47075 Credit

Credit for course 47075 in UTrain can be received by completing either the course or by testing out:

- **Complete the Course** - After reading the material, click the Click for Credit box.
- **Test Out** - Close out of this course, then search for and launch course number 47926 in UTrain. Testing out requires a minimum score of 80%. If you are accessing this course externally, you will need to log into the UTrain system to access course 47926 (requires A-level CRYPTOCard to access).

Information Security Refresher Briefing

Course #47075 – rev. 2
LA-UR 11-06761
Updated August 2011

Los Alamos NATIONAL LABORATORY EST. 1943

Introduction and Overview

This refresher training reviews important information about your cyber security responsibilities and requirements and highlights major changes in the last year:

- Certain Blackberry devices are now allowed "behind the fence." Other mobile devices are now being evaluated, and wireless network pilot programs are underway across the Lab
- Do not install unauthorized software on Laboratory information systems.
- Follow the practice of "least privilege" while using privileged user accounts. All users will use their general user account for all actions that do not require elevating to a privileged account.
- Remain diligent against phishing, spam, and other advanced persistent threats

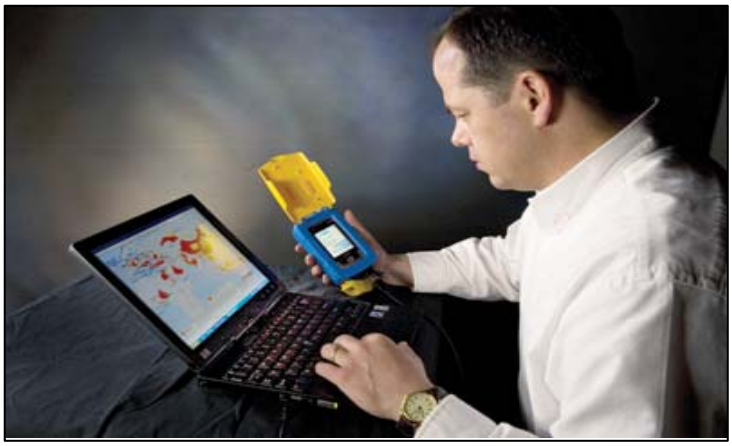
Objectives

When you have completed this training, you will be able to recognize

- important user requirements and responsibilities
- potential information security incidents and events
- vulnerabilities posed by installing unauthorized software
- vulnerabilities posed by email and actions you can take to reduce email associated risks, and
- the process for reporting potential incidents and events.

Completion of this course will imply that you acknowledge your responsibilities as a computer user. You must complete this course every year. Failure to keep this training current will result in the automatic disabling of your CRYPTOCard/WIN account.

Threats and Vulnerabilities



Threats to the security and stability of LANL's information systems are constantly evolving, so every computer user must diligently manage and protect their system and electronic information. Never underestimate the importance of each person in securing our information and serving LANL's mission.

Hackers, intelligence collectors, and malicious or careless users pose a threat to our information systems. News reports of hackers stealing personal information from computer systems in banks, credit card companies, and even hospitals have become common. It should not be surprising that computing systems at LANL and other Department of Energy (DOE) sites are also targeted by hackers.

Each month LANL records millions of unauthorized attempts to gain access to its computing systems. So far, our track record in preventing loss of information and damage to computing systems has been excellent. But we cannot let down our guard. The methods being used to gain unauthorized access to computing systems are constantly changing. Each computer user is a link in the LANL information security chain.

Recognizing a Security Event

An information security event is anything that affects normal operations of or has an undesirable impact on a computer system and/or computing facility. Some events are of such concern or potential impact that they become categorized as "incidents of security concern." An unclassified computer that is contaminated with classified information and the loss of PII are examples of incidents of security concern.

Unusual occurrences, frequent system crashes, or unexplained or suspicious poor performance of your system may signal a problem; potential scams, phishing attempts, social engineering attacks, and viruses also pose a risk. These types of events may or may not constitute an incident of security concern.

Social Engineering

Many compromises of data begin as social engineering attacks or email contaminated with malicious software. The term "social engineering" refers to nontechnical intrusions that rely heavily on human interaction and often involves tricking people into breaking normal security procedures. Attackers may send you email that appears to be from your bank, asking you to confirm your user account information (including your password). Or you may receive a thumb drive during a conference that is contaminated with malicious software.

Social engineering attacks constitute information security events and must be reported. Treat all communications from unknown persons as suspected social engineering attempts. Be polite, but verify. Protect yourself from social engineering attacks:

- Do not put media (thumb drives, flash drives, CDs, etc.) into LANL information systems without verifying that the information is from a legitimate source and is needed for your work.
- Never share passwords or CRYPTOCard personal identification numbers (PINs).

Unauthorized Software

Computer attackers often deploy software to remotely exploit information systems. Once a machine has been exploited, attackers can use it to collect information. When unsuspecting users install malicious software (malware), the security of their systems and the entire network can be compromised. The Laboratory requires the cooperation of users to protect the integrity of its systems.

- LANL provides many software applications that have been analyzed for potential security risks and issues. The user is responsible for any additional software installations.
- Organizations should monitor and control software installed by users to identify systems running vulnerable or malicious software.
- Software for which source code is not available or from sources with limited or no vendor maintenance (i.e., freeware or shareware) must not be used on information systems at the Laboratory, unless
  - the software is necessary for mission accomplishment
  - no alternative solutions are available
  - the software has been scanned for potential viruses and malware.

Authorized hardware and software

PurchaseIT is the LANL methodology for the procurement, receiving, hardening, and deployment of information technology hardware, software, and services. It is designed to enhance security, lower costs, and maximize efficiency.

Electronic Software Distribution (ESD) is the preferred method for purchasing, downloading, and updating application software. Ensure that you have proof of legal ownership (for example, licenses) for all applications, and avoid using unapproved software.

Contact your OCSR/ISSO or system administrator before purchasing, transferring, or salvaging any computer hardware or if you need software from outside of ESD.

Email, Spam, and Phishing

Email is an important tool for communication and enhancing productivity. It is also useful for dissemination of information—including malicious content—and for acquiring sensitive information.

Spam is the general name for broadly disseminated, unsolicited email. Spam includes email distributed as general marketing and solicitations as well as malicious emails such as those carrying embedded links or attachments designed to compromise computer security measures. It can also be used to encourage the receiver to open attachments or click embedded links that contain malware.

Phishing is a type of email spam that appears to come from a trustworthy entity and attempts to acquire sensitive information such as user names, passwords, personally identifiable information (PII), or financial information and therefore poses a risk to our information security.

Email vulnerabilities

Email is filtered as it comes into LANL. Although most suspicious email is blocked at the firewall, potentially dangerous email may nevertheless be delivered to your inbox. You might even receive email that has been "spoofed," appearing to come from a lanl.gov or other familiar address. In some cases, the email might appear to be from someone you know. Most suspicious email can simply be deleted. If you're unsure about the need to report suspicious email, contact the Security Inquiry Team at 665-3505.

To protect your computer systems and the information they contain

- Keep your virus protection and virus definition files up-to-date
- Install only approved software on Laboratory systems
- Protect your email address
- Open email from only the people you recognize
- Do not click on URLs or attachments within an email unless you know the sender is trusted and the email is legitimate. Also, be especially wary of emails, even from trusted sources, that have weird subject lines or simply links and or attachments
- Send spam to the trash unopened.

Email and Classified Information

Email is also a risk for the inadvertent, unauthorized disclosure of classified information to unauthorized recipients. The following practices will also help prevent unauthorized disclosure of classified information in unclassified environments:

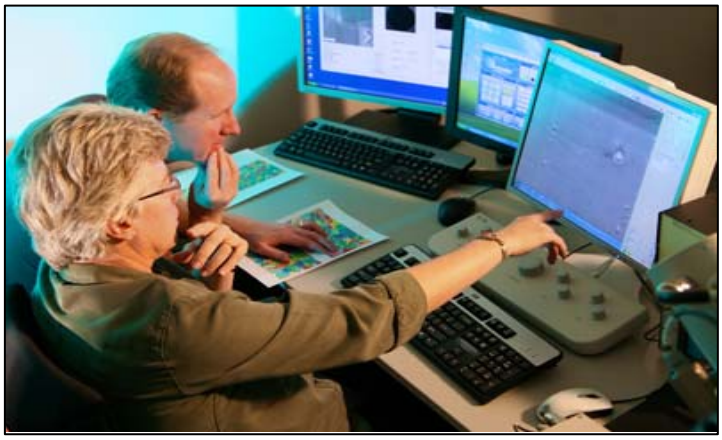
- Have derivative classifier review email and any attachments if
  - it contains technical or programmatic information, or
  - you are unsure of the email's classification.

- Do NOT auto-forward email received at lanl.gov outside the Yellow network.
- Use a LANL-approved encryption tool (Entrust) when sensitive unclassified information is sent outside LANL.
- When sending PII electronically, you must identify it as such in the subject line of the email. When sending PII outside LANL, it must be encrypted.
- Mark email and attachments with the sensitivity level and applicable caveats if they contain sensitive unclassified information.

- Send classified email only on systems approved for classified transmission.
- Keep the list of recipients as short as possible and send only to recipients with a need to know.
- When in doubt, don't send it out.

Lesson Learned

A researcher had been working on a white paper describing a new process. The document, verified as unclassified by a derivative classifier, is sent to a colleague for review and input. He modifies the document slightly, and it is electronically sent to the division for their information.
After the document was sent, an observant recipient noticed that two words had been placed together, changing the document to Secret Restricted Data. The resulting security incident was reported to the Security Inquiry Team, and a team of people was required to manage the incident.



What could have prevented the incident? The author of the document should have had it reviewed again by a derivative classifier before distributing the document. If he had, the incident would have been confined to the author's and the colleague's machines. Even better, the colleague could have consulted a derivative classifier before making the changes or before returning it to the author.

Adding or changing one word within a document can change the classification of the document. A derivative classifier should review documents as each draft is completed.

Portable Electronic Devices

Portable electronic devices (PEDs) are devices that can store and/or transmit data; examples include cell phones, laptops, iPhones, iPads, iPods, thumb drives, etc. Restrictions are placed on the introduction and use of PEDs depending on ownership, security requirements of the area, and potential risks.

Confusion about requirements for handling portable electronic devices leads to frequent breaches of security. Always consult a cyber security policy or representative, such as an OCSR or ISSO, prior to introducing a PED into your work area.
Be aware that government-issued Blackberry devices have been approved for use in certain security areas. Additional information about the Laboratory's Blackberry service can be found at:
http://int.lanl.gov/source/orgs/nie/nie4/blackberry/index.shtml

Reporting Events and Suspicious Computer Activities

All events and suspicious computer activities must be reported to the Security Inquiry Team at 665-3505. Outside of normal hours of operation (7 a.m. to 5 p.m.), report potential incidents immediately to the Associate Directorate for Security and Safeguards on-call duty officer (949-0156).

The Security Inquiry Team will categorize the event and determine what actions are necessary. If you are uncertain whether to report something, err on the side of caution and report it.

Do NOT discuss the event over the phone, email, or voicemail. Details about events might be classified. Simply contact the Security Inquiry Team stating that you have a problem and follow their directions.

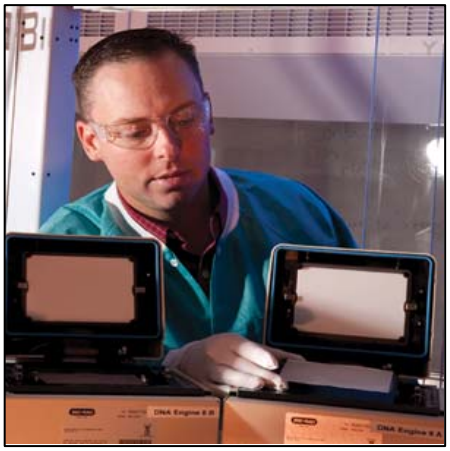
In addition, you should immediately disconnect your computer system from the network if you suspect it is contaminated with a virus or if an unclassified system is contaminated with classified information. However, do not turn off your computer—wait for instructions from the Security Inquiry Team and/or computing or networking professionals.

After notifying the Security Inquiry Team, you must contact your responsible line manager (RLM) and your organizational computer security representative (OCSR) and/or information system security officer (ISSO).

General User Responsibilities

General users of LANL computer systems have many responsibilities:

- Know your OCSR/ISSO
- Keep your information security training up-to-date
- Never use your system for
  - pornography, gambling, or political purposes
  - inappropriate or malicious purposes (harassment)
  - accessing or tampering with other systems or networks
  - personal gain (selling items, downloading music, etc.)
- Ensure that system configurations are in compliance with the applicable information system security plan (ask your OCSR/ISSO when in doubt)
- Protect the sensitivity level of the information you process
- Share information with others only on a need-to-know basis
- Recognize potential security events and promptly report them to the Security Inquiry Team at 665-3505
- Protect, control, disseminate, and ultimately destroy unneeded information and/or information systems
- Comply with LANL password policies, and never share your password or CRYPTOCard PIN with anyone.
- Use least privilege principles while using privileged user accounts. All users should use their general user account for all actions that do not require elevating to a privileged account.



Access Controls

Every computer user's duties, responsibilities, and privileges are assigned when access is granted to an information system. Access is based on your clearance, your "need-to-know" for the information, "least privilege" (access only to information you need to do your job), and "separation of duties" (for sensitive information systems and activities).

The user's responsible line manager works with the user and system administrator to determine and administer proper access authorizations.

Privileged User Accounts

The Laboratory applies the principle of least privilege by allowing computer users only those privileges that are essential for their work. Every user is given a password-protected work space associated with their general user account; privileged user accounts are to be used only when absolutely necessary.

Many computer users at the Laboratory have privileged user accounts, but these users must use their general user account for all actions that do not specifically require using their privileged user account.

Privileged user accounts significantly increase the risks of improper system configuration and a compromised computer. These risks can have a ripple effect and impact Laboratory operations.

The least privilege principle is intended to protect data from faults and malicious behavior while maintaining the functionality and integrity of a computing system and network. Least privilege helps protect and stabilize the Laboratory's computing and information security posture.

Identifying Privileged Users

A privileged user has additional rights, privileges, or access to control, monitor, or administer functions of an information asset or computer. Privileged users go by different names on different computer platforms:

- Mac operating systems use the term "administrator" for privileged user. Administrator accounts and any account that runs UID 0 / GUID 0 / GUID 80, or has sudo privileges, can change the security posture of the computer.
- Windows uses the term "administrators" for privileged user, meaning any account that is a member of the local administrator user group or has any extra privileges granted to the account using local security policy.
- Linux and Unix use the terms "power user" and "root user" for those with extra privileges, for example, the ability to run sudo commands and similar utilities or membership in adm, wheel, UID 0 user root, or GID 0 group root.

Scenario: Too Much Privilege

Consider the manager who regularly visits sites outside LANL to give presentations from a personal laptop. The manager insists on having a privileged user account on the computer. The manager is just about to deliver a presentation to colleagues when an offensive message appears on the screen, which then locks up. Upon restarting the laptop, the manager finds that the hard drive has been reformatted. In this case, the offensive message and subsequent destruction of data resulted from malicious software that infected the laptop from a compromised web site.

Because the manager was a privileged user, the escalated rights and privileges of the user account enabled the malicious software to disable the antivirus software, install itself, manipulate the registry, and place files in the Windows system directory.

Best Practice

While many scenarios can exploit administrative privileges, the common factor is that users who routinely log in using privileged user accounts when a general user account is sufficient are significantly more likely to compromise their computers than those who use general user accounts (least privilege principle) while computing.

It is in the best interest of computer users to opt for the least privilege while computing. Therefore, it is required that all users computing at the Laboratory use their general user account for all actions that do not require elevating to a privileged user account.

Wireless Network Access: AccessIT

LANL is offering wireless access to the Yellow and Visitor networks in select buildings, both on campus and within the Los Alamos town site. WiFi zones currently are available at select buildings at LANSCE and at TA-3 in the Otowi Building, University House, and the second floor of the Study Center.

- Yellow access requires a device certificate
- Visitor access requires proper credentials for login. Contact your manager for visitor login credentials.
- Contact Departmental Computing Services (DCS) or your IT support person for assistance with device certificates.

Please note that AccessIT is for LANL-appropriate use only; this service is not available to the general public. AccessIT also is not authorized within security areas (behind the fence). Networks are monitored and users should have no expectation of privacy.

For more information and a listing of buildings, go to http://network.lanl.gov/wireless/

Resources

Information Security Web Site and Customer Support Center

Detailed information about roles and responsibilities, program elements, and procedures can be found at the Information Security Web site (http://int.lanl.gov/security/cyber). You can also pose a question to the Information Security Customer Support Center via email sent to cybersecurity@lanl.gov or calling 665-1795

Organizational Computer Security Representative

Your OCSR/ISSO serves as a point-of-contact for information security and assists your RLM in ensuring that the information security program is implemented in your organization for computing systems. Your OCSR/ISSO can provide information and resources to help
you implement information security requirements.

The OCSR/ISSO list can be found online at http://services-catalog.lanl.gov/docs/OCSR-ISSO.xlsx

Senior Cyber Security Leader

The senior cyber security leader provides information security expertise and works with information security professionals within a directorate. A listing of senior cyber security leaders can be found online at the Information Security Web site.

Institutional Procedures

Institutional procedures communicate requirements to LANL workers regarding LANL-specific operations. Implementing these procedures ensure compliance with DOE directives. The procedures that pertain to Safeguards and Security can be found online at http://int.lanl.gov/security/cyber/ (click on “Policies” at the Information Security Web site).

- PD 210 Cyber Security Program
- P 210-1 Cyber Security Program Exceptions, Variations, and Deviations
- PD 226 Information Technology Configuration Management
- P 211 Sanitizing Information System Storage Media, Memory Devices, and Other Related Hardware
- P 212 Marking Information Systems and Media
- P 213 Cyber Security Wireless Computing Devices
- P 214 Information Security Incident Management
- P 216 Cyber Information Security Certification and Accreditation
- P 217 Portable Electronic Devices (PEDs)
- P 218 Cyber Security Access Controls
- P 219 Cyber Security Risk Management
- P 220 Information Security Education and Awareness
- P 222 Approval Process for Non US Citizen Privileged User Accounts
- P 225 Identifying and Handling Electronic Sensitive Unclassified Information (SUI), Including Personally Identifiable Information (PII)

Course Credit

To receive credit for reviewing this course information, please click the button below. If you have any issues with receiving credit, please contact the Information Security Customer Support Center via email sent to cybersecurity@lanl.gov or calling 665-1795.

Click For Credit