subprograms: 1) Undergraduate Internships, for undergraduate students wishing to enter science, technology, engineering and mathematics (STEM), as well as with science and math teaching careers; 2) Graduate/Faculty Fellowships for STEM teachers and faculty; and 3) Pre-College Activities for middle and high school students such as the National Science Bowl. Each of the subprograms target a different group of students and teachers to attract as broad a range of participants to the programs and to expand the pipeline of students who can enter the STEM workforce. In this fashion, the subprograms use our National Laboratories to meet the demand for a well-trained scientific and technical workforce, including those teachers that help spawn that workforce[5].

According to an Open Doors survey for the 2005-2006 academic year, new foreign students at American colleges and universities have increased 8 percent to a record 143,000 students, with the largest numbers coming from India, China, Korea, Taiwan and Mexico.[6] Therefore it is fairly certain that the workforce development program described above reaches out to a significant number of foreign nationals, at the undergrad, graduate and faculty levels.

In addition to the workforce program, SC reaches out to foreign nationals in a physical and cyber sense. SC sponsored over 25,000 visits to the Laboratories in 2004, and of this, over 17,500 were for assignments longer than 30 days[7]. This "on site presence" is in addition to all the worldwide scientists who access grid computing or other experiments remotely. No other sub-element within DOE has as diverse a workforce as SC.

3.1 GENERAL DESCRIPTION OF ACTORS

According to the annual report on Foreign Economic Collection and Industrial Espionage, 108 foreign countries (or their citizens) were involved in collection efforts against sensitive and protected US technologies in FY 2005.[8] As usual the cheapest, easiest and least risky methods for acquiring sensitive information were the most commonly used. These techniques included:

- Making direct request for classified, sensitive or export controlled information.
- Offering technical services to cleared contractors in the hopes of getting access to protected technology or information
- Using cyber tools to collect information

[5] http://www.energy.gov/sciencetech/workforcedev.htm
[6] Publicdiplomacy.org – updated January 2007. USIA Alumni Association
[7] Statement by Dr. Raymond L. Orbach Director, Office of Science U.S. Department of Energy The Impact of U.S. Visa Policy on the Department of Energy Office of Science Missions Senate Foreign Relations Committee Roundtable Discussion April 4, 2005
[8] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – August 2006

- Exploiting foreign visits to government sites or conventions to perform social engineering attacks.
- Use of cell phone cameras or Personal Digital Assistants (PDA) technology with significant storage capability to steal information.

The "profile" of the foreign government agent most used include students, professors, and researchers. These individuals may not have originally intended to acquire information, but found themselves in a position to acquire information after the visit started and decided to exploit the situation. This general description of the profile and techniques used closely mirrors the scientific community at the Laboratories and Site Offices.

Following is a list of the human threats that are most likely to cause harm to SC.

3.1.1 Nation States – Foreign Intelligence Services

Foreign Intelligence Services (FIS) use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively developing information warfare doctrine, programs, and capabilities. Such abilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power, with consequences that could affect the daily lives of U.S. citizens.

FIS are more likely interested in the acquisition of information than in its destruction or modification. As advanced countries like the United States outsource their programming to less expense middle and Far East countries the risk of rogue programmers using their access to commit cyber crime increases.

3.1.2 Foreign National Visitors – short term

SC granted approximately 7,500 short term visits to foreign nationals in 2004. These visits are for less than 30 days and usually center on a symposium or a convention. Visitors to Laboratories for these events usually arrive with cell phones, laptops, physically small storage devices, and PDAs. As a courtesy, internet access is provided at many sites. While on the facility foreign nationals are usually restricted to "public access" space, but can be taken on "private tours" of the facilities by the host sponsors or assigned Laboratory personnel. These visits are prime opportunities for social engineering attacks or to provide surveillance of the faculties to determine the best methods of compromise.

3.1.3 Foreign National Visitors – long term

In addition to the authorities and privileges granted short term foreign national visitors, they may also be furnished with a workstation, but they may also request that their laptop be connected to the network. As in the short term assignment, these visits provide opportunities for social engineering attacks with the added benefit that as an "insider," there is more opportunity for social interaction with more people. Furthermore individuals on long term assignments receive access badges to the facilities so their movements are not monitored closely, and they may have access to at one or more of the internal networks on the facility so the opportunity to acquire information is much higher.

3.1.4 Arrogant User

Unfortunately almost anyone can become an arrogant user. These are personnel that have received security awareness training but have decided that the "rules" simple do not apply to them. Actions of these individuals include, establishing rogue wireless access points within the facility, performing actions at higher privilege levels than what is required for the job, writing passwords down in easily accessible places, not updating virus or spam tools regularly, or failure to install encryption software or other information protection software on portable devices.

The arrogant user can be a user, a system administrator or a domain administrator. Obviously the more privileges the individual has the higher the degree of risk. Another characteristic of the arrogant user is the perception that limitation of user rights is a demotion of stature within the community and sometimes individuals that have privileges reduced become insolent to the cyber controls of the organization which in turn increases the vulnerability of the site.

3.1.5 Remote User – CONUS

Domestic users that have a need to remotely access computers in the science complex are provided an RSA token. The RSA tokens provide one time passwords and are considered a strong authentication mechanism. Remote users may be given science or university affiliate e-mail accounts to facilitate their communication with other researchers at the facility or as "proof" to others of the individual's affiliation with the Science Laboratory or university. However personnel who receive tokens to conduct research often do not return these tokens when the research or the contracted period ends. Furthermore since the period of engagement is "open ended" inactivity of a specific account is not often used as the criteria for termination of access.

Students (workforce development project) have unfortunately been caught sharing SC passwords with other students not affiliated with the program so these people can have access to SC resources, such as better internet access or perhaps to partake in Peer to Peer computing activities sponsored by the site.

3.1.6 Remote User – OCONUS

The Open Science Grid (OSG) is built and operated by a unique partnership of universities, National Laboratories, scientific collaborations and software developers that work together to create a common distributed computing environment, or grid, for scientific research. Computing resources from more than 50 sites in the United States, Asia and South America are shared through the OSG. These resources range from small clusters of ten computers to large facilities with thousands of processors and millions of gigabytes of data storage. Therefore the international researcher is the last bastion of quasi-anonymous access. Researchers who have no need to visit SC sites are "vetted" though their local government or academic institution as having a need to access the OSG. The scientific community imposes self monitoring and peer pressure to assure that access is granted to authenticated individuals – however there is no central authentication server or standardization of tokens, biometric, or other access controls to assure the identity of the individuals on the grid so the opportunities for unauthorized monitoring or simply using the infrastructure to attempt to gain unauthorized access to the grid supporting sites.

3.2 SPECIFIC VULNERABILITIES

There are a number of areas of concern when assessing the vulnerabilities to any organization. The list below reflects vulnerabilities that are of specific concern to SC.

3.2.1 Failure to Patch workstations and laptops

A recent study indicated that 80 percent of successful cyber attacks are the result of workstations, servers, laptops not being at the proper patch level for the operating system or applications installed[9]. Furthermore, the most prevalent critical vulnerabilities are replaced by new vulnerabilities each year. SC is making a concerted effort to enforce patch management on all government furnished equipment; however there are many devices which for "experiment baseline control" purposes are not routinely updated. These devices represent a known vulnerability to the infrastructure of the facilities where they reside. Additionally, many researches take their government or personal laptops on travel, and while there is a policy to have these devices scanned before and after the foreign visit, it is not practical to do so in all cases due to the sheer number of foreign trips taken by the Science population. These un-patched laptops represent another risk to the infrastructure when they are reconnected to the network after the trip is concluded. Laptops may also have been compromised as a result of connection to networks outside the science infrastructure.

3.2.2 Voice over IP (VOIP) and Peer to Peer (P2P) networking

SC uses VOIP and P2P networking on many of the systems that are part of the OSG. A major VOIP application is SKYPE communication which uses the internet to make long distance phone calls. Peer to Peer networking is integral to the scientific community for sharing of information – the predominate application being BitTorrent. BitTorrent is a method of distributing large amounts of data widely without the original distributor incurring the entire costs of hardware, hosting and bandwidth resources. Instead, when data is distributed using the BitTorrent protocol, recipients each supply data to newer recipients, reducing the cost and burden on any given individual source, providing redundancy against system problems, and reducing dependence upon the original distributor.

However there are vulnerabilities in the H.232 protocol (VOIP protocol), especially in the Cisco product line. The vulnerability could allow a remote user to obtain unauthorized administrative control of the router and then cause a denial of service. This vulnerability also allows an attacker to initiate a router shut down or restart. Peer to Peer communication while not specifically vulnerable has a poor connotation because this technology has been instrumental in the extensive abuse of copyright laws (e.g. Napster, Limewire, Shareaza, etc.). Indiscriminate use of P2P may cause scientific information to traverse unsecured pathways where it may be acquired by others outside the scientific community. SC needs to monitor the P2P servers to assure that only scientific file and data are being transmitted.

[9] The laws of Vulnerabilities – six axioms for understanding risk – Qualys, Inc. 2006

3.2.3 Grid Computing

Because grid networks are composed of loosely coupled, heterogeneous resources managed by different administrators, they are far more vulnerable than single administrator networks. Therefore, grid infrastructures are easy targets for cyber-terrorists. The grid, if commandeered by a nation state, has the bandwidth to disrupt the banking infrastructure, health networks, or even basic communications – if the processors of the grid are turned to denial of service attacks. Recently (May 22, 2007) Estonia, a former Soviet territory, was under heavy cyber attack which resulted in the shutdown of their banking infrastructure. "*These attacks were massive, well targeted and well organized," Estonian defense minister Jaak Aaviksoo said, adding that" they can't be viewed as the spontaneous response of public discontent with the actions of the Estonian authorities. Rather, we have to speak of organized attacks on basic modern infrastructures."*

3.2.4 Mobile Devices – Laptops/PDA/ Cell Phone

We have an era in communication in which an individual can always be in "touch" with everyone. The typical government researcher is usually issued a Blackberry or other PDA and a cell phone. In addition, taking a "laptop on the road" has become a standard accessory in the workforce. There are three specific vulnerabilities with using these devices that specifically apply to SC because of visits to foreign countries, and attendance at workshops, conventions, or seminars.

1. USE - People using cell phones are often not the most discrete in their choice of subjects of conversation or the volume at which the conversation is maintained. Specific information may be obtained simply by standing in "hearing" range. In random walks through multiple science facilities, conversations that contained financial information, contract information, meeting times and places, etc. were overhead. People using laptops in public places, (on the plane) were not aware that much of the information on the screen could be read.
2. LOSS – Unfortunately all mobile devices may be lost at some point. PDAs contain e-mail lists, phone lists, calendar appointments, and possibly documents. Cell phones may contain pictures (mostly personal but perhaps some business related), phone lists, text messages, etc, and laptops most likely contain specific research or business related information. Loss of the device places all the people on these lists at risk because the "finding" person may decide to impersonate the owner. Loss of a laptop may seriously delay the specific project the individual was supporting
3. THEFT or EXPLOITATION – While the loss of a device is annoying and potentially harmful, the theft of a device most certainly raises the harm that may be sustained by the organization or the individual from the theft. Theft of mobile devices occurs because the owner was specifically targeted, or simply because there was an opportunity for the device to be stolen (left in the hotel). Exploitation of a device occurs when the object is to insert a virus, Trojan or worm, in the hope that this code will help compromise the home infrastructure when the traveler returns.

Government and business travelers often report that their belongings have been searched while they were absent from their hotel room. In some cases, they have returned to their room soon

after departing, to retrieve a forgotten item, and find persons in their room claiming they are there to repair a broken TV, etc. Seldom is anything missing; the purpose is only to copy documents or download information from a traveler's laptop computer. Sometimes there is little effort to conceal the search. Other times it is more subtle. If done correctly, the traveler will not be aware of the search.[10]

3.2.5 Loss of Personally Identifiable Information (PII)

SC is a collection of scientists that work collaboratively and share information extensively. Most researchers have several resumes, biographical summaries, or other information about them and their peers which are freely shared. While many of these documents do not contain PII, some do. Furthermore, e-mail or phone lists which contain home, work, and mobile phone numbers is considered PII. Research heads may have spreadsheets which contain the social security or employee numbers of the people they manage or perhaps the name and addresses of employee family members. When these mobile devices are lost or stolen, PII information can be compromised.

3.2.6 Extensive use of System Administrator Rights

No other organization within DOE has as many people with administrative privilege to the workstations and laptops provided by the government or supporting contractors. Users should have only those rights that are required for the normal accomplishment of their responsibilities. Infrequent or one time needs should not be used to justify the assignment of excessive rights. Administrative rights should be used only when completing administrative functions. At all other times the user should be using normal user rights accounts. Furthermore the majority of the people with this privilege have not had training in the proper use of the rights. Sites where system administrative rights are not restricted are vulnerable to downloads of unauthorized software, spoofing of the IP address by an insider, blocking of scanning ports, and suspension of logging activities. Additionally when these workstations or laptops are compromised, they impart a greater threat to the organization because the individual may be able to use the system administrator rights on the compromised device to raise the privileges of the connected resources.

3.2.7 Legacy Systems

SC has numerous legacy systems that are no longer supported by the vendor. These systems (workstations, servers, etc) typically run custom software that was developed specifically for the hosting operating system. In most cases the individual that developed the application is no longer employed by the department, making transitioning of the application to a newer operating system difficult.

These legacy systems are the weak link in the infrastructure. Many of the devices do not support the access controls or auditing functions required by even low risk systems. Because these devices are no longer supported by the vendor, patches to remove vulnerabilities have not been developed or applied so they continue to be “targets of opportunity.”

[10] http://www.ntc.doe.gov/cita/CI_Awareness_Guide/T4travel/Theft.htm

3.2.8 Rootkits

Every component in a PC, such as graphics cards, DVD drives and batteries, has some memory space for the software that runs it, called firmware. Miscreants could use this space to hide malicious code that would load each time the PC boots Malicious code delivered via the memory on hardware components poses a rootkit threat since it will run on the PC before the operating system loads which will hide it from security software and other protection mechanisms. This low-level malicious code is known as a rootkit, and because the malicious code is stored on the hardware component and not a PC's hard disk, reinstalling the operating system or otherwise wiping the disk will not remove the threat. Attackers can use rootkits to access and modify personal information or attack other computers while remaining undetected.

The danger to SC is the pervasive use of personal laptops within the scientific community. Personal laptops are typically not protected as robustly as government equipment. While the majority of people have anti-virus and firewall software (either on their system or from their ISP) most do not have spyware protection, system patching, spam filtering, anti-phishing and wireless protection software installed. Failure to fully secure the personal device leaves it vulnerable to rootkit compromise. Even if the device is not connected to the wired infrastructure, the mere transfer of information via a USB thumbdrive is sufficient to pass a rootkit to a Science workstation.

3.2.9 Social Engineering

In addition to social engineering through conversation, the opportunity to insert rootkits or other malware into the environment is possible through the use of thumb-drives, CD or simply phishing. Sharing information by downloading files to a co-worker thumb-drive is a common practice within SC. However the thumb-drive could easily upload a rootkit or back door Trojan into the workstation. This means of insertion would bypass the virus signatures on the border firewall and the anti-virus software on the workstation itself (rootkit upload).

Additionally many scientists receive CDs in the mail from research workgroups, government forums, or even from DOE Headquarters. A rogue CD can be sent to multiple people within SC that could appear to be legitimate, but upon insertion may install malware that could start collecting specific types of information for transmission at some future period, or perform some other nefarious activity.

Phishing (being directed to open bogus e-mail, or log onto a spoofed website) is also another social engineering attack for which caution is required. Many scientists have world-wide distributed e-mail lists and so the opportunity to receive a phishing attack is ever present.