§ 3: Common Threats and Mitigation

DANIEL SHIN, ESQ.
CYBERSECURITY RESEARCHER
CENTER FOR LEGAL & COURT TECHNOLOGY

Common Threats and Mitigation

- There will never be a one-size-fits-all approach to mitigate all cyber threats.
- You cannot simply delegate all cybersecurity risk to a single cybersecurity vendor.
- Effective risk mitigation must come from all levels within the organization.

Common Threats and Mitigation

- A combination of implementing best practices for good cyber hygiene, keeping up to date with the latest cybersecurity threats, and scrutinizing newly installed technologies can best mitigate current and future cyber threats.

Common Threats

Malicious Code

Harmful computer code or web script designed to create system vulnerabilities leading to back doors, security breaches, information and data theft, and other potential damages to files and computing systems.

- Virus: a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.
- Ransomware: a form of malware that encrypts a victim's files.
- Spyware: an unwanted software that infiltrates a computing device, stealing internet usage data and sensitive information. Spyware gathers personal information and relays it to advertisers, data firms, or external users

Denial of Service Attack

An attack meant to shut down a machine or network, making it inaccessible to its intended users.

- Flooding services vs. crashing services
- Distributed Denial of Service (DDoS) Attack: a DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target.

Social Engineering

Exploiting human weakness to encourage others to act that may not be of the others' interest.

Social Engineering

exploiting human weakness to encourage others to act that may not be of the others' interest

- Phishing Attack: practice of sending fraudulent communications that appear to come from a reputable source

Social Engineering

exploiting human weakness to encourage others to act that may not be of the others' interest

- Insider Threats: a threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the parent organization
  - *Negligent insiders*
  - *Collusive insiders*
  - *Malicious insiders*
  - *Third-party insiders*

Cyber Hygiene Check I

Cyber Hygiene Check I

Peter has the latest antivirus and antimalware software loaded on his work computer. And he personally runs prompted security updates as recommended.

While checking his email one afternoon, Peter noticed an email from his co-worker with an executable attachment labeled “SimsAccount.exe.” Suspicious of the attachment -it is against company policy to email account files- Peter scanned the attached file using the virus software installed on his computer. NO viruses were detected.

Satisfied with the results of the scan, Peter continued to download the file to his computer. Now downloaded, Peter again scanned the attached file again for viruses and malware. Again, the scan results did not detect a threat.

Cyber Hygiene Check I

Should Peter open the file?

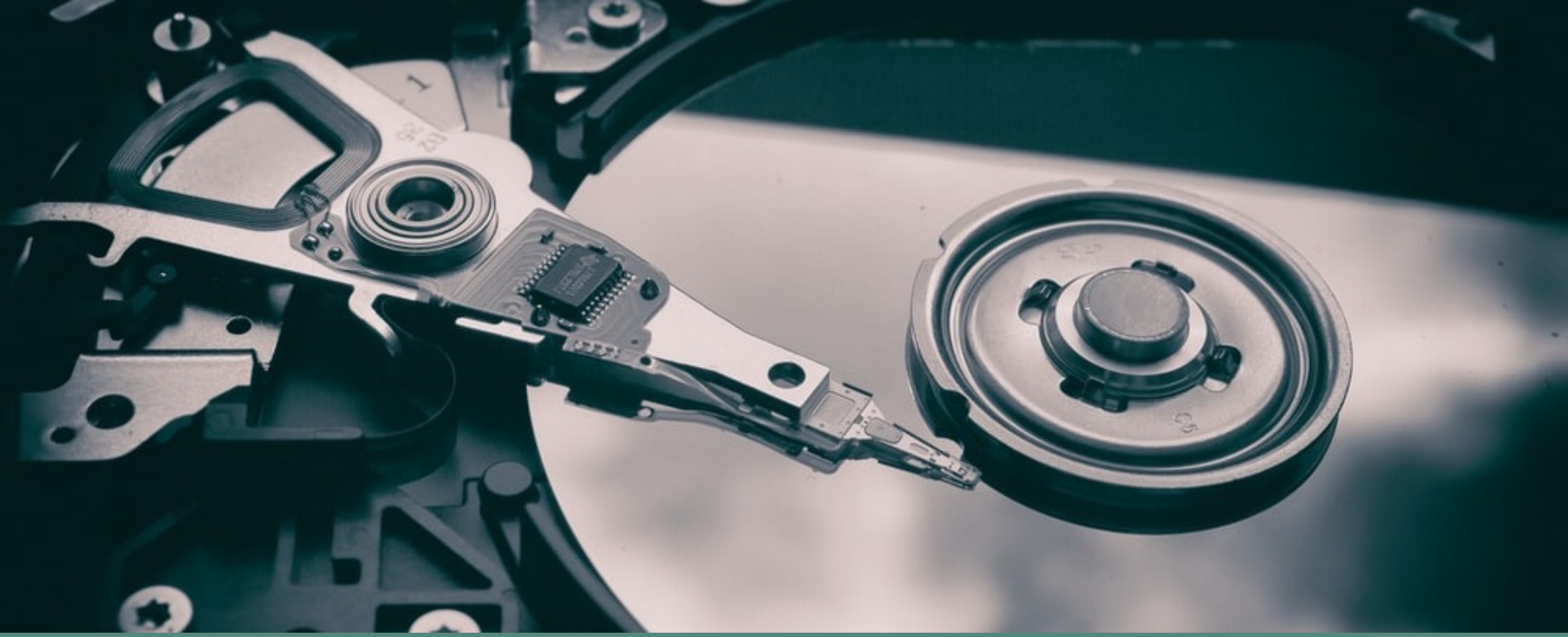
- (A) Yes. Peter performed due diligence by scanning the suspicious attached file three different times using the latest antivirus and antimalware software. The file is likely safe.
- (B) No. Even though Peter scanned the file using multiple antivirus and antimalware software, there is a possibility that the attached file is a novel malicious code that has not been recognized by even the latest antivirus and antimalware software. Peter should call his colleague to inquire why the Sims file was emailed and to offer to review the file within the accounts folder, following standard account review protocol.

Cyber Hygiene Check I

Should Peter open the file?

- (A) Yes. Peter performed due diligence by scanning the suspicious attached file three different times using the latest antivirus and antimalware software. The file is likely safe. – Wrong Answer
- (B) No. Even though Peter scanned the file using multiple antivirus and antimalware software, there is a possibility that the attached file is a novel malicious code that has not been recognized by even the latest antivirus and antimalware software. Peter should call his colleague to inquire why the Sims file was emailed and to offer to review the file within the accounts folder, following standard account review protocol. – Correct Answer

Mitigation Strategies



Backing-up

CLCT

WILLIAM & MARY

Commonwealth Cyber Initiative

Backing-up

- 3-2-1 backup rule: three copies of data on two different mediums with one off site copy
- Rapid backup restoration plan: if a situation arises where computer systems need to be restored at the latest backup state, what will be the procedures to quickly restoring the system backup?

Backing-up

- Single Points of Failure: Putting all the eggs in one basket. Avoid!
- RAID (Redundant Array of Independent Disks): using multiple hard drives to store a single set of data.
- When considering what to backup, do not only consider work files but the system as a whole (including programs, etc.).

Principal of Least Privileges

Users should be granted only the minimum amount of privileges needed to complete their task, lasting for the shortest amount of time.

CLCT

Principal of Least Privileges

- Administrative privileges vs. standard privileges:
  - Administrative privileges are the ability to make major changes to a system, typically an operating system.
  - Standard privileges are the ability to make enough changes to a system to work with a system for a given task.

Principal of Least Privileges

- Need for Access: whenever an access privilege is granted to the individual, there needs to be a legitimate need behind the privilege.

Principal of Least Privileges

- Malicious code attack mitigation: if a ransomware unintentionally executed under a non-administrative user account (standard user privileges), then the ransomware can only infect files as far as the user account has access to.

Layering

Setting up multiple levels of independent security systems.

CLCT

Layering

- Layering with Diversity: independent security systems should be diverse in terms of role and function to create a more difficult security environment for threat actors to infiltrate.
  - Example: Multi-factor authentication with password access.

Authentication Strategies

CLCT

WILLIAM & MARY

Commonwealth Cyber Initiative

Authentication Strategies

- Go back to the “Three As” on Section I: Authentication, Authorization, and Accounting.
- Checking security certificates and digital signatures on websites, emails, and certain types of files (installation programs, PDF files).

Authentication Strategies

- "If not sure, verify offline": If you receive communication that appears to have originated from a trusted colleague, but the message feels suspicious, then contact the colleague via different communication method (e.g., phone or in-person meeting) to verify the authenticity of the message.

Regular training and incident response plan

Clear understanding of responsibilities of different departments and a responsive timeline to timely address the issue.

Cyber Hygiene Check II

Cyber Hygiene Check II

Jordan is the manager of a cloud company. Jordan was recently told by upper management to provide cybersecurity and incident response training to employees that might need it.

Cyber Hygiene Check II

Which of the following groups of employee should Jordan give cybersecurity and incident response training?

- (A) The Information Technology Team, who is responsible for managing IT and other technical infrastructure for the company.
- (B) The Rapid Response Data Breach Team, who is responsible for responding to cyber attacks and data breaches for the company.
- (C) The Cleaning Staff, who is responsible for cleaning all the work area, emptying all the trash in the office, and shredding discarded documents.
- (D) All of the above. The Information Technology Team, the Rapid Response Breach Team, and the Cleaning Staff

Cyber Hygiene Check II

- Correct Answer: (D) All of the above. The Information Technology Team, the Rapid Response Breach Team, and the Cleaning Staff

Cyber Hygiene Check II

- Everybody in an organization has a role to maintain strong cybersecurity, not merely those who work in technology departments.
- Cleaning Staff may notice inadvertent misplacement of sensitive documents while cleaning the office, which should trigger an (inadvertent and somewhat contained) incident response protocol.
- Just like how fire drills apply to everyone inside the building, cybersecurity and incident response training should be available for everyone in an organization.

Thank you

DANIEL SHIN, ESQ.
CYBERSECURITY RESEARCHER
CENTER FOR LEGAL & COURT TECHNOLOGY