SBIR·STTR
America's Seed Fund™
POWERED BY SBA

COURSE 10, TUTORIAL 2

INTRODUCTION TO CYBERTHREATS

The objective of this tutorial is to increase your awareness of the various types of cyberthreats and lay the foundation for your company's cybersecurity plan. Cybersecurity, also referred to as information technology or IT security, is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Ensuring cybersecurity requires coordinated efforts throughout an information system.

One of the most problematic elements of cybersecurity is the quick and constant evolving nature of security risks. Cybercriminals are rapidly evolving their hacking techniques. They attack quickly, making timely security more critical than ever. Consequently, one of the first actions involved in initiating an effective cybersecurity strategy is to gain an understanding of the threat.

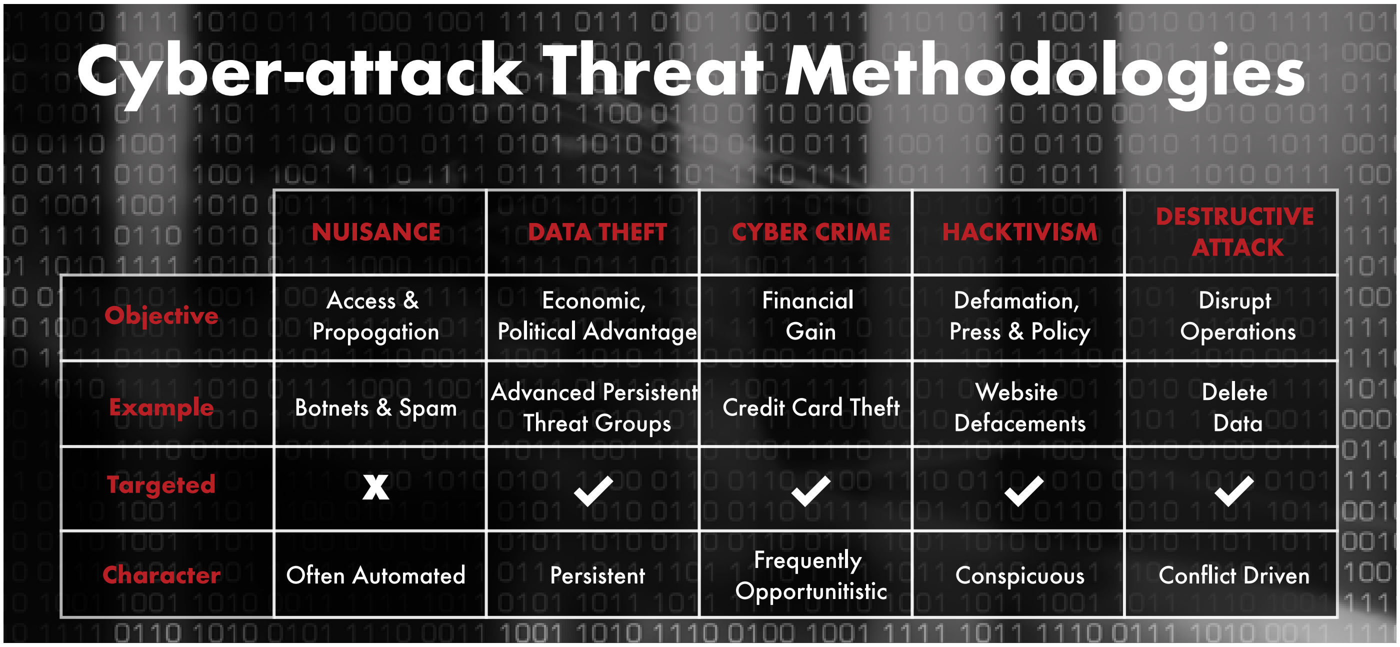
WHAT IS A CYBERATTACK?

A cyberattack is "an attack initiated from a computer against a website, computer system or individual computer … that compromises the confidentiality, integrity or availability of the computer or information stored on it. Cyber attacks take many forms."[1]

Their objectives include (verbatim):

- Gaining, or attempting to gain, unauthorized access to a computer system or its data.
- Unwanted disruption or denial of service attacks, including the take down of entire web sites.
- Installation of viruses or malware - that is malicious code on a computer system.
- Unauthorized use of a computer system for processing or storing data.
- Changes to the characteristics of a computer system's hardware, firmware or software without the owner's knowledge, instruction or consent, and
- Inappropriate use of computer systems by employees or former employees.[2]

Protecting your IT infrastructure and data involves the development and implementation of appropriate and effective safeguards to ensure delivery of critical infrastructure services. Typical threat methodologies associated with the execution of a cyberattack are presented in the accompanying graphic.[3]



Cyber-attack Threat Methodologies

	NUISANCE	DATA THEFT	CYBER CRIME	HACKTIVISM	DESTRUCTIVE ATTACK
Objective	Access & Propogation	Economic, Political Advantage	Financial Gain	Defamation, Press & Policy	Disrupt Operations
Example	Botnets & Spam	Advanced Persistent Threat Groups	Credit Card Theft	Website Defacements	Delete Data
Targeted	✗	✓	✓	✓	✓
Character	Often Automated	Persistent	Frequently Opportunitistic	Conspicuous	Conflict Driven

Source: 2015 Mandiant M-Trends® Report

THE MOST COMMON TYPES OF CYBERATTACKS

- "**Advanced persistent threats,** or APTs, are long-term targeted attacks that break into a network in multiple phases to avoid detection. The five stages of an APT are reconnaissance (researching and understanding the target), incursion (delivering targeted malware), discovery (mapping the target's internal defenses), capture (acquiring data over an extended period) and exfiltration (exploiting captured information).

- **Distributed Denial of Service or DDoS** occur when a server is intentionally overloaded with requests, with the goal of shutting down the targets website or network system. Users will not be able to access your site or network, resulting in a partial or complete shutdown of your business operations, depending on how heavily you rely on the Internet.

- **Inside attack:** For this type of cyberattack, a sophisticated software program may not even be required: Someone with administrative privileges, usually from within the organization, purposely misuses his or her credentials to gain access to confidential company information. Ex-employees in particular present a threat if they left the company on bad terms, so your business should have a protocol in place to revoke all access to company data immediately upon an employee's termination. Inside attacks can also happen in the form of a hacker posing as a representative of a company your business works with to gain access to sensitive data.

- **Malware or "malicious software,"** covers any program introduced into the target's computer with the intent to cause damage or gain unauthorized access. There are many different types of malware, including viruses, spyware, worms, ransomware, Trojan horses and keyloggers, to name a few.

- **Password attacks:** Cracking a password is the simplest way for hackers to gain access to their target's accounts and databases. There are three main types of password attacks: brute force attack, which involves guessing at passwords until the hacker gets in; dictionary attack, which uses a program to try different combinations of dictionary words; and key logging, which tracks all of a user's keystrokes including login IDs and passwords.

- **Phishing:** Perhaps the most commonly deployed form of cybertheft, phishing involves collecting sensitive information like login credentials and credit card information through a legitimate-looking (but ultimately fraudulent) website, often sent to unsuspecting individuals in an email. As people become more aware of common phishing techniques — for instance, a notice from a financial institution with a mismatched or unsecured URL — hackers have become more sophisticated, so it's essential to keep up with the latest tactics to protect yourself." [4]

Taking into account the objectives of a cyberattack and some of the methodologies used to execute them, a small business' cybersecurity plan should address physical, network, and data security.

ENDNOTES

1. "Cyber Attacks: Prevention and Proactive Responses," Practical Law Company, 2011 [Authors: Vince Farhat, Bridget McCarthy and Richard Raysman, Holland & Knight LLP], https://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf [Reprinted with permission from the author]

2. "Cyber Attacks: Prevention and Proactive Responses," Practical Law Company, 2011 [Authors: Vince Farhat, Bridget McCarthy and Richard Raysman, Holland & Knight LLP], https://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf [Reprinted with permission from the author]

3. "M-Trends® 2015: A View from the Front Lines," [Threat Report], Mandiant®, a FireEye® Company, 2015, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

4. "Cybersecurity: A Small Business Guide," Business News Daily, 7/28/15, http://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html [Reprinted with permission from the author]