Antiterrorism
Awareness

U.S. ARMY
Army Strong℠

Cyber Threat Vignettes

November 2012

Always Ready, Always Alert
Because someone is depending on you

The Cyber Threat

Ends: Adversaries will use cyberspace to commit espionage, subversion (including insider threat), and sabotage.

Ways: Adversaries gain intelligence and access via cyberspace in order to:

- Recruit insiders (subversion)
- Commit acts of sabotage (stop Army missions; crash networks, electrical power, water facilities)
- Harm Army personnel, families, units, and operations
- Commit criminal actions against Army installations, facilities, units, personnel, and/or family members
- Enable conventional threat capabilities
- Identify U.S. vulnerabilities in weapons systems, facilities, and tactics, techniques, and procedures

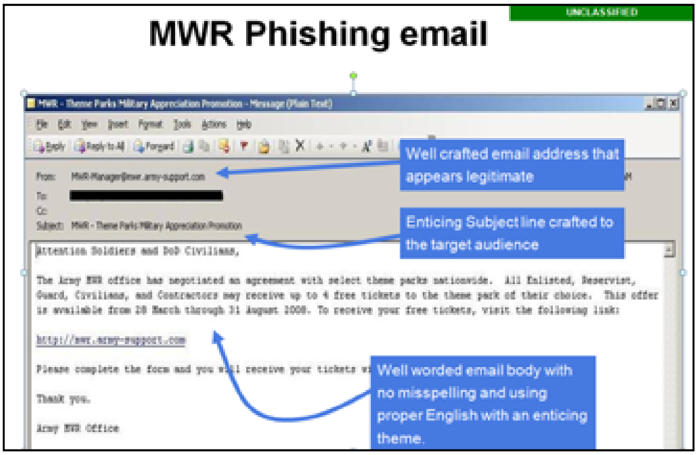
Means: To do this, adversaries tactics include:

- Exploiting people's trust through Phishing attacks
- Infiltrating Malware to perform unauthorized and often surreptitious actions on computers
- Exploiting Social Media through false personas
- Gathering open source information from online postings
- Using infected thumb drives, CDs, DVDs, or other computer memory products to transfer attack mechanisms
- Tampering with cell phones and laptops (both personal and official) especially while personnel are traveling overseas
- Exfiltrating information that enables sabotage and other harmful actions

Phishing

Attack Summary

During an Army phishing exercise, service members assigned to Fort Hood, TX were sent email messages enticing them to click on a counterfeit link to a Morale Welfare and Recreation (MWR) website. The site, which appeared to be authentic, requested that service members provide personal information in exchange for free tickets to an amusement park of their choosing. During this exercise, over 50% of service members contacted fell victim to this phishing scam and provided personal sensitive information in response to the fake email.



MWR Phishing email

UNCLASSIFIED

MWR - Theme Parks Military Appreciation Promotion - Message (Plain Text)

From: MWR-Manager@mwr.army-support.com

To: [redacted]

Cc:

Subject: MWR - Theme Parks Military Appreciation Promotion

Attention Soldiers and DoD Civilians,

The Army MWR office has negotiated an agreement with select theme parks nationwide. All Enlisted, Reservist, Guard, Civilians, and Contractors may receive up to 4 free tickets to the theme park of their choice. This offer is available from 28 March through 31 August 2008. To receive your free tickets, visit the following link:

http://mwr.army-support.com

Please complete the form and you will receive your tickets v

Thank you.

Army MWR Office

Well crafted email address that appears legitimate

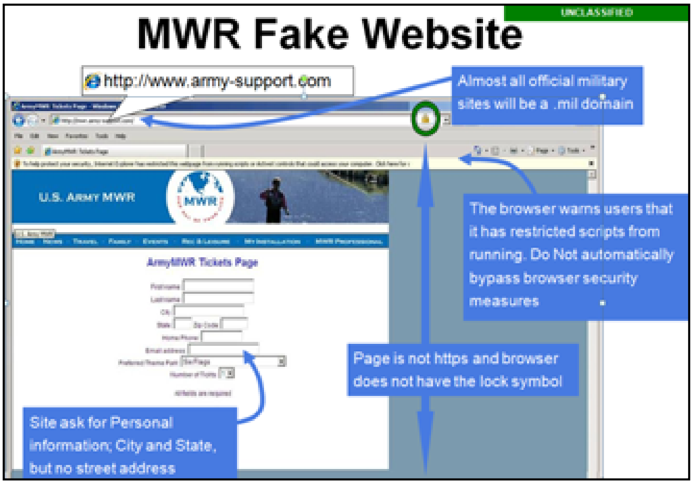
Enticing Subject line crafted to the target audience

Well worded email body with no misspelling and using proper English with an enticing theme.

Figure 1. Army Phishing Exercise Email

How Phishing Works

1. A hacker sends a fake or "spoofed" email that appears to be from a trusted organization
2. The email typically instructs the user to login to verify information and contains a website link
3. The website link in the email directs the user's web browser to a fake website operated by the hacker



MWR Fake Website

UNCLASSIFIED

http://www.army-support.com

Almost all official military sites will be a .mil domain

The browser warns users that it has restricted scripts from running. Do Not automatically bypass browser security measures

Page is not https and browser does not have the lock symbol

Site ask for Personal information; City and State, but no street address

Figure 2. Indicators of a Fake Website

4. The fake website looks exactly like a company's real website and requires the user to log in

5. Any information the user enters into the fake website is immediately delivered to the hacker, which they can use to access the user's accounts

Exercise Scenario Red Flags: The screen shots on the previous page show a phishing email sent during the exercise and the red flags that personnel receiving the email should have caught.

Other Red Flags

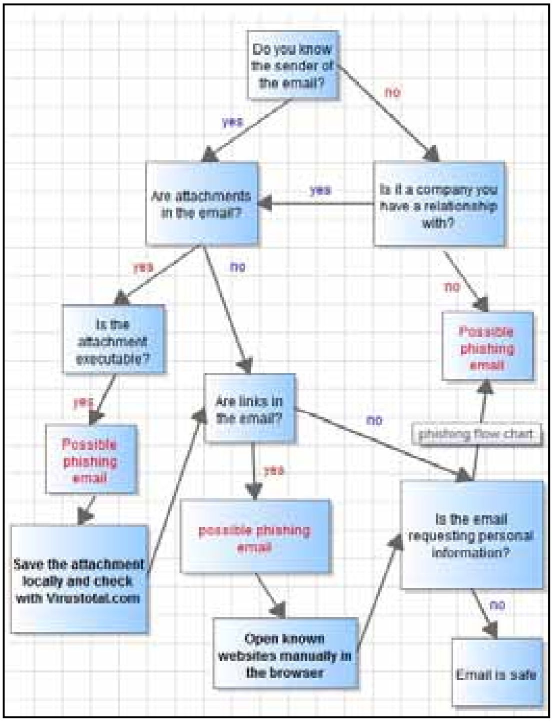

Do you know the sender of the email?
no
yes
Are attachments in the email?
yes
Is it a company you have a relationship with?
yes
no
no
Is the attachment executable?
Possible phishing email
yes
Are links in the email?
no
phishing flow chart
Possible phishing email
yes
Save the attachment locally and check with Virustotal.com
possible phishing email
Is the email requesting personal information?
no
Open known websites manually in the browser
Email is safe

Figure 3. Email Authentication Screening Process

- Almost all official military sites will be a .mil domain
- Almost all official government sites will be a .gov domain
- Phishing emails usually do not address the recipient by name
- Look for a closed padlock icon in the web browser's status bar indicating a legitimate site
- Any unsolicited communication regarding any account you do not have
- Unsolicited or unexpected email attachments
- Requests for you to send your username and/or password or other personal data
- Obvious spelling, grammar, or factual errors
- An overwhelming emphasis on urgency
- Anything "too good to be true"
- FROM addresses that do not match the REPLY address
- Hyperlinked URLs whose targets do not match the link text (for example: the text for the link may read as www.paypal.com but when you click on the link it takes the user to a phony site such as www.paypal.net)
- Hyperlinks that use shortened URLs (for example: an email containing a link supposedly for Army Knowledge Online listed as www.ako.mil vice https://akologin.us.army.mil)

- Hyperlinks with very long and complex targets, even to "legitimate" websites (for example, the actual link to AKO would be https://www.us.army.mil/suite/login/login.fcc?TYPE=33554433&REALMOID=06-56ac however most users do not see these full addresses; any address excessively long should initially be suspicious)

Phishing Countermeasures / Key Lessons

- Watch out for phishing; email addresses can be easily faked
- Do not disclose any information
- Do not open suspicious emails or email attachments; they may contain malware that will infect your computer and network
- Do not click on suspicious links in emails or popup windows
- Do your own research to determine the validity of the email
- Do not do anything they ask, in the way they want you to do it
- Do not reply, react, or contact the website's support listed in the suspicious email
- Do not call telephone numbers provided in suspicious emails
- Delete suspicious emails
- If you are using a home computer that has been compromised via a phishing email, change your password immediately at the real website:
    - Type the website name in your browser's address bar
    - Sign into your account and click the "user profile" or "change password" link
    - Follow the website's instructions to change your account information and password
    - Click the "contact us" link found on most websites and inform them about the phishing attack you just experienced
- If you are using a government computer, contact your Information Assurance (IA) Officer or your servicing Network Enterprise Center (NEC)

Protection Principles

- Educate users about phishing to help prevent successful phishing attacks
- No matter what the potential phishing email tells you, do not rush yourself; if someone is initiating contact with you, taking time out of your day, they can stand to wait a few

minutes (or even hours) while you sort things out for yourself and decide what you are going to do

- If you receive an email you believe to be fake, report it your IA Officer or your servicing NEC; assume that you were not the only person to receive the email

Potential Impact

If a computer user falls victim to a phishing attack, the user compromises their personal and/or professional information and potentially subjects their computer to an upload of malware that could allow a hacker access to the user's home computer and/or unit's computer network.

When a hacker has access to a user's personal computer, the hacker may be able to commit identity theft, withdraw money out of the user's bank accounts, and/or hijack the user's computer so it can be used for illicit purposes.

When a hacker has access to an Army computer network, the hacker may be able to disrupt unit command and control, as well as exfiltrate sensitive information that compromises the unit's mission (such as real world schedules and movements, weapon system vulnerabilities, and upcoming missions).

The Robin Sage Experiment: December 2009

"Do You Know Who You're Friending?"

Attack Summary

Robin Sage was a fictional American cyber threat analyst created in December 2009 by Thomas Ryan, a security specialist and "White Hat" hacker from New York, as part of an effort to expose weaknesses in the nation's defense and intelligence communities. Robin Sage, according to her profiles on Facebook and other social-networking websites, was an attractive, flirtatious 25-year-old woman working as a "cyber threat analyst" at the U.S. Navy's Network Warfare Command. Within less than a month, she amassed nearly 300 social-network connections among security specialists, military personnel, and staff at intelligence agencies and defense contractors. Her connections on LinkedIn included men working for the Joint Chiefs of Staff, the National Reconnaissance Office, a senior intelligence official in the U.S. Marine Corps, the chief of staff for a U.S. congressman, and several senior executives at defense contractors. Through these connections, Thomas Ryan gained access to email addresses and bank accounts, learned the location of secret military units based on soldiers' Facebook photos and connections between different people and organizations, was given private documents for review, and was offered to speak at several conferences.

Red Flags:

- Robin Sage is code name of an U.S. Special Forces military exercise
- At the age of 25, Robin Sage claimed to already have had 10 years of professional experience in the cyber security field
- There was no such job as "cyber threat analyst" at the Naval Network Warfare Command
- The fictional character "Robin Sage" was not dressed like a government professional in any of her profile photographs
- Several of those "she" tried to befriend attempted to verify her identity using her profile phone number, checking email addresses outside of the social networking sites, or using the Massachusetts Institute of Technology alumni network to confirm her identity; every piece of information included in her profile was false

Key Lessons

- The experiment revealed important vulnerabilities in the use of social networking by people in the national security field
- Up to 20% of all traffic on DoD computer networks involves social networking on public sites, which are unprotected and potentially harmful
- Although many of the security breaches in the Robin Sage incident were unintentional, in the intelligence field, many of the most important leaks are inadvertent
- Many people entrusted with vital and sensitive information will share this information readily with third parties when asked
- Be careful who you allow into your social network; if you do not know a person who attempts to connect with you, investigate who they are and why they want to join your social network
- Do not offer personal or professional information, such as email addresses, which could open yourself to a phishing or spear phishing attack
- Do not open email attachments, hyperlinks, or URLs from anyone whom you do not know personally
- Train yourself, your Soldiers, your employees, and family members on responsible use of the Internet at work and home

Protection Principles

- Educate the community on safe internet practices, with an emphasis on social networking; be careful who you allow into your social network
- If you do not know a person who attempts to connect with you, investigate who they are and why they want to join your social network; do not be deceived by attractive photos which are easily harvested from internet websites
- If you receive a social networking invitation that you believe is suspicious, do not accept the invitation; report suspicious activity to your unit leadership, command S-2/G-2, or your installation U.S. Army Counterintelligence office

Potential Impact

Those entrusted with vital and sensitive information could unknowingly compromise both their personal information and national security if an adversary employs similar tactics as the Robin Sage experiment.

Website Woes

Summary

An Army command created a forum on its unit webpage to allow contractors to voice grievances about an active contract. The intent was to promote transparency between the government and the contract. The forum was not password protected and was accessible to the public. This presented a problem because one of the contracts discussed included information about a classified facility currently under construction in a foreign country. The forum was operational for some time before it was brought to the attention of Operations Security (OPSEC) personnel. The website information that was accessible and vulnerable to compromise and exploitation included: schematics of the facility under construction, protective measures incorporated into its structure, and equipment it would contain. After an OPSEC review, the forum was relocated to a password protected domain and content of the site was screened for sensitive or classified information.

Results

- Critical information and security concerning the construction, mission, and protection of a sensitive site overseas were compromised for the sake of contractual transparency
- The command did not conduct website reviews and did not consider OPSEC measures when establishing the site
- Although there is no proof suggesting that collection occurred in this instance, adversaries collect at least 80% of their information from open sources

Key Lessons

- Commands should conduct regular reviews of content on unit webpages in order to identify potential leaks of critical information
- Webpage developers and those who post information on websites must practice OPSEC and attend a course on OPSEC Web Content
- Contracts and personnel advertisements that reveal security and/or access requirements, special skills, or familiarity with sensitive equipment or equipment associated with military operations can provide indicators of a unit or facility’s mission; this information should be protected

Protection Principles

- Educate webmasters of the mandatory requirement for OPSEC reviews on unit web pages and ensure that all Army web sites are registered
- Protect open forums discussing information that pertains to capabilities, actions, limitations, and intentions with at least a login and password
- Review unit web pages and ensure they are OPSEC compliant
- Verify there is a valid mission need to disseminate information on unit websites
- Limit details about the organization's specific capabilities, readiness, and operational matters

Potential Impact

Official Department of Defense webpages may contain vital and sensitive information that the adversary can collect to compromise the safety and security of the United States.

Dangers of Posting to Social Media Sites

Summary

Recently, an Army garrison commander cancelled classes at a school located on the installation due to inclement weather, but did not close the installation. As a result, parents had to find ways to take care of their children and still work. One parent used a social media site to complain about the situation. In her complaint, she discussed the fact that her children were home alone because she was at work and the other parent was deployed. However, using information from the parent's profile, the family's home address could be located through people search engines (veromi.com, pipl.com, or zabasearch.com). In addition, more than 900 registered sex offenders lived in the local area. Although the children at home were of legal age to be home alone, the information from the post revealed an address and window of opportunity. Besides increasing the risk to her children, the parent's social media post also revealed a window of opportunity for theft.

Results

- Critical information concerning family, lifestyle, and location was made available on social media websites to adversaries
- Family, personal, and professional lives could have been endangered through the open forum
- The apparent desire to be "heard" combined with the lack of knowledge of the risks inherent with the use social media sites presented unnecessary risk to family members

Key Lessons

- Consider the secondary impacts of posting personal information on social media sites
- Do not assume that only individuals you know are reading your postings
- Update your social media privacy and account settings; don't rely on default settings to secure your posts
- Balance your unit's use of social networking against the risk of providing information to criminals and adversaries

Protection Principles

- Educate your workforce and families of the dangers of social media; it is not about avoiding it, but using it intelligently

- Regularly check and if necessary, update privacy settings and account settings on social media websites
- Conduct regular Operations Security (OPSEC) reviews of official Department of Defense social media webpages for posted comments by service members and their families

Potential Impact

A parent's reaction to a garrison commander's decision to close schools could have placed the spouse's unit and family at risk. Assume adversaries are monitoring social websites. Before posting anything, assume the information is available to adversaries including terrorists, and criminals.

The Theft of U.S. Military Technology Information

Summary

Since World War II, the U.S. military has maintained a technological "overmatch" or advantage over its adversaries. This advantage has largely been due to the increased amount of time, effort, and money the U.S. has invested in the research, development, and production of advanced weapon systems. However, over the past 14 years, unpatched computer networks, malware, and successful phishing emails have enabled unauthorized access to U.S. Government and U.S. Defense contractor unclassified networks, resulting in alarming increases in state-sponsored intrusions and data exfiltration. Unclassified but sensitive research and development information shared collaboratively between U.S. government, private industry, and academia have been stolen from our information technology networks and obtained by foreign governments. This stolen information may have provided our adversaries with an advantage over the U.S. in the development of advanced weapons systems.

Are we providing foreign militaries an advantage in advanced weapons systems development?

Nothing illustrates this claim better than a comparison of the U.S. Air Force F-22 Raptor and the People's Republic of China's (PRC) newest stealth fighter, the J-20. Similar features between the J-20 and the F-22 include:

- A curvy aerodynamic design shape that minimizes flat surfaces, preventing radar from cleanly bouncing back to the source.
- Angular air intakes that are positioned so that they don't form corner reflectors.
- The use of materials other than metal that appear to be better at absorbing radar.
- The potential ability to fly at supersonic speeds without using afterburners; this feature, referred to as super cruise, lowers the aircraft's infrared signature significantly.

U.S. Air Force F-22 Raptor

People's Republic of China RC J-20 Stealth Fighter

Key Lessons

- Adversaries gain access to U.S. computer networks through the employment of malware that exploits network system vulnerabilities. To protect our networks, Network Enterprise Centers (NEC) regularly and frequently patch operating systems and software application to mitigate system vulnerabilities. In addition, everyone has a part to play in ensuring that Army networks stay secure and our national assets are protected. Network users must be conscious of the risks and take measures to prevent falling prey to phishing attacks. Users must also stay away from attractive, but malicious websites that contain harmful malware that enables adversary exploitation of our networks.

- The development and production of the F-22 Raptor was expensive and took many years of research and development. The PRC may have obtained information from government and private industry networks, allowing them to produce a similar stealth fighter in significantly less time and at much less expense.

Protection Principles

- Educate users about phishing, to help prevent successful phishing attacks.
- Delete suspicious emails without opening them. Do not click on suspicious links in emails or popup windows. Do not call telephone numbers provided in suspicious emails, and do not disclose any information.
- Stay alert to spear phishing emails - if you have access to sensitive information, you may be specifically targeted.
- Encrypt all sensitive information transmitted over unclassified networks or stored on unclassified servers. As appropriate, use classified networks.
- If you receive an email you believe is fake, report it your Information Assurance Officer or your servicing NEC. Assume that you were not the only person to receive the email.

Potential Impact

The Army will increasingly face adversaries who will exploit our networks to obtain U.S. advanced technological information. With the inevitable reduction of the U.S. defense budget in the upcoming years and the increased defense budgets of our potential adversaries, protection of our sensitive defense information has never been more critical. Any Research, Development, Test, and Evaluation (RDT&E) data obtained by adversaries from U.S. networks may bolster adversary warfighting capabilities while potentially revealing U.S. warfighting vulnerabilities.

The Stuxnet Computer Worm

Attack Summary

Stuxnet was a highly sophisticated computer worm that was designed to target specific Supervisory Control and Data Acquisition Systems (SCADA), which are used to control and monitor specific industrial or technology processes. Stuxnet became well known after a June 1st, 2012 article in The New York Times (NYT) reported that Stuxnet successfully led to the failure of uranium enrichment centrifuges at the Natanz nuclear facility in Iran in November 2010, thus disrupting Iranian development of nuclear weapons. The most successful feature of the Stuxnet worm was its ability to “trick” industrial control sensors into failing to recognize abnormalities, thus failing to shut down the affected systems and maximizing harm. The NYT article further revealed that the Stuxnet worm was probably delivered to the Natanz facility through a human Intelligence (HUMINT) method, either by an unknowing employee or a recruited spy, on a USB thumb drive. Stuxnet did not terminate after the attack, however, and spread harmlessly via the internet to over six countries, including Iran, Indonesia, India, Azerbaijan, the United States, and Pakistan. Information Technology expert David Gerwitz, director of the U.S. Strategic Perspective Institute, described Stuxnet as “a watershed event in weaponization, ushering in a new era and type of weapon that will have a profound effect on the theater of war.” Cyber security officials at the U.S. Department of Homeland Security are concerned about how Stuxnet could be downloaded online and modified by cyber hackers to target new systems.

Key Lessons

- Cyber war is rapidly evolving from the defense of information technology systems to the asymmetric battlespace where offensive cyber sabotage (cybertage) on a large scale can affect entire national industries and economies.

- Stuxnet is a form of malware that initially spread indiscriminately via Microsoft Windows; however, the worm includes a highly specialized malware payload designed to lie dormant until it reaches a specific target.

Protection Principles

- Never open unknown or suspicious email attachments. Remember, Stuxnet was originally designed to enter a system via Microsoft Windows software.
- Avoid using pirated CDs and DVDs on your home and work computers, especially those purchased overseas—they may carry suspicious code, viruses, and worms.
- Because malware (like Stuxnet) can spread easily, DOD has prohibited all military and civilian personnel from bringing personal CDs, thumb drives, and DVDs to work and inserting them into government computers.
- Even “closed,” well-guarded government computer systems have vulnerabilities. Individual awareness is crucial. Treat your government computer like a weapons system that must be protected.
- Be aware that you could be a target for cyber espionage. Immediately report any “gifted” thumb drives, CDs, DVDs, or cyber related products, regardless of how official they appear.
- If you travel overseas, keep your cell phone and laptop with you at all times, or do not bring them with you. Immediately report any tampering to your unit or command S-2/G-2, or your installation U.S. Army Counterintelligence office.
- If you believe that your government computer has been infected with malware, contact your local Information Assurance Officer and servicing Network Enterprise Center (NEC).

Potential Impact

Opening unknown or suspicious email attachments or use of unauthorized computer memory products could seriously damage or compromise Army missions, DOD information systems, U.S. industry, or U.S. critical infrastructure.

Insider Threat

"Beware the Insider Threat"

"More damage is being done by insiders than by foreign spies."

– Dr. Stephen Cambone, Undersecretary of Defense for Intelligence

Summary

Both the U.S. public and private sectors have long been aware of the "insider threat" to information systems, databases, and computer network infrastructure. The insider threat, including fraud, theft of intellectual property, sabotage, inadvertent violation of security and information technology policies, and the unauthorized release of personal or classified information, has had major adverse impacts on the defense, telecommunications, public health, transportation, banking, finance, chemical, energy, food service, and shipping industries. In the digital age, individuals who previously had to photocopy and smuggle documents to take them from their work areas can now simply email or download them onto portable devices or databases. Also, disgruntled individuals with computer access can easily cause disproportionate harm to the entire organization.

Consider the following recent examples:

- An engineering firm suffered $10 million in property damage and lost a significant amount of data after a disgruntled computer-system administrator crashed the company server and stole backup files. As a result, the firm was forced to lay off eight employees and lost several clients.
- In 1997, a former employee of a Fortune 500 company crashed five of the company's eight servers which shut down operations for two days. The company lost critical information on the affected servers. The individual was a temporary hire who worked in the company's information technology department, and according to government affidavits, utilized hacking and sabotage programs that he downloaded from internet open sources.
- An employee from a large computer corporation tampered with performance test results and transferred confidential information outside the company. As a result, company executives were forced to cancel the release of a product, costing the company millions of dollars and damaging its reputation and competitiveness.

- In 2012, five individuals and five companies were charged with economic espionage and theft of trade secrets, which were passed to companies controlled by the government of the People's Republic of China.

Red Flags

- Anger, disgruntlement, disloyalty, extreme ideology, addictive behaviors, behavioral disorders, separation from loved ones, thrill-seeking, or a combination thereof, can cause Army personnel to betray positions of trust and responsibility by leaking or downloading sensitive or classified information to unauthorized sources or individuals, or by sabotaging information systems.
- Individuals who work odd hours without authorization, email government information home, copy government material unnecessarily, install personal software or hardware on their government computers, use unauthorized thumb drives or disks, or take short trips to foreign countries for unexplained reasons may be engaging in insider threat activities.

Key Lessons

- Cyber-security compromises caused by an insider threat often cause the most damage among all types of cyber-security incidents.
- Foreign and domestic economic espionage facilitated by the insider threat is a significant and growing threat to America's defense, as well as its economic health and security.

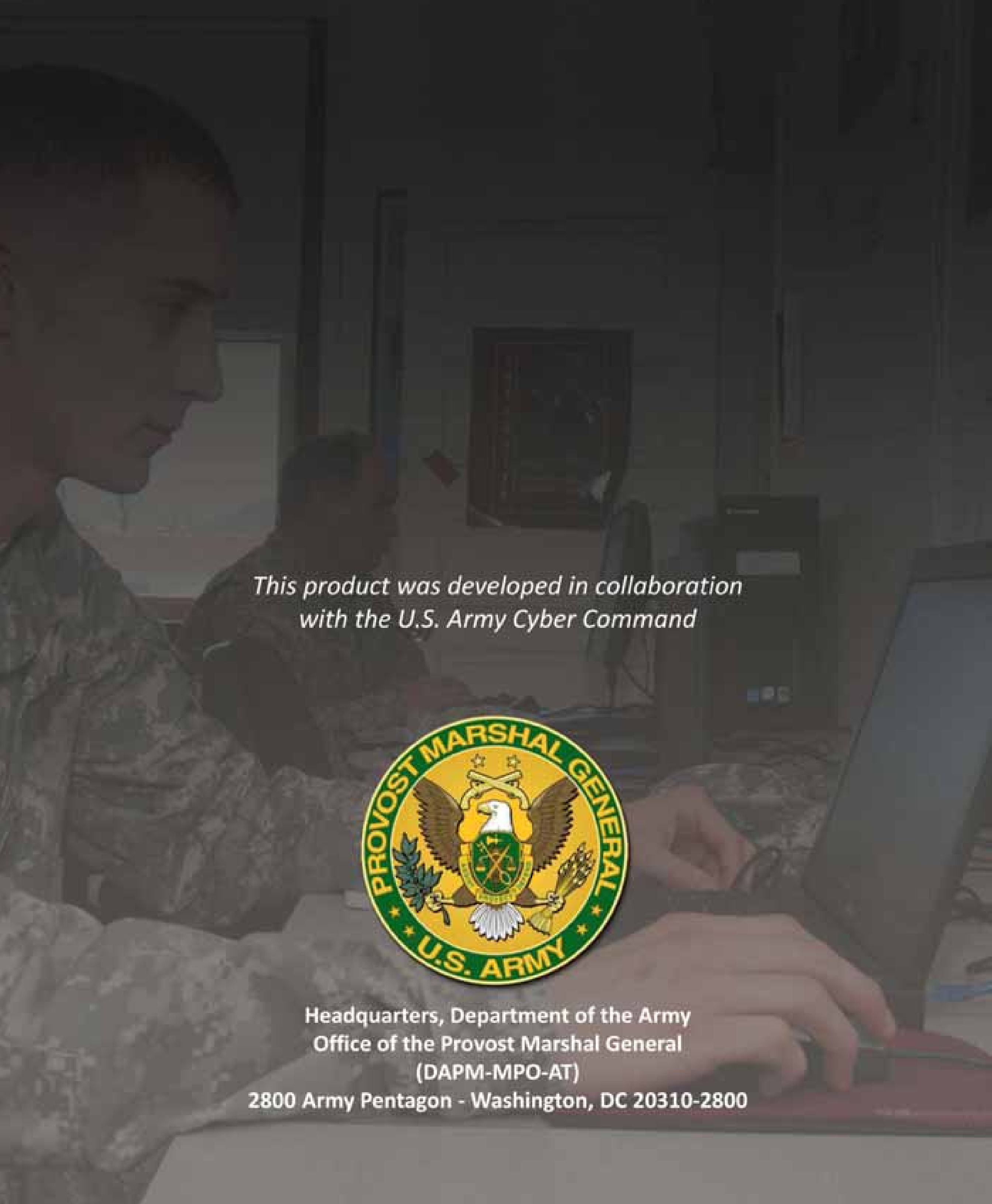
Protection Principles

- Army leaders must know the personnel records and performance backgrounds of their subordinates to manage risk and project assignments accordingly.
- Army units must ensure that all personnel know the warning signs of the insider threat; regular Antiterrorism and OPSEC training are perfect forums for this education.
- Follow the concept of "need-to-know." Authorized holders of classified information should make the determination whether or not a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
- Undertake a concerted, reasonable effort to limit computer and classified access to those personnel who do not need them to perform their regular duties.
- Establish a command climate that enforces security measures and informs Army personnel about serious consequences for infractions.

- Be aware of national and Army level efforts to address the insider threat. For example, in October 2011, the President of the United States signed an Executive Order establishing an Insider Threat Task Force to develop a government wide program to deter, detect, and mitigate insider threats.
- Army personnel at all levels should be vigilant for behaviors and attitudes that might identify an individual as an insider threat. Studies indicate that a behavioral pattern of tardiness, arguments with co-workers, and poor job performance often precede insider threat activities.
- Designated information systems security managers, law enforcement officials conducting police investigations under legal authorities, and counterintelligence officers engaged in or supporting national security investigations or inquiries, monitor information systems in accordance with applicable laws, statues, and policies. Communications Security (COMSEC) monitoring is used as an OPSEC tool (IAW AR 380-53) to monitor security violations on government information systems.
- Implement and follow strict password and account management policies and practices; insider threat provocateurs often steal credentials and mask their activities behind the identities of other personnel.
- Implement secure backup and recovery processes in the event of sabotage.
- If you suspect someone of being an insider threat, report your suspicions to your unit security officer or and supporting counterintelligence unit.

Potential Impact

Insider threat activity negatively impacts U.S. national security, jeopardizes American military personnel and government civilians, and can cause serious repercussions for U.S. international policy and economic well-being.



This product was developed in collaboration with the U.S. Army Cyber Command

Headquarters, Department of the Army
Office of the Provost Marshal General
(DAPM-MPO-AT)
2800 Army Pentagon - Washington, DC 20310-2800