STUDENT GUIDE

CYBER SECURITY AWARENESS

Contents

Course Overview

This is a scenario-based course in which you will learn about various cyber attacks used to target cleared defense contractors. An overarching scenario is threaded throughout the course to provide a context for more detailed scenarios that are specific to each attack type.

The most common cyber attacks leverage the following:

- Phishing
- Malicious code
- Weak and default passwords
- Unpatched or outdated software vulnerability
- Removable Media

Throughout the course, each scenario will end with a question to help you assess your understanding of these attack types. Your responses will not be judged in any way; in fact, all responses will provide an opportunity for you to broaden your knowledge of the subject matter.

Course Introduction

Setting the stage

A multi-faceted cyber attack has resulted in three, large, “worst-case” events affecting the general population, cleared defense contractors, and the U.S. military.

Scenario

The Internet has changed the world immeasurably. It is woven into our economy, our national security, and our lives. Nothing has ever changed the world faster. But the advantages and capabilities that come with the Internet come with a cost.

Not long ago, it was science fiction to imagine worst-case scenarios where hackers and others who seek to do us harm disable critical infrastructure, infiltrate defense systems, steal proprietary information, and extort millions of dollars from industry. But now, these threats are no longer outside the realm of possibility. Our intellectual property, innovative skills, and military technology are at risk. The threat is real and it is here. *You* are the first line of defense.

Each year, network intrusions aimed at our government and defense industries increase and become more sophisticated. The Global Information Grid, or GIG, is probed 3 million times each day. Imagine how many times less secure networks are targeted. Individually, many of these attacks go largely unnoticed, but the cumulative effect and the damage done are staggering. Some estimate the magnitude of data theft that has already occurred is equivalent to the size of a digitized Library of Congress. That translates to billions and billions of dollars, not to mention the immeasurable strategic loss.

Your role

Who is attacking us and how are they doing it?

As you follow this examination of cyber attacks that resulted in the loss of U.S. defense-related information and technology, you will learn about how you may be targeted and some ways to help stop these attacks.

Along the way, you will meet people that both knowingly and unknowingly played a part in these events. You will also meet three advisors who will give you insight into how you can protect yourself and your organization

You will also have access to examples of what hackers and other adversaries gain from successful cyber attacks.

Other key players

Before we get started, let's first review some of the key players that are involved not only in protecting against cyber threats but also in causing them.

If you work for the DoD, you may have a **Security Officer (SO)** or other security point of contact, such as a Security Specialist. If you work for a defense contractor, your facility has a Facility Security Officer, or FSO. Regardless of the title, these individuals are responsible for security at their facilities and for ensuring that security regulations and policies are followed.

Counterintelligence (CI) analysts support the various intelligence and law enforcement activities that handle cyber threats. They rely on you to be their eyes and ears within your organization.

The term **"adversary"** is used throughout this course to represent the adversary that the SO and CI analyst are trying to protect you from. Adversaries may include:

- Foreign intelligence entities
- Terrorist organizations
- Business competitors
- Hackers
- Cyber criminals
- Organized crime

Phishing

Timeline Introduction

Cyber attacks are the fastest-growing method of operation for our adversaries. Taken individually, many of these attacks go largely unnoticed. However, you never know which attack will be the one that provides adversaries with the key piece of information they're seeking – the final piece that invites disaster in.

This course presents you with a timeline that outlines various cyber attacks. Some of these attacks include case files that you will examine to learn more about cyber attacks.

Date	Event
August 2011	List of targets obtained via social networking sites
September 2011	Denial of Service (DoS) attack shuts down large CDC
October 2011	Foreign Intelligence Entity (FIE) infiltrates DoD network
November 2011	**Case File: Phishing**
December 2011	Virus corrupts CDC network data
January 2012	**Case File**
February 2012	Hackers target critical infrastructure; bring down power grid
March 2012	**Case File**
April 2012	Hacker steals proprietary information from CDC; sells to foreign company
May 2012	**Case File**
June 2012	CDC cyber attack clean up estimated at $1B
July 2012	Foreign group sabotages surveillance satellite imagery and software
August 2012	**Case File**

Contact: November 2011
Targeted through: Email

Scenario: A cleared defense contractor was awarded a large government contract.

Immediately following the contract award, employees received an email from who appeared to be their IT department, asking personnel to provide their system passwords. Believing the email was a legitimate request from the IT department, many employees provided the information.

As it turns out, the email was not from the IT department. It wasn't from within the contractor's facility at all. The email was sent by a foreign group disguising or "spoofing" their identity, looking for a way into the contractor's network. By providing the requested information, the employees have allowed the foreign group access to their system.

The foreign group is now able to move within the contractor's network, stealing proprietary information that allows them to build a competing product. Over the next few years, the impact to the defense contractor is millions of dollars in lost revenue. The national security implications of having such technology in foreign hands are grave.

Take a look at what the adversary collected from the CDC's network. When you're satisfied with your review of this file, you may move on to the knowledge check and feedback.

Adversary File: Information collected from CDC network
Information obtained: • Employee user names/passwords • Access to CDC network
CDC data lost: • Personnel information • DoD program information • Sensor component manufacturers • Sensor component manufacturers • Sensor technology specifications and schematics

Scenario Question

To: Employees
From: IT Department

Subject: Project Alpha Ramp Up

Dear employees,

Project Alpha requires its data to be stored separately on a secure server. To expedite the process, the IT department is adding all users. Please provide your user name and password: www.projectalpha@123.com

If you received an email asking for personal information, how would you respond? Select your response; then review the feedback that follows.

a. If the email is from within my organization, there's no harm in providing the information. I'd provide the requested information.

b. I'm not sure why my user name and password would be required. I'd notify my security point of contact or help desk.

c. I don't care who is requesting my password, I would never provide it. I'd delete the e-mail.

Scenario Question Feedback

This type of email is known as phishing - a scam that places you and your organization at risk. For you personally, phishing may result in identity theft and financial loss. For your organization, phishing jeopardizes the security of information and information systems.

Choice B is an appropriate response to receiving an email asking for personal information. When you receive suspicious email, you should notify your security point of contact or help desk.

Choices A and C are risky responses; you should not provide personal information if you receive any suspicious e-mail. You're IT department will need the email to track its origination, so you should also not delete it. Instead, you should contact your security point of contract or help desk.

Take a moment to review indicators of phishing and when you are ready, review Countermeasures to learn how to protect against phishing.

Cyber Attack: Phishing
A scam that places you and your organization at risk.
Technique
• A high-tech scam that uses e-mail to deceive you into disclosing personal information • Spear Phishing: a type of targeted phishing that appears to be from a specific organization, such as your employer or bank
Indicators
The following are suspicious indicators related to phishing and spear phishing: • Uses e-mail • May include bad grammar, misspellings, and/or generic greetings • May include maliciously-crafted attachments with varying file extension or links to a malicious website • May appear to be from a position of authority or legitimate company: • Your employer • Bank or credit card company • Online payment provider • Government organization Spear phishing specifically: • Has a high level of targeting sophistication and appears to come from an associate, client, or acquaintance • May be contextually relevant to your job

- May appear to originate from someone in your email address book
- May contain graphics that make the email look legitimate

Effects include, but are not limited to:

- Deceives you into disclosing information
- Allows adversary to gain access to your and/or your organization's information

Countermeasures
The following countermeasures can be taken to guard against phishing and spear phishing: • Watch out for phishing and spear phishing • Delete suspicious e-mails • Contact your system security point of contact with any questions • Report any potential incidents • Look for digital signatures • Configure Intrusion Detection Systems (IDS) to block malicious domains / IP addresses • Appears to direct you to a web site that looks real **Do Not:** • Open suspicious e-mails • Click on suspicious links or attachments in e-mails • Call phone telephone numbers provided in suspicious e-mails • Disclose any information

NOTE: If you suspect you may have been a target of phishing, report it to your Facility Security Officer (FSO) or security point of contact.

Cyber Threats and Their Targets

Who are adversaries?

Adversaries are anyone that seeks to do you and your organization harm – they may include insiders from your own organization, hackers, cyber criminals, terrorists, members of organized crime, or foreign intelligence entities

What do adversaries target?

The short answer is that they target *anything* that may be of value. Their targets aren't limited to classified information. No piece of information is too small; adversaries often obtain unclassified data and when they're able to collect enough of it, they can piece it together and learn things—even classified things—that may do you, your organization, and our country harm.

Review the table below to learn about the types of information and technology adversaries may target.

Targeted Technology and Information
The Threat • Insiders • Hackers • Cyber Criminals • Terrorists • Organized Crime • Foreign Intelligence Entities
The Target • Sensitive company documents and proprietary information • Export controlled/classified information and technology • Information on DoD-funded contracts • Sensitive technological specification documents • Users' login IDs and passwords • Personal Identifying Information (SSN, date of birth, address) • Contact rosters and phone directories

What do adversaries do with the information they collect?

Once the information is in the adversaries' hands, there's no end to what they may do with it. Sometimes they use it to simply see what you are up to. Sometimes they use it to help their countries or others build a similar program. There are endless examples of foreign countries saving millions of dollars—sometimes billions of dollars! —taking advantage of the research and development we've spent years building. In an instant, our nation's strategic and competitive edge can be gone.

Review the table below to learn the most targeted technologies in recent years.

Most Targeted Technologies
• Information systems • Aeronautics, including technology related to unmanned aerial vehicles (UAVs) • Lasers and optics • Sensors • Marine systems • Positioning, navigation, and time • Electronics • Militarily Critical Technologies List (MCTL) technology • Armaments and energetic materials • Materials and processing

NOTE: To view the most up-to-date information on targeted technology and information, refer to the Targeting U.S. Technologies: A Trend Analysis of Defense Reporting from Industry report. This report is accessed within the Counterintelligence section of the DSS website at www.dss.mil.

Malicious Code

Timeline update

Have you ever dealt with malicious code on your computer? Likely you have, though you may not even be aware of it. Let's take a look at a case involving malicious code.

Date	Event
August 2011	List of targets obtained via social networking sites
September 2011	Denial of Service (DoS) attack shuts down large CDC
October 2011	Foreign Intelligence Entity (FIE) infiltrates DoD network
November 2011	**Logon credentials stolen in phishing attack; CDC network compromised**
December 2011	Virus corrupts CDC network data
January 2012	**Case File: Malicious Code**
February 2012	Hackers target critical infrastructure; bring down power grid
March 2012	**Case File**
April 2012	Hacker steals proprietary information from CDC; sells to foreign company
May 2012	**Case File**
June 2012	CDC cyber attack clean up estimated at $1B
July 2012	Foreign group sabotages surveillance satellite imagery and software
August 2012	**Case File**

Contact: January 2012
Targeted through: Link in online forum

Scenario: A DoD employee often frequented social networking sites and online forums.

On one forum, he saw a link to an article related to the project he was working on. Curious to learn more, he clicked on it.

That link contained malicious code, planted on the online forum by a foreign group. When the DoD employee selected the link, it automatically downloaded the code onto the DoD's network.

The code then allowed the adversary's organization to view the information on the system.

Take a look at what the adversary collected from the CDC's network. When you're satisfied with your review of this file, you may move on to the knowledge check and feedback.

Adversary File: Information collected from R. Solias
Information obtained: • CDC network access • DoD program details • Names and contact information of CDC and DoD personnel • Corruption of network data • Loss of weapons program schematics • Surveillance system compromised

Scenario Question

www.socialnetworkingsite1.com

New Technology forum:

JBrown posted: I just read a really interesting article, check it out – Emerging sensor technology: Next big thing

Selecting the link downloaded malicious code. Would you have selected the link? Select your response; then review the feedback that follows.

a. Definitely, my organization has strong anti-virus software. I'd open the link.

b. No; I wouldn't open a link from an unknown forum poster.

c. It depends. If I was on a reputable site, I'd have no problem opening it.

Scenario Question Feedback

Malicious code includes any program which is deliberately created to cause an unexpected and unwanted event on an information system. Using malicious code, adversaries can steal information, sabotage systems, or even take over systems. Can you imagine the consequences of a weapons system under an adversary's control?

Choices A and C are risky responses. Opening a link from an unknown poster can open your computer up to malicious code. Once malicious code is downloaded, it allows adversaries to see what you're working on. Adversaries place links in all sorts of places and have been known to compromise even the most reputable sources, hoping you'll open the links. Anti-virus software may not detect the malicious code activated by selecting a link.

Choice B is an appropriate response; you should not select links posted by individuals you do not know and trust.

Take a moment to review indicators of malicious code and when you are ready, review Countermeasures to learn how to protect against it.

Cyber Attack: Malicious Code
Software that does damage and/or creates unwanted behaviors
Technique
Embeds malicious code into links which, once selected, download the malicious code to the user's computer and network. Malicious code includes: • Viruses • Trojan horses • Worms • Keyloggers • Spyware • Rootkits • Backdoors
Indicators
The following are suspicious indicators related to malicious code; malicious code may be distributed via: • E-mail attachments • Downloading files • Visiting an infected website

- Removable media

Effects include, but are not limited to:

- Corrupt files and destroyed or modified information
- Compromise and loss of information
- Hacker access and sabotaged systems

Countermeasures
The following countermeasures can be taken to guard against malicious code. To guard against malicious code in email: • View e-mail messages in plain text • Do not view e-mail using the preview pane • Use caution when opening e-mail • Scan all attachments • Delete e-mail from senders you do not know • Turn off automatic downloading To guard against malicious code in websites: • Block malicious links / IP addresses • Block all unnecessary ports at the Firewall and Host • Disable unused protocols and services • Stay current with all operating system service packs and software patches

NOTE: If you suspect your information system has been compromised, report it to your FSO or security point of contact.

Anatomy of a Computer Intrusion

Do you know how adversaries launch a cyber attack?

First, they research and identify targets through open source means such as social networking sites. With targets identified, adversaries look for a way into your organization's network.

Reconnaissance: Attackers research and identify targets through open source means

Intrusion into the network: Phishing emails containing malicious code sent to targets

Once they gain access to your network, adversaries can easily obtain user credentials and install backdoors and utilities that let them enter your system at will and take what they find.

Obtain user credentials

Establish a backdoor: Attackers install backdoors for future and continued exploitation.

Install multiple utilities: Utility programs are installed on the victim's network

Data exfiltration: Attackers obtain data from the victim's servers

After accessing your system, adversaries can usually cover their tracks so their presence on the network goes unnoticed. Even if detected, they will use other means and try again.

Maintaining persistence: Attackers use other methods if they suspect detection

Weak and Default Passwords

Timeline update

Your password is critical to protecting you and your organization's information from an adversary. But passwords are not often taken seriously. In fact, many intrusions occur because people use weak, easy-to-remember passwords. Let's take a look at an example of how this may happen.

Date	Event
August 2011	List of targets obtained via social networking sites
September 2011	Denial of Service (DoS) attack shuts down large CDC
October 2011	Foreign Intelligence Entity (FIE) infiltrates DoD network
November 2011	**Logon credentials stolen in phishing attack; CDC network compromised**
December 2011	Virus corrupts CDC network data
January 2012	**Malicious code infiltrates CDC network; proprietary information stolen**
February 2012	Hackers target critical infrastructure; bring down power grid
March 2012	**Case File: Weak and Default Passwords**
April 2012	Hacker steals proprietary information from CDC; sells to foreign company
May 2012	**Case File**
June 2012	CDC cyber attack clean up estimated at $1B
July 2012	Foreign group sabotages surveillance satellite imagery and software
August 2012	**Case File**

Contact: March 2012
Targeted through: Weak or Default Passwords

Scenario: A cleared defense contractor was awarded a large defense contract.

News of the contract award was published online and in several major newspapers. Employees of the contractor congratulated one another on several social networking sites.

Adversaries heard of the contract award.

Using the contractor's website and the information posted on social networking sites, adversaries were able to quickly find employees and target them. By successfully using a socially engineered email that tricked a user into introducing malicious code into the network, adversaries were able to obtain the user names and passwords of several employees.

Once it had login data, the adversary group used the data to obtain a great deal of information.

The loss of this information was devastating from a competitive and strategic advantage standpoint, both for the company and the country.

Take a look at what the adversary collected from the CDC's network. When you're satisfied with your review of this file, you may move on to the knowledge check and feedback.

Adversary File: Information collected from adversary use of weak passwords
Information obtained: • CDC personnel user names/passwords • CDC network access • CDC personnel SSNs and birthdates • DoD program details • Weapons technology specifications • Weapons components and their manufacturers

Scenario Question

What philosophy do you follow when creating passwords? Select your response; then review the feedback that follows.

a. I use the same, very secure password for everything. It's 8 characters and includes lower and upper case letters, numbers, and special characters. There's no way a password cracker is getting my information.

b. I change passwords frequently and always use a combination of numbers, letters, and special characters. I'm fairly confident my passwords are secure.

c. I don't worry about my password; my organization's security is strong enough to defeat a hacker. I make sure to use something I can remember like a significant date or name.

Scenario Question Feedback

There's really no excuse for a weak password – it's the easiest thing you can control.

You think passwords don't make a difference? Consider this: Readily available password cracking software running on an average computer can crack an 8-character, all lowercase letter password in seconds. Take that same password and increase the complexity of the password by adding upper and lower case letters, numbers, and special characters and the time to crack it increases exponentially. Passwords matter.

Choices A and C are risky responses. If one system is compromised, all systems are at risk. The security for the online forum you frequent is likely not as secure as your organization's virtual private network, or VPN. If you use the same password for both and a hacker compromises the online forum, your organization may also be at risk. Using birthdays or anniversaries and names significant to you put your information and your organization at risk.

Choice B is an appropriate response; you should use a combination of number, letters, and special characters when creating passwords and change your passwords frequently.

Take a moment to review indicators of weak and default passwords and when you are ready, review Countermeasures to learn how to protect against it.

Cyber Attack: Weak and Default Passwords
• Create an easily exploitable system vulnerability • Is a vulnerability that is easily controllable by users
Technique
Adversaries easily gain access to computer and network using legitimate login credentials
Indicators
The following are indicators of weak passwords; weak passwords include those that use: • Words found in the dictionary • Readily available information significant to you (names, dates, cities, etc.) • Lack of character diversity (e.g., all lower case letters) Effects include, but are not limited to, hackers:

- Exploiting users' habit of repeating passwords across sites and systems
- Cracking passwords to less secure sites
- Accessing your and your organization's information

Countermeasures
The following countermeasures can be taken to guard against password compromise, when creating a password: • Combine letters, numbers, special characters • Do not use personal information • Do not use common phrases or words • Do not write down your password, memorize it • Change password according to your organization's policy • Enforce account lockout for end-user accounts after a set number of retry attempts • Do not save your passwords or login credentials in your browser • NEVER SHARE YOUR PASSWORD

NOTE: If you suspect your password has been compromised, report it to your FSO or security point of contact.

Reporting Requirements

You are the first line of defense against cyber threats.

It is essential you report any incident or behavior that may be related to a potential compromise of classified information or inappropriate disclosure of sensitive unclassified information, including those listed here, to your facility security officer or security point of contact. He or she will direct your information to the appropriate authorities, who will assess it and determine if a concern exists.

DoD personnel and cleared defense contractors are both required to report such information. DoD Directive 5240.06, Counterintelligence Awareness and Reporting, outlines requirements DoD personnel must follow. The National Industrial Security Program Operating Manual, or NISPOM, outlines requirements contractors must follow.

DoD Reportable Foreign Intelligence Entity (FIE)-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors *(Source: DoDD 5240.06, May 17, 2011)*

DoD personnel who fail to report the contacts, activities, indicators, and behaviors in items 1-10 are subject to punitive action.

1. Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
2. Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3. Network spillage incidents or information compromise.
4. Use of DoD account credentials by unauthorized parties.
5. Tampering with or introducing unauthorized elements into information systems.
6. Unauthorized downloads or uploads of sensitive data.
7. Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8. Downloading or installing non-approved computer applications.
9. Unauthorized network access.
10. Unauthorized e-mail traffic to foreign destinations.

The indicators in items 11-19 are reportable, but failure by DoD personnel to report these indicators may not alone serve as the basis for punitive action.

11. Denial of service attacks or suspicious network communications failures.

12. Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13. Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14. Data exfiltrated to unauthorized domains.
15. Unexplained storage of encrypted data.
16. Unexplained user accounts.
17. Hacking or cracking activities.
18. Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19. Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers

Contractor Reporting Requirements for Cyber Intrusions (NISPOM 1-301)
(Source: Industrial Security Letter 2013-05 July 2, 2013)

Cyber intrusions into classified systems fall under the reporting requirement of NISPOM 1-301 and must be reported to the FBI, with a copy to DSS. Contractors should or must consider reporting Cyber intrusions into unclassified information systems if the contractor believes they meet certain conditions.

Specifically, contractors must report cyber intrusions against classified information systems that indicate:

- Espionage
- Sabotage
- Terrorism
- Subversive activity

A cyber intrusion reportable under NISPOM 1-301 may involve one or more of a combination of active efforts, such as:

- Port and services scanning from consistent or constant addresses
- Hacking into the system
- Placing malware hacking tools into the system
- Passive efforts (e.g., unsolicited emails containing malware or internet sites that entice users to download files that contain embedded malware)
- Exploitation of knowledgeable persons through “phishing” and “social engineering”

Contractors should consider the following guidelines when making a determination to report a cyber intrusion to the FBI and to DSS under NISPOM paragraph 1-301:

- Evidence of an advanced persistent threat
- Evidence of unauthorized exfiltration or manipulation of information
- Evidence of preparation of contractor systems or networks for future unauthorized exploitation
- Activity that appears to be out of the ordinary, representing more than nuisance incidents
- Activities, anomalies, or intrusions that are suspicious and cannot be easily explained as innocent

Contractors are also reminded they are required to report to DSS:

- Efforts by any individual, regardless of nationality, to “obtain illegal or unauthorized” access to an information system processing classified information (NISPOM paragraph 1-302b)
- “Significant vulnerabilities” identified in information system “hardware and software used to protect classified material” (NISPOM paragraph 1-302j)

Contractors should also report cyber intrusions into unclassified information systems if the contractor determines they meet the following conditions:

- "(i) the facts and circumstances of the intrusion are sufficient to qualify as "actual, probable, or possible espionage, sabotage, terrorism, or subversive activities,"
- and "(ii) these activities constitute a threat to the protection of classified information, information systems, or programs that are otherwise covered by the NISPOM." (ISL 2013-05 July 2, 2013)

Suspicious Internet Activity

Timeline update

We've seen examples of how adversaries use phishing, malicious code, and weak passwords to target our information and information systems. Let's look at the next file.

Date	Event
August 2011	List of targets obtained via social networking sites
September 2011	Denial of Service (DoS) attack shuts down large CDC
October 2011	Foreign Intelligence Entity (FIE) infiltrates DoD network
November 2011	**Logon credentials stolen in phishing attack; CDC network compromised**
December 2011	Virus corrupts CDC network data
January 2012	**Malicious code infiltrates CDC network; proprietary information stolen**
February 2012	Hackers target critical infrastructure; bring down power grid
March 2012	**Case File: CDC personnel passwords cracked; system infiltrated and data stolen**
April 2012	Hacker steals proprietary information from CDC; sells to foreign company
May 2012	**Case File: Unpatched or Outdated Software Vulnerabilities**
June 2012	CDC cyber attack clean up estimated at $1B
July 2012	Foreign group sabotages surveillance satellite imagery and software
August 2012	**Case File**

Contact: May 2012
Targeted through: Unpatched or Outdated Software Vulnerabilities

Scenario: A cleared defense contractor's business was booming. After winning several large contracts, the company was busy hiring new employees to meet tight deadlines.

With everything going on, the contractor decided to delay its initiative to upgrade key software. Network administrators were busy supporting and getting new employees up-to-speed, so temporarily set aside notices to apply software patches.

The cleared defense contractor's information system was targeted by a foreign group. The vulnerability created by the outdated, unpatched software allowed the group to access the contractor's network.

The foreign group was able to obtain volumes of information and data. The group sold several pieces of the information and used other pieces to advance related programs in its own country.

This loss has potentially devastating consequences for the cleared contractor, its employees, and the safety of U.S. war fighters.

Take a look at what the adversary collected from the CDC's network. When you're satisfied with your review of this file, you may move on to the knowledge check and feedback.

Adversary File: Information collected from adversary infiltration as a result of unpatched/outdated software
Information obtained: • Access to CDC network • Identification of information system vulnerabilities • Proprietary software • Operations plans • Company personnel information

Scenario Question

The defense contractor's information system was made vulnerable by outdated and unpatched software. How does your organization handle this? Select your response; then review the feedback that follows.

a. System administrators are on top of it and we have a strict policy. I pay close attention to notices to upgrade and apply patches.

b. We use what works; we're not necessarily concerned with upgrading to the latest and greatest thing.

c. I have no idea; I'm busy enough as it is. I see notices about upgrades and patches, but I don't have time to worry about software versions or if my computer has every software patch installed.

Scenario Question Feedback

Vulnerabilities created by outdated and unpatched software are very serious. These vulnerabilities essentially leave an open door for adversaries to enter and steal your data.

Choices B and C are risky responses. While it may not seem like a necessity, ensuring the software on your network has the latest updates helps prevent network intrusion. A lax attitude toward software patches and updates basically invites adversaries into your organization's network.

Choice A is an appropriate response. You should work with your organization's system administrators to ensure the latest upgrades and patches are applied.

There are several indicators that your system is compromised. Take a moment to review them and when you are ready, review Countermeasures to learn how to protect against this threat.

Cyber Attack: Unpatched or Outdated Software Vulnerabilities
Provide vulnerabilities and opportunities for adversaries to access information systems
Technique
• Targets known software vulnerabilities to gain access to computer or network
Indicators
The following is a list of suspicious indicators related to unpatched and outdated software: • Unauthorized system access attempts • Unauthorized system access to or disclosure of information • Unauthorized data storage or transmission • Unauthorized hardware and software modifications Effects include, but are not limited to: • Corrupt files and destroyed or modified information • Hard drive erasure and loss of information • Hacker access and sabotaged systems

Countermeasures

The following countermeasures can be taken to guard against software vulnerabilities:

- Comply with the measures in your organization's policies, including the Technology Control Plan (TCP)*
- Stay current with patches and updates
- Conduct frequent computer audits
  - Ideally: Daily
  - At minimum: Weekly
- Do not rely on firewalls to protect against all attacks
- Report intrusion attempts

*Technology Control Plan:

- Stipulates how a company will control access to its export-controlled technology
- Outlines the specific information that has been authorized for release
- May be required by the National Industrial Security Program Operating Manual (NISPOM) and the International Traffic in Arms Regulations (ITAR) under certain circumstances
- Protects:
  - Classified and export-controlled information
  - Control access by foreign visitors
  - Control access by employees who are foreign persons

Cyber Security Tips

You've received many of these tips already, but let's quickly review how you can protect yourself and your organization from cyber threats.

Employees should:

- Use complex alphanumeric passwords
- Change passwords regularly
- Do NOT open emails or attachments from unfamiliar sources, even if it looks official
- Do NOT install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department
- Report all suspicious or unusual problems with your computer to your IT department

There are also tips managers and IT departments should follow. They're listed here:

- Implement defense-in-depth*
- Implement technical defenses**
- Update anti-virus software daily
- Regularly download vendor security patches for all software
- Change the manufacturer's default passwords on all software
- Monitor, log, and analyze successful and attempted intrusions to your systems and networks

*Defense-in-depth is a layered defense strategy that includes technical, organizational, and operational controls

**Technical defenses include firewalls, intrusion detection systems, and internet content filtering

Removable Media

Timeline update

We've reached our last case file. Let's see what we learn from this one.

Date	Event
August 2011	List of targets obtained via social networking sites
September 2011	Denial of Service (DoS) attack shuts down large CDC
October 2011	Foreign Intelligence Entity (FIE) infiltrates DoD network
November 2011	**Logon credentials stolen in phishing attack; CDC network compromised**
December 2011	Virus corrupts CDC network data
January 2012	**Malicious code infiltrates CDC network; proprietary information stolen**
February 2012	Hackers target critical infrastructure; bring down power grid
March 2012	**Case File: CDC personnel passwords cracked; system infiltrated and data stolen**
April 2012	Hacker steals proprietary information from CDC; sells to foreign company
May 2012	**Case File: Software vulnerability compromises CDC network, foreign group obtains data**
June 2012	CDC cyber attack clean up estimated at $1B
July 2012	Foreign group sabotages surveillance satellite imagery and software
August 2012	**Case File: Removable Media**

Contact: August 2012
Targeted through: Removable Media

Scenario: Employees of a cleared defense contractor attended an industry conference.

While at the conference, venders handed out free product samples, including thumb drives. Several employees took the free thumb drives.

Unknown to the cleared defense contractor, during the conference, a foreign group replaced the vendor's thumb drives with malicious ones. When the employees plugged their new thumb drives into their computers, malicious code was installed allowing the foreign group access to the employees' computers and the contractor's network.

The consequences to both the contractor and military were grave.

Take a look at what the adversary collected from the CDC's network. When you're satisfied with your review of this file, you may move on to the knowledge check and feedback.

Adversary File: Information collected from infiltration through malicious code stored on removable media devices
Information obtained: • CDC network access • DoD program details • Proprietary technology capabilities, limitations, and vulnerabilities

Scenario Question

The defense contractor was targeted via removable media. What is your organization's policy on thumb drives and other removable media? Select your response; then review the feedback that follows.

a. We use removable media; it's convenient and is an efficient way of sharing and transferring information.

b. Removable media is strictly prohibited.

c. I'm not sure.

Scenario Question Feedback

Removable media is an excellent way for adversaries to target CDCs and government agencies. It's essentially a key that allows adversaries into your system. It is for this reason that the DoD has a policy prohibiting the use of removable media.

Choices A and C are risky responses. While removal media may be convenient, its convenience does not outweigh the risk it poses. Your organization should have a policy that details the acceptable and prohibited use of removable media.

Choice B is an appropriate response. Your organization should strictly enforce the DoD policy prohibiting use of removable media.

Take a moment to review indicators of infiltration through removable media and when you are ready, review Countermeasures to learn how to protect against it.

Cyber Attack: Removable Media
Is any type of storage device that can be added to and removed from a computer while the system is running
Technique
Malicious code can be stored in removable media devices. Once the device is activated, the code initiates and infiltrates the user's computer and any network connected to the computer Examples of removable media devices include: • Thumb drives • Flash drives • CDs • DVDs • External hard drives
Indicators
The following is a list of suspicious indicators related to removable media, adversaries and hackers may: • Leave removable media, such as thumb drives, at locations for personnel to pick up • Send removable media to personnel under the guise of a prize or free product trial Effects include, but are not limited to:

- Corrupt files and destroyed or modified information
- Hacker access and sabotaged systems

Countermeasures

The following countermeasures can be taken to guard against removable media vulnerabilities.

Contractors: Follow your organization’s removable media policy

DoD personnel:

- Do not use flash media unless operationally necessary and government-owned
- Do not use any personally owned/non-Government removable flash media on DoD systems
- Do not use Government removable flash media on non-DoD/personal systems
- Encrypt all data stored on removable media
- Encrypt in accordance with the data's classification or sensitivity level
- Use only removable media approved by your organization
- Store in GSA approved storage containers at the appropriate level of classification

The DoD severely restricts or prohibits the use of removable media. Consult your security point of contact (POC) for current policy.

Investigation Wrap Up

Timeline update

The attacks we've just highlighted are all fictitious. These particular events never happened, though cyber attacks similar to those you've just seen happen every day.

Taken individually, these attacks can seem minor. But imagine the effect of the millions of attacks that occur every day. Imagine the amount of information our adversaries can cull because we are not as vigilant as we should be. Imagine how much information they can gather over time. Imagine what they can do with this information.

And imagine the impact to individuals, the companies they work for, and to the country as a whole. The potential impact on national security and our strategic military advantage cannot be overstated.

You can help prevent consequences like these by staying up to date on the kinds of cyber attacks you might encounter, and applying best practices to protect yourself and your network.

Date	Event
August 2011	List of targets obtained via social networking sites
September 2011	Denial of Service (DoS) attack shuts down large CDC
October 2011	Foreign Intelligence Entity (FIE) infiltrates DoD network
November 2011	**Logon credentials stolen in phishing attack; CDC network compromised**
December 2011	Virus corrupts CDC network data
January 2012	**Malicious code infiltrates CDC network; proprietary information stolen**
February 2012	Hackers target critical infrastructure; bring down power grid
March 2012	**Case File: CDC personnel passwords cracked; system infiltrated and data stolen**
April 2012	Hacker steals proprietary information from CDC; sells to foreign company
May 2012	**Case File: Software vulnerability compromises CDC network, foreign group obtains data**

June 2012	CDC cyber attack clean up estimated at $1B
July 2012	Foreign group sabotages surveillance satellite imagery and software
August 2012	**Case File: Foreign group accesses CDC network via corrupted thumb drives**

Conclusion

You have just learned about some of the cyber threats that target DoD employees, cleared defense contractors, and people like you.

You need to be aware of these threats. You need to consider your facility, its technology and programs, and the information you know. How might you be a target?

If you are subject to a suspicious cyber incident, you must report it.

Acknowledgement

Sign the acknowledgement below indicating that you understand your obligation to report all suspicious cyber activities.

I understand that I shall report all suspicious cyber activities and attempts to acquire U.S. export-controlled, restricted, or classified information and technology to my Facility Security Officer (FSO) or security point of contact.

_____

Student Signature