CHAPTER 16: CYBER ATTACK

2022 PLAN UPDATE

Chapter 16: visual and thematic updates were included throughout the chapter, including updates to fonts, colors, and the addition of a cover page.

Page 16-1: Updated Sections 16.1.1 thru 16.1.5 to make sure the definitions utilized for the groups: national governments, terrorists, industrial spies and organized crime, hacktivists, and hackers are up to date.

Page 16-6: Updated Section 16.3.2 with the HIRA ranking from the State and local level. The State ranks Cyber Attack as "medium-low" risk and the County ranks Cyber Attack as "High" risk.

Page 16-6: Added narrative regarding the February 2021 ransomware attack at TidalHealth, Bayhealth, which resulted in a massive data breach f health information.

Page 16-6: Section 16.3 Mitigation Efforts was updated to include information about the County's Information Technology Networking Academy (CISCO) program at the County's Technical Highschool.

Page 16-7: Updated the Section 16.4 Mitigation and Responding to a Cyber Attack, added two hyperlinks to resources.

Page 16-9: Section 16.5 Future Conditions has been added to this chapter. The section discusses present and past cyber incident trends to glean how cyber attacks will change in the near future.

Chapter 16: Cyber Attack

16.1 Hazard Profile

According to the Department of Homeland Security – Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect against these threats, it is necessary to create a secure cyber-barrier around the Industrial Control System (ICS). Though other threats exist, including natural disasters, environmental, mechanical failure, and inadvertent actions of an authorized user, this discussion will focus on the deliberate threats mentioned above.

For this discussion, deliberate threats will be categorized consistent with the remarks in the Statement for the Record to the Joint Economic Committee by Lawrence K. Gershwin, the Central Intelligence Agency's National Intelligence Officer for Science and Technology, 21 June 2001. These include: national governments, terrorists, industrial spies, organized crime groups, hacktivists, hackers, and the GAO Threat Table. Activities could include espionage, hacking, identity theft, crime, and terrorism.

16.1.1 National Governments

National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm U.S. interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to U.S. critical infrastructures.

The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures.

Their goal is to weaken, disrupt or destroy the U.S. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the US economy, full scale attack of the infrastructure when attacked by the U.S. to damage the ability of the US to continue its attacks.

16.1.2 Terrorists

Traditional terrorist adversaries of the U.S., despite their intentions to damage U.S. interests, are less developed in their computer network capabilities and propensity to pursue cyber

means than are other types of adversaries. They are likely, therefore, to pose only a limited cyber threat. Since bombs still work better than bytes, terrorists are likely to stay focused on traditional attack methods in the near term. We anticipate more substantial cyber threats are possible in the future as a more technically competent generation enters the ranks.

Their goal is to spread terror throughout the U.S. civilian population. Their sub-goals include: attacks to cause 50,000 or more casualties within the U.S. and attacks to weaken the U.S. economy to detract from the Global War on Terror.

16.1.3 Industrial Spies and Organized Crime Groups

International corporate spies and organized crime organizations pose a medium-level threat to the US through their ability to conduct industrial espionage and large-scale monetary theft as well as their ability to hire or develop hacker talent.

Their goals are profit based. Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and gain access and blackmail affected industry using potential public exposure as a threat.

16.1.4 Hacktivists

Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-U.S. motives. They pose a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause.

16.1.5 Hackers

Although the most numerous and publicized cyber intrusions and other incidents are ascribed to lone computer-hacking hobbyists, such hackers pose a negligible threat of widespread, long-duration damage to national-level infrastructures. The large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as critical U.S. networks and even fewer would have a motive to do so. Nevertheless, the large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage or loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled and malicious hacker attempting and succeeding in such an attack.

In addition, the huge worldwide volume of relatively less skilled hacking activity raises the possibility of inadvertent disruption of a critical infrastructure.

For the purposes of this discussion, hackers are subdivided as follows:

- Sub-communities of hackers

- Script kiddies are unskilled attackers who do NOT have the ability to discover new vulnerabilities or write exploit code and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages.
- Worm and virus writers are attackers who write the propagation code used in the worms and viruses but not typically the exploit code used to penetrate the systems infected. Their goal is notoriety. Their sub-goals are to cause disruption of networks and attached computer systems.
- Security researcher and white hat have two sub-categories; bug hunters and exploit coders. Their goal is profit. Their sub-goals are to improve security, earn money, and achieve recognition with an exploit.
- Professional hacker-black hat who gets paid to write exploits or actually penetrate networks; also falls into the two sub-categories-bug hunters and exploit coders. Their goal is profit.

16.2 Nature Of The Computer Security Community

Hackers and researchers interact with each other to discuss common interests, regardless of color of hat. Hackers and researchers specialize in one or two areas of expertise and depend on the exchange of ideas and tools to boost their capabilities in other areas. Information regarding computer security research flows slowly from the inner circle of the best researchers and hackers to the general IT security world, in a ripple-like pattern.

16.2.1 GAO Threat Table

Table 16-1, below, is an excerpt from NIST 800-82, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security," provides a description of various threats to CS networks:

Table 16-1: Threats to CS Networks

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.

Table 16-1: Threats to CS Networks	
Threat	**Description**
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power - impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, most hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434..[i]

16.3 Mitigation Efforts

16.3.1 2022 National Cybersecurity Legislation

At least 40 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity. Twenty-four states enacted at least 41 bills in 2022 so far, as indicated in boldface in the list below. The most common enactments in 2022 will:

- Require government agencies to implement cybersecurity training; to set up and follow formal security policies, standards and practices; to have incident response plans in place; to provide mandatory training for employees; and to report security incidents, including ransomware attacks.
- Provide funding for cybersecurity programs and practices in state agencies, local governments and schools. (Not all cybersecurity appropriations are listed here, although significant funding or funding for specific statewide mandates or state projects may be listed.)
- Mandate security practices related to elections.
- Establish or support programs or incentives for cybersecurity workforce training and education programs.

16.3.2 Local Efforts

The State ranks Cyber Attack as "medium-low" risk in the 2021 State Hazard Mitigation Plan. Somerset County ranks the Cyber Attack hazard as "high" risk for the County, possibly on the heels of a massive data breach reported at TidalHealth, Bayhealth in February of 2021. According to a Delmarva Now news report, the target of the ransomware attack was CaptureRx, a health IT company that helps hospitals manage certain drug programs. In response, TidalHealth reached out to each patient impacted within its own health system, and the organization internally addressed the issue with a third-party provider.[ii]

Security measures currently in place for Somerset County are physically secure with video monitoring and include the following:

- Firewalls at each remote location, which:
  - Monitor network,
  - Block incoming connections from known threats, and
  - Block connections to and from unsafe countries.
- Cisco Email Security, which includes:
  - Email malware protection, and
  - Scans all incoming emails for phishing attempts.
- ESET Antivirus, which provides:
  - Real time virus scanning,
  - Scans emails locally for infections, and
  - Exploit/Botnet blocking.
- Cisco Umbrella, conducts:

  - Web filtering,
  - Web traffic reporting, and
  - Protect against known malicious websites.
- Group Policies, which conducts:
  - Software file restriction,
  - Path restriction, and
  - User restriction.
- Shadow Protect, which provides:
  - System backup and recovery,
  - Remote location backups,
  - Full backups daily, and
  - Incremental backups hourly.

Somerset County also offers a cybersecurity operations program via the Information Technology Networking Academy (CISCO) program at the County's Technical Highschool. The goal of the program is to "prepare students for today's technology-based careers and industries, with relevant instruction in all aspects of personal computing including: multimedia telecommunications, technical writing, end-user information systems, troubleshooting, and hardware maintenance. The information technology degree is designed to provide the flexibility to integrate specialized technology and skills into a customized program.

16.4 Mitigating and Responding to a Cyber Attack

16.4.1 Before A Cyber Incident

You can increase your chances of avoiding cyber risks by setting up the proper controls. The following are things you can do to protect yourself, your family, and your property before a cyber incident occurs.

- Only connect to the Internet over secure, password- protected networks
- Do not click on links or pop-ups, open attachments, or respond to emails from strangers.
- Always enter a URL by hand instead of following links if you are unsure of the sender.
- Do not respond to online requests for Personally Identifiable Information (PII); most organizations – banks, universities, companies, etc. – do not ask for your personal information over the Internet.
- Limit who you are sharing information with by reviewing the privacy settings on your social media accounts.
- Trust your gut; if you think an offer is too good to be true, then it probably is.

Password protect all devices that connect to the Internet and user accounts.

- Do not use the same password twice; choose a password that means something to you and you only; change your passwords on a regular basis.
- If you see something suspicious, report it to the proper authorities.
- Familiarize yourself with the types of threats and protective measures you can take by:

- Sign up for the United States Computer Emergency Readiness Team (US-CERT) mailing list.
- Sign up for the Department of Homeland Security's Stop.Think.Connect. Campaign and receive a monthly newsletter with cybersecurity current events and tips.

16.4.2 During A Cyber Incident

Immediate Actions

- Check to make sure the software on all your systems is up to date.
- Run a scan to make sure your system is not infected or acting suspiciously.
- If you find a problem, disconnect your device from the Internet and perform a full system restore.
- If in a public setting immediately inform a librarian, teacher, or manager in charge to contact their IT department.
- Report the incident to your local police so there is a record of the incident. You may also contact federal agencies able to aid and investigate the incident:
  - FBI field offices and Internet Crime Complaint Center
  - National Cyber Investigative Joint Task Force or call 855-292-3937
  - United States Secret Service
  - National Cybersecurity and Communications Integration Center or call 888-282-0870
  - U.S. Computer Readiness Team

At Work

- If you have access to an IT department, contact them immediately. The sooner they can investigate and clean your computer, the less damage to your computer and other computers on the network.
- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be on alert for any suspicious or unusual activity.

Immediate Actions if your Personally Identifiable Information (PII) is compromised:

PII is information that can be used to uniquely identify, contact, or locate a single person. PII includes but is not limited to:

- Full Name
- Social security number
- Address
- Date of birth
- Place of birth
- Driver's License Number

- Vehicle registration plate number
- Credit card numbers
- Physical appearance
- Gender or race

If you believe your PII is compromised:

- Immediately change all passwords; financial passwords first. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Contact companies, including banks, where you have accounts as well as credit reporting companies.
- Close any accounts that may have been compromised. Watch for any unexplainable or unauthorized charges to your accounts.

16.4.3 After a Cyber Incident

- File a report with the local police so there is an official record of the incident.
- Report identity theft to the Federal Trade Commission.
- Contact additional agencies depending on what information was stolen. Examples include contacting the Social Security Administration if your social security number was compromised, or the Department of Motor Vehicles if your driver's license or car registration has been stolen.
- Report online crime or fraud to your local United States Secret Service (USSS) Electronic Crimes Task Force or the Internet Crime Complaint Center.
- For further information on preventing and identifying threats, visit US-CERT's Alerts and Tips page.

16.5 Future Conditions

Technology will only become more complex in the future, and current trends show people interacting with each other online more frequently and in diverse ways. This means that cyber attacks are no longer events that only effect high-level organizations and companies; anyone who utilizes online services can be a target.

According to an article by Bitdefender[iii], data gathered by Microsoft (formerly RiskIQ) suggests cybercrime costs organizations $2.9 million every minute. Research suggests that things are only going to get worse. The article makes the following statements regarding present and future trends in the cybercrime sphere:

1. Cybercrime has been on an ascending pace since the widespread adoption of commercial and residential Internet

   a. There is a sharp increase in the number of cyber-attacks, there is also a growing diversity in the types of cyber threats, making it difficult to effectively protect important data moving forward.
2. Ransomware attacks have become mainstream with the proliferation of ransomware-as-a-service, where cyber-criminal groups create and market ransomware to affiliates
3. Data breaches have become the new normal as attackers are capitalizing on illegally gained access to steal customer information, intellectual property or trade secrets to be sold or exchanged in specialized underground forums.

While most sectors are vulnerable to these cyber-attacks, it is predicted that sectors such as hospitals, critical infrastructure, transportation, and education will experience an increase in cyber incidents in the future, as they are already frequently targeted. According to the CyberPeace Institute, hospitals specifically need to exercise precautions, as health records are "low-risk high reward" targets for criminals. Ransomware attack on the healthcare industry occurred at a rate of four incidents per week in the first half of 2021, based on available reporting.[iv]

Local governments, departments, businesses, and information technology professionals will need to work together and adopt new protective strategies. Educating people and employees on how to spot suspicious emails or links and then providing them a means to report suspicious activity is an important step in reducing cyber attacks moving forward.

[i] Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434. Washington, D.C.: May 2005.
[ii] www.delmarvanow.com/story/news/local/maryland/2021/06/23/tidalhealth-hit-data-breach-targeted-capturerx/5322228001/
[iii] businessinsights.bitdefender.com/what-are-the-biggest-cyber-threats-of-the-future
[iv] cyberpeaceinstitute.org/news/if-healthcare-doesnt-strengthen-its-cybersecurity-it-could-soon-be-in-critical-condition/