Responding to Cyber Attacks: Introduction

Overview

- Introduction
- Anatomy of a Cyber Attack
- Most Common Threat (Ransomware)
- Understanding Vulnerability
- Methods of Attacking Your System

Who am I?

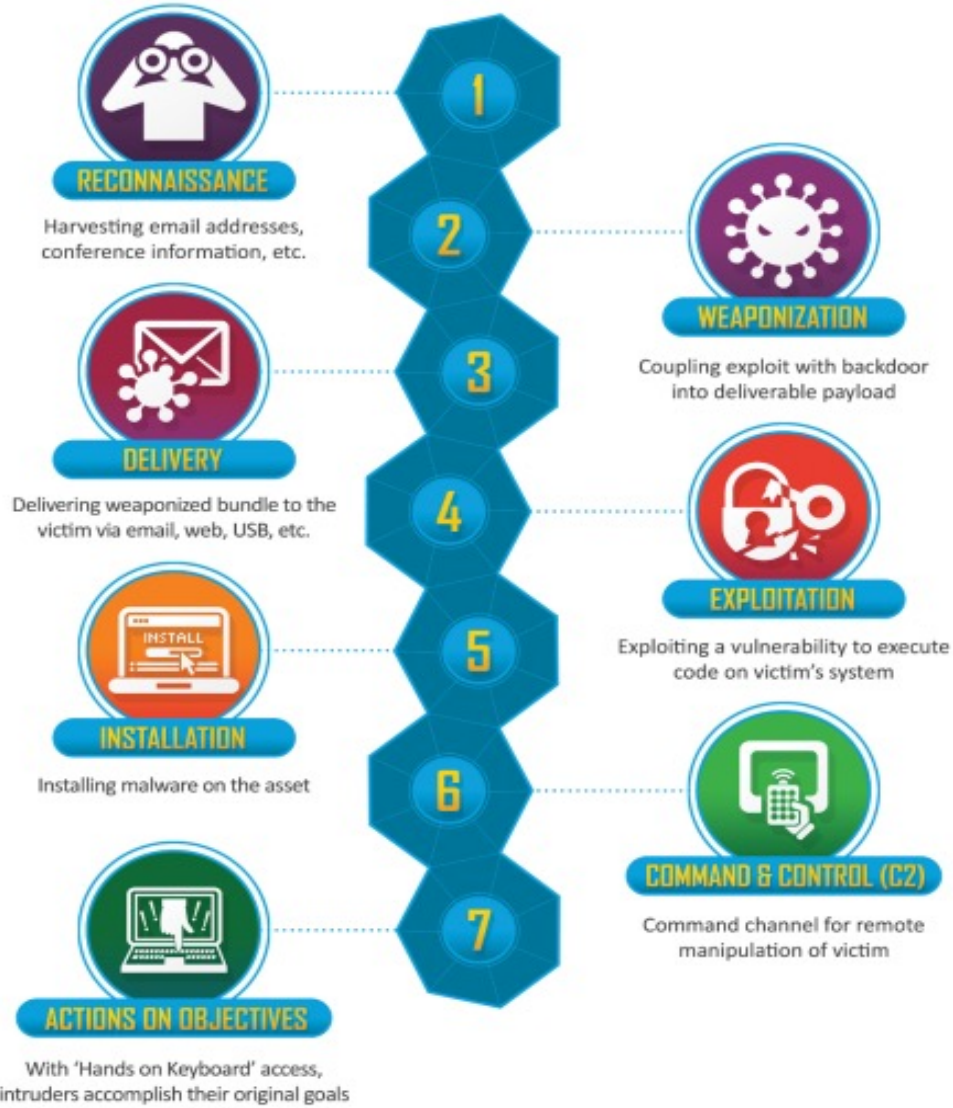
- Dr. Patrick Pape
- Principal Research Engineer @ UAH CCRE
- Email: papep@uah.edu
- Research Areas:
  - Digital forensics
  - Malware reverse engineering and analysis
  - Network security
  - Secure Software Development
  - Machine learning

Responding to Cyber Attacks: Anatomy of a Cyber Attack

Cybersecurity CIA Triad

- Core concepts that are the foundation of information security
- **Confidentiality**: privacy, ensuring that only authorized actors have access to/visibility of protected data
- **Integrity**: protecting data from unauthorized deletion/modification, ensuring that the data that you send is what is received
- **Availability**: ensuring that systems and services are accessible as desired, including data

Cyber Kill-Chain



Responding to Cyber Attacks: Most Common Attacks (Ransomware)

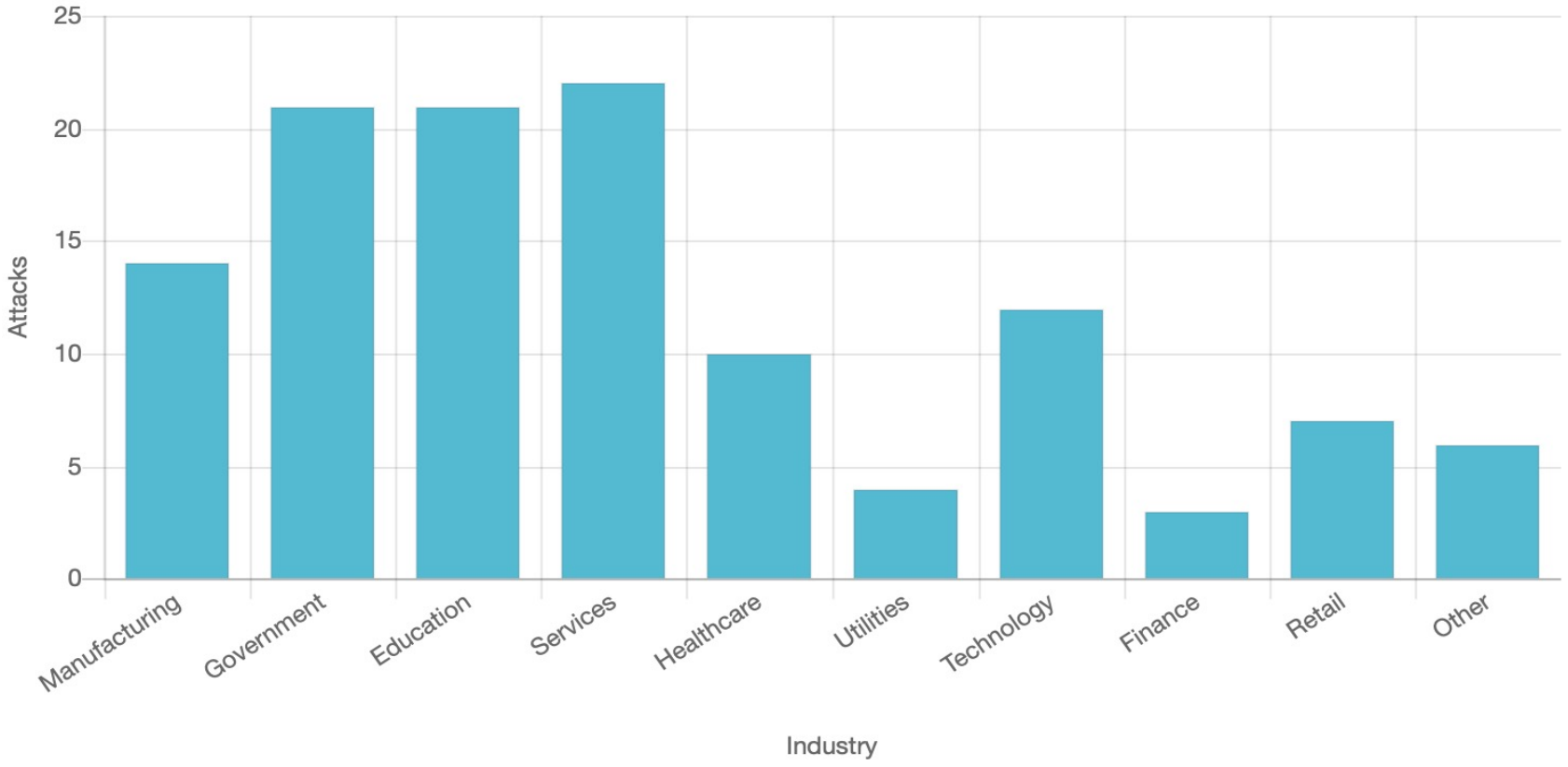
Malware: Ransomware

- *Define:* hardware, firmware, or software that is intentionally included or inserted in a system for the harmful purpose of encrypting, and sometimes exfiltrating, data/files on the system with the intent to sell access back to the owner for a fee.
- *Example:* Broward County Public School district was the target of a ransomware attack on March of 2021. The attackers gained access to secured files and encrypted them, causing disruption to services and demanding $40M to release the files. The ransom was not paid and ~26k files were released on the attackers' darknet website, though very little PII was found.

Malware: Ransomware

- K-12 schools made up 57% of targets for ransomware attacks between 8/2020 and 9/2020
- According to Emsisoft (https://www.emsisoft.com/en/company/about/)
  - >12 school district affected already in 2021, 58 last year
  - At least 8 cases of data being released in 2021, 22 last year
- Already upward trend in ransomware attacks targeting school districts accelerated by COVID forcing remote learning
- IBM report indicated 60% of teachers interviewed received no additional training for remote learning during pandemic and half received no cybersecurity training at all
- IBM also found that >30% of K-12 administrators polled said district employs 1-3 IT staffers in total

Ransomware by Industry



Cost of Data Breaches

- Money
  - Average cost of a ransom paid in 2019: $115k
  - Average cost of a ransom paid in 2020: $312k
- Reputation
  - Loss of trust with parents & students (customers)
  - Can become target for future attacks
- Privacy
  - Loss of Personally Identifiable Information (PII)
  - Loss of user account data, .e.g passwords, leading to future exploits

Malware: Ransomware

- *Mitigation:*
  - Regular data backup
    - Password protected offline copies: hard drive and long-term storage
    - Move data storage to a cloud environment
  - Air gap & network separation/segmentation
  - Update/patch OS, software firmware
  - Install and regularly update and scan systems with anti-virus/malware technology
- FBI alert: PYSA, aka Mespinoza, ransomware has been used against schools in 12 states and in the United Kingdoms

Responding to Cyber Attacks: Understanding Vulnerability

Definitions

- The National Institute of Standards most commonly defines a **vulnerability** as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- Can be more abstractly defined as any potential weakness in your enterprise/organization that a malicious actor could use to access or otherwise negatively impact your network or computer systems
- An **exploit** most commonly refers to the specific action(s) taken on a vulnerability discovered in your enterprise/organization which performs some malicious activity
- When evaluating the cyber-preparedness of your organization, it is important to consider the **surface area of attack**, that is, the number of options, or exposed space, in which an attacker can seek to find vulnerabilities to exploit

Vulnerabilities: People vs Technical

- When considering how best to secure your organization, from the seemingly endless number of possible cyber attacks which could come your way, it is important to consider all angles
- Security is not just the responsibility of your IT department or information security officer
- The most common “vulnerability” or initial point of failure in an organization is its people
  - Lack of training/care
  - Insider threat
- As we cover some key types of cyber concerns, we will discuss to what degree they are a people problem or a technical problem

Solving the People Problem

- Cyber awareness training and cybersecurity education modules
- Cybersecurity certifications for IT employees
- Regular auditing of user accounts to limit unnecessary access → Principle of Least Privilege
- Consider the problem of how to best protect potentially sensitive data being exchanged between a student or employee and a remote school district server
  - People: always using properly secured networks, utilizing VPNs to connect to the server
  - Technical: utilizing secure protocols for data exchange, proper management and upkeep of server software

Responding to Cyber Attacks: Methods of Attacking Your System

Phishing

- *Define:* technique for attempting to acquire sensitive data through a fraudulent solicitation, e.g. email or web site, in which the perpetrator masquerades as a legitimate business or reputable person
- *Example:* an attacker sends an email out to all users it can find within the @aasb.edu domain indicating that there was a problem with their registration to the Summer 2021 Conference. The email contains a hyperlink which when clicked takes the user to a website that automatically begins a download for malware onto their system.
- *Mitigation:*
  - Disable hyperlinks in emails
  - Add explicit tags/banner for external emails
  - Cyber awareness training

Credentials – Brute Force

- *Define:* using brute force to guess a valid login set on a network/computer system
- *Example:* an attacker hypothesizes that the user login to an organizational system is based on a user id that is the same as the user's email id taken from a public online directory. Using that id, the attacker tries all possible alphanumeric sequences until successfully finding the correct login.
- *Mitigation:*
  - Regular password updates with sufficiently different passwords, consult proper authorities, e.g. NIST, for proper length and complexity of passwords
  - Multi-factor authentication (hardware/software)
  - Cyber awareness training

Credentials – Password Cracking / Data Leak

- *Define:* the process of recovering secret passwords stored in a computer system, transmitted over a network, released in a data leak and using them to access a secured system;
- *Example: a*n employee uses the same password at work that they use for some educational service. The employee also uses their work email as their login for that service. That educational service is hit with a data breach and the email/login is exposed. This same email/login is then used to access the employee's account on the work network.
- *Mitigation:*
  - Regular password updates, no repeat passwords, consult proper authorities, e.g. NIST, for proper length and complexity of passwords
  - Multifactor authentication (hardware/software)
  - Cyber awareness training

Insecure Protocols / External Services

- *Define:* improperly configured web-based login/server access, vulnerabilities in 3rd party services used to support remote education
- *Example:* school district website uses insecure protocols for data security, e.g. http vs https, ftp vs sftp; a vulnerability is found in educational support technology, e.g. Blackboard or Canvas, that an attacker uses to gain access to PII
- *Mitigation:*
  - Update/patch operating system, software, firmware
  - Disable unused services/remote access
  - Vetting educational technology services:
    - How do they store data?
    - How do they manage data?
    - What data is tracked and shared?

Legal Issues for Data Integrity

Chris Pape
Shareholder, Education Group
Lanier Ford Shaver & Payne, P.C.
June 17, 2021

LANIER FORD

Topics

- The Alabama Data Breach Notification Act of 2018
  - Ala Code Section 8-38-1, *et seq.*
  - Data Management Requirements
  - Notice Requirements
- Liability
- Insurance

LANIER FORD

What is the Board's Obligation?

"(a) Each covered entity and third-party agent shall implement and maintain reasonable security measures to **protect sensitive personally identifying information** against a breach of security."

Ala. Code § 8-38-3(a)

Governmental entities, like boards of education, are covered entities!

LANIER FORD

What is Sensitive PII?

first name/first initial and last name in combination with one of the following:

1. A non-truncated Social Security number or tax identification number;
2. ***Any*** non-truncated government issued Identification number;
3. A financial account number, in combination with any security code, access code, password, expiration date, or PIN;
4. Any medical information (history, conditions, treatment, or diagnosis);
5. Health insurance policy number and unique identifier; or
6. User's name or email along with info that would allow access to your entity's online accounts.

LANIER FORD

Reasonable Security Measures

(1) Designate responsible employee(s);

(2) Identify internal and external risks of a breach of security;

(3) Adopt and assess effectiveness of safeguards to address identified risks of a breach of security;

(4) Retain service providers contractually required to maintain appropriate safeguards;

(5) Evaluate and adjust security as necessary to protect PII;

(6) Keep the Board appropriately informed of the overall status of its security measures

NOTE: This can be done in executive session.

LANIER FORD

Example Measure: Device Security

- "Bring Your Own Device" - situation in which students and employees bring personal devices and interface with school district systems
  - Potentially introducing malware into the systems from their unregulated devices
  - Require good cyber "hygiene" and awareness education for students and employees
  - Allow limited and secured connectivity to school systems with personal devices
- Student tablets/laptop loan programs
  - Same need for cybersecurity course or module for students
  - Regular scanning and re-imaging of loaned devices

Example Measure: Recovery Plan

- Establish detailed plan for recovering from and enduring state of affairs after successful cyber attack
- How to get back to normal operating procedures?
- How to store back-ups of data and reboot systems from back-ups
- Alternative approaches to work flow until systems are back online
- Update policies and technologies to fix cause of security failure to prevent being exploited again

What to Do If There Is A Breach?

- Be transparent **BUT DO NOT (3 Os)**:
  - Overshare
  - Overpromise
  - (Indulge in) Overconfidence
- Wait to provide details until you have **all** the facts.

What Investigative Steps Must Be Taken If There Is A Breach?

(1) Assess the nature and scope of the breach.

(2) Identify any PII that may have been involved in the breach.

(3) Determine whether PII has been acquired (or is reasonably likely have been) and whether it is likely to cause substantial harm to the affected individuals.

(4) Identify and implement measures to restore the security and confidentiality of the compromised systems.

LANIER FORD

How To Determine If PII is Acquired?

(1) Loss of physical control;

(2) Indications of PII being downloaded or copied.

(3) If there are examples of PII use; or

(4) Indications that the PII is now public (dark web).

LANIER FORD

If There Is A Breach, What Notice Must Be Given?

- Prompt Notice (not later than 45 days from breach)
- Notice that will not impair a criminal investigation
- Notice by mail or electronic mail (unless there are specific, applicable exemptions)

Notice to Individuals

The notice shall include, at a minimum, all of the following:

(1) The date, estimated date, or estimated date range of the breach.

(2) A description of the PII that was acquired by an unauthorized person.

(3) A general description of the actions taken by a covered entity to restore the security and confidentiality of the PII involved in the breach.

(4) A general description of steps an affected individual can take to protect himself or herself from identity theft.

(5) Information that the individual can use to contact the covered entity to inquire about the breach.

LANIER FORD

Exception, Substitute Notice

If notice is not feasible due to any of the following:

(1) Excessive cost to the entity or in excess of $500,000.

(2) Lack of sufficient contact information for the individual required to be notified.

(3) The affected individuals exceed 100,000 persons.

LANIER FORD

Then, the Board Can:

Do **both** of the following:

(1) A conspicuous notice on the Internet website of the covered entity, if the covered entity maintains a website, for a period of 30 days.

(2) Notice in print and in broadcast media, including major media in urban and rural areas where the affected individuals reside.

Notice to Attorney General

- **Why**: If 1,000 people impacted.
- **When**: No later than 45 days.
- **How**: Written notice
  - Synopsis
  - Approximate number of impacted individuals
  - Services to be offered without charge
  - Contact info for Board's response

- **Note:** Confidential information isn't subject to Alabama Open Records.

LANIER FORD

Notice to Consumer Reporting Agencies

- **Why**: If 1,000 people impacted.
- **When**: Without unreasonable delay.
- **How**: Written notice
- **What**: The timing, distribution, and content of the notices you are sending to impacted individuals.
- **Who**: ***Experian, Equifax, and TransUnion***

LANIER FORD

Liability

- No private right of action.
- Attorney General enforces the statute.
- Board:
  - Can be compelled to comply with statute, but no monetary penalties
- Individuals:
  - As always, may be subject to personal negligence
  - State Agent Immunity:
    - ***Applicable to employees IF they are adhering to Board policies and procedures***

LANIER FORD

Insurance Considerations

- Can be more expensive than the cost of repair
- The F.B.I. does not condone paying the ransom
  - Ransomware — FBI
- Insurance policies may have exclusions for client "mistakes"
  - Phishing

Questions?

References and Bio

Alabama Data Breach Notification Act of 2018

- Ala. Code § 8 -38-1. Short Title
- Ala. Code § 8 -38-2. Definitions
- Ala. Code § 8 -38-3. Reasonable Security Measures; Assessment
- Ala. Code § 8 -38-4. Investigation of Security Breach
- Ala. Code § 8 -38-5. Notice of Security Breach – Individuals Affected
- Ala. Code § 8 -38-6. Notice of Security Breach – Attorney General
- Ala. Code § 8 -38-7. Notice of Security Breach – Consumer Reporting Agencies
- Ala. Code § 8 -38-8. Notice of Security Breach – Covered Entities
- Ala. Code § 8 -38-9. Violations of Notification Requirements
- Ala. Code § 8 -38-10. Disposal of Records Containing Sensitive PII
- Ala. Code § 8 -38-11. Exemptions – Federal
- Ala. Code § 8 -38-12. Exemptions – State

LANIER FORD

References

https://blog.eccouncil.org/4-types-of-cyberattacks-that-youre-most-likely-to-face/

https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

https://www.securitymagazine.com/articles/95164-now-ransomware-is-inundating-public-school-systems

https://www.databreachtoday.com/ransomware-attacks-on-schools-latest-developments-a-16451

https://www.ic3.gov/Media/News/2021/210316.pdf

https://www.preferreditgroup.com/2019/08/27/the-three-goals-of-cyber-security-cia-triad-defined/

https://abcnews.go.com/US/wireStory/large-florida-school-district-hit-ransomware-

Dr. Pape's Relevant Experience

- Education:
  - Summer Workshops (grades 6-12)
  - Professional Workshops (cyber certifications and digital forensics)
  - Auburn University Montgomery – Assistant Professor
- Research:
  - Mississippi State University – Assistant Research Professor
    - Distributed Analytics and Security Institute
    - Center for Cyber Innovation
  - University of Alabama in Huntsville – Center for Cybersecurity Research and Education

Center for Cybersecurity Research and Education - CCRE

- https://www.uah.edu/ccre
- Interdisciplinary approach to defending networks, data, and computer operating systems from attacks
- Provide educational opportunities, including camps and scholarships:
  - Student and teacher training camps
  - Cybersecurity curriculum design and instruction
  - Cybersecurity certification training (Security+)
- Research expertise in a variety of topics:

- Identity management	- Vulnerability analysis
- Supply chain security	- Medical device security
- Intrusion Detection	- Digital forensics