DEFENDING INTERNET ACCESSIBLE SYSTEMS

Notice

Commercial Endorsement Disclaimer: The United States Government through the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA or DHS.

Simulated Non-Production Data Disclaimer: No production data was used in this demonstration.

Sensitive Information Disclaimer: Be aware that this event is live! Events such as these are attended by people from many different federal agencies. As a student, PLEASE DO NOT DISCLOSE ANY AGENCY SENSITIVE INFORMATION DURING THIS EVENT.

CISA Comment Policy: This course abides by the CISA Comment Policy (https://www.cisa.gov/cisa-moderation-comment-policy).

DISCLAIMER: This webinar is being recorded and may be made public for the benefit of other students. While you are encouraged to engage with the speaker, you are advised against disclosing personally identifiable information (PII) on the recording. Please contact licensing@cisa.dhs.gov with any questions or comments.

Agenda

Introduction and Overview

- Learning Objectives
- Define IAS
- Vulnerability Impacts

Internet Accessible System Vulnerabilities

- Identification
- Mitigation
- Response/Recovery

Case Studies

- OPM Breach
- University of Washington Exposed Data
- Oklahoma Dept of Securities (ODS) Exposure of Data

Knowledge Check

- Questions
- Summary
- Resources

Learning Objectives

Terminal Objective

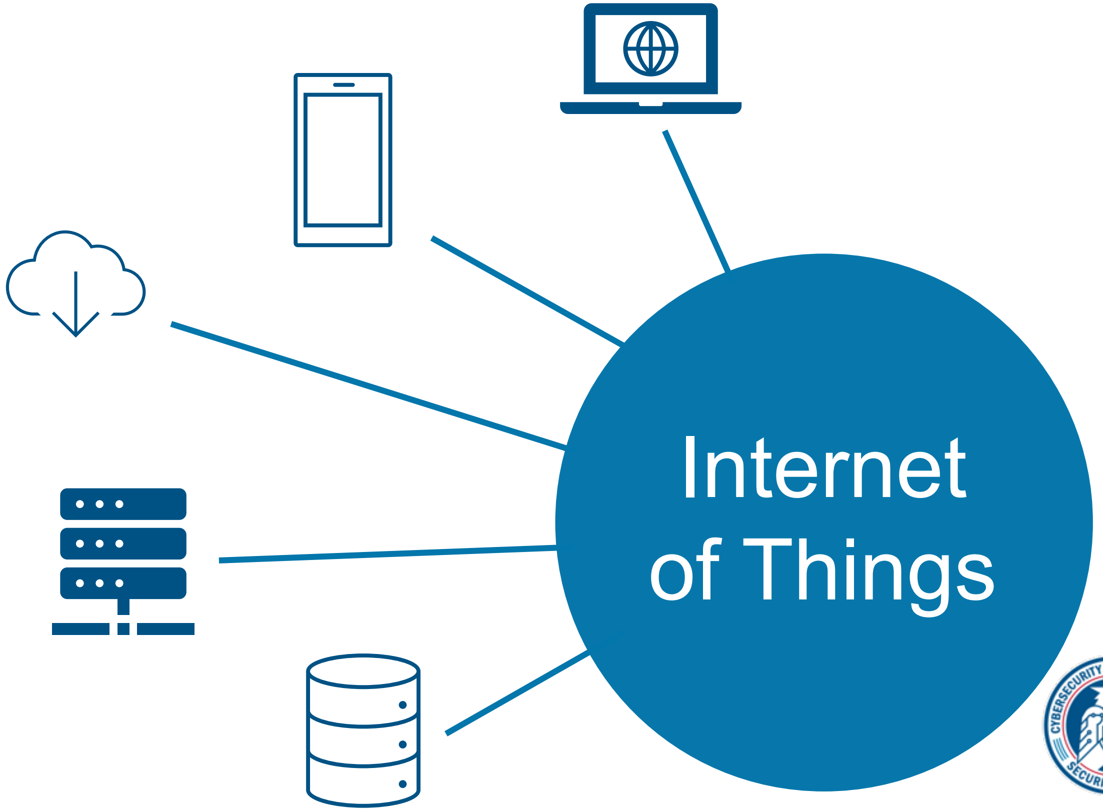
- Enable you to protect yourself and your organization from attacks against your internet accessible system (s) (i.e., Internet Accessible System Attacks-IAS), through awareness of individual and organizational points of vulnerability.

Enabling Objectives

- Define Internet Accessible System Vulnerabilities
- Present cyber hygiene best practices, to prevent threat attempts from being successful
- Explain the potential impacts of Internet Accessible System Vulnerabilities and what an effective organizational response looks like
- Categorize the steps to identify, mitigate, recover from Internet Access System (IAS) Attacks
- Explain the impacts of IAS Vulnerabilities through a series of real world scenarios

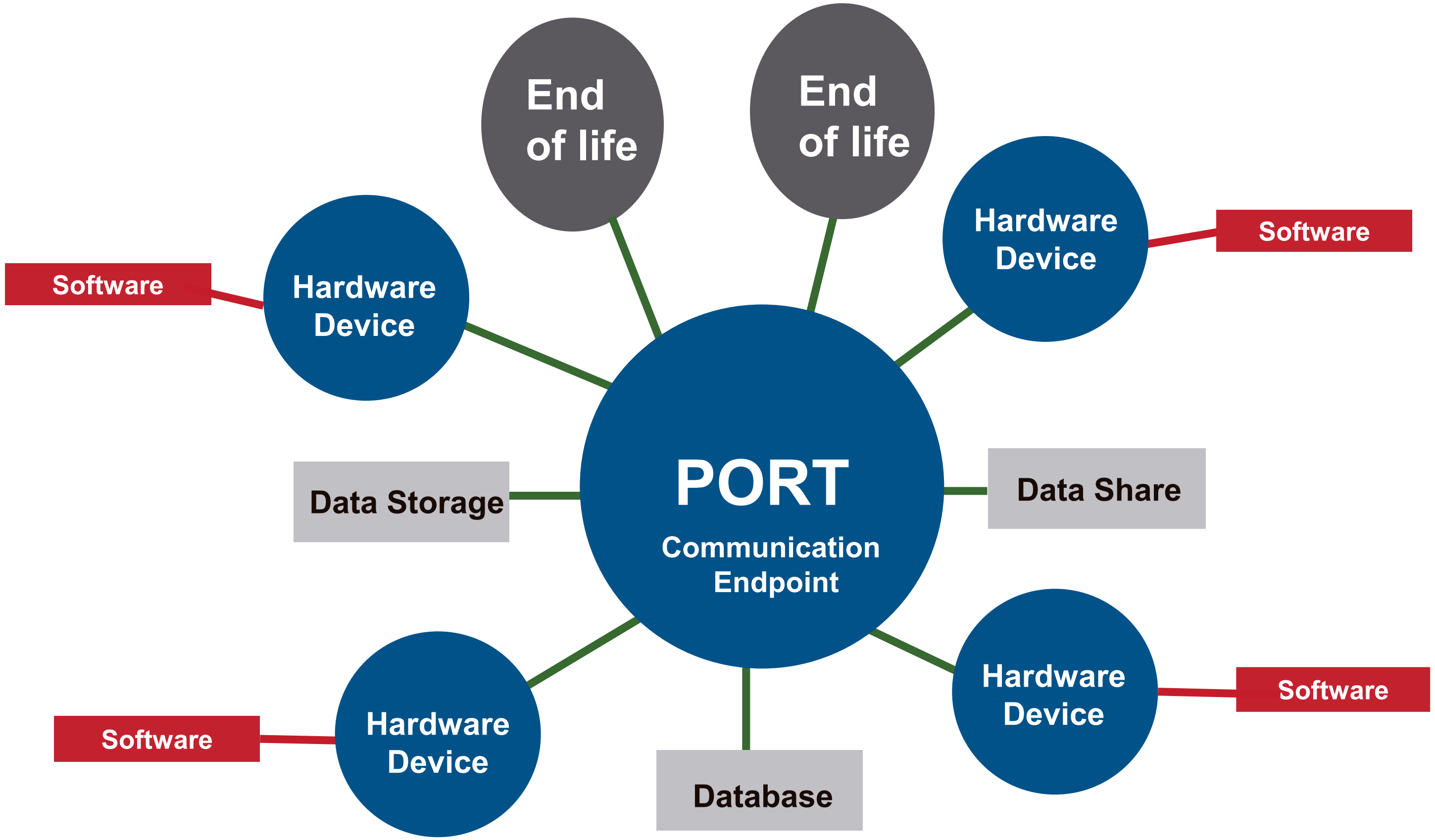
What is an Internet Accessible System?

Internet-Accessible Information systems include any system that is globally accessible over the public internet and encompasses those systems directly managed by an organization, as well as those operated by a third-party on an organization’s behalf.



Internet of Things

Internet-Accessible Systems Explained



TCP Ports: 22 – SSH, 80 – HTTP, 443 – HTTPS, RDP, FTP

IAS Vulnerabilities Exploited

If a vulnerability is found and exploited, attackers can establish unauthorized access to system memory, destroy or modify sensitive data, install malware, or take other actions to compromise the network and its data.

Cyber criminals can create havoc with an organization’s website through Structured Query Language (SQL) Injections by instructing databases and systems to execute unauthorized commands.

Top Exploitation Methods of 2021

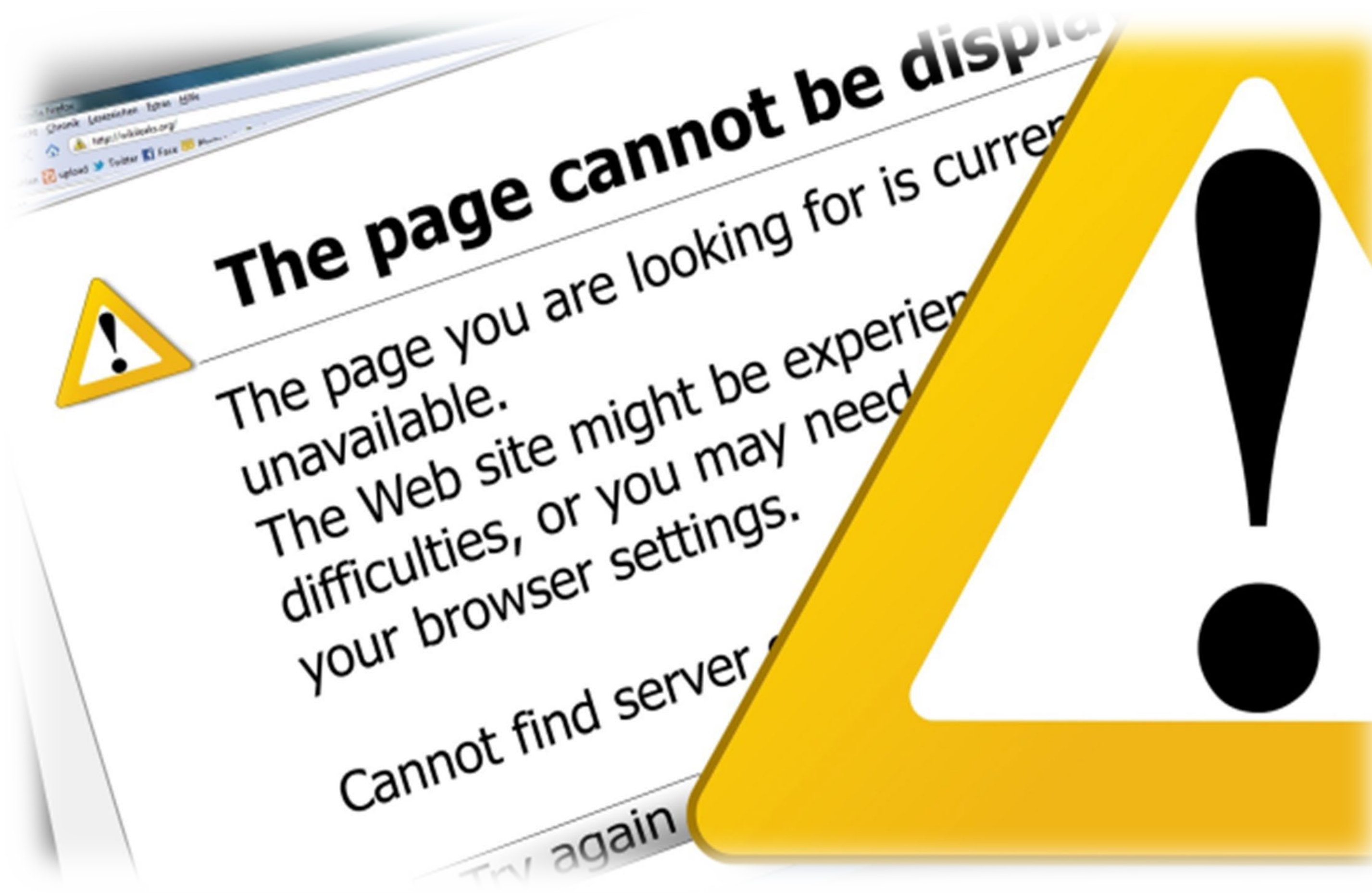
The top 15 exploited services in 2021 used the following methods:

- Remote Code Execution (RCE)
- Elevation of Privilege
- Security Feature Bypass
- Arbitrary Code Execution
- Arbitrary File Reading
- Path Traversal

Ref Source: CISA: https://www.cisa.gov/uscert/ncas/alerts/aa22-117a

IAS Vulnerability Indicators

- Slow Network Performance
- System Errors
- Access Denial



The page cannot be displa

The page you are looking for is curren
unavailable.
The Web site might be experien
difficulties, or you may need
your browser settings.

Cannot find server

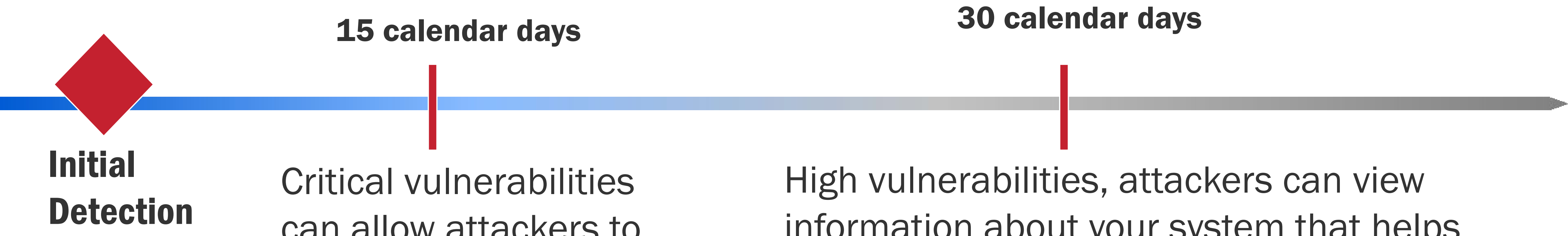
Try again

Mitigate IAS Vulnerabilities

Best practices to mitigate IAS Vulnerabilities:

- Hire scanning service to scan and monitor all internet accessible system IP addresses weekly
- Create and maintain an asset inventory of IP addresses
- Be aware of system privacy policies
- Secure IAS systems programs (i.e., encryption and firewall software)
- Notify scanning service of modifications to business Internet-Accessible IPs
- Ensure passwords have sufficient complexity and secrecy

Respond to IAS Vulnerabilities



15 calendar days

30 calendar days

Initial Detection

Critical vulnerabilities can allow attackers to take complete control of your web applications and web servers

High vulnerabilities, attackers can view information about your system that helps them find or exploit other vulnerabilities that enable them to take control of your website and access sensitive user and administrator information.

Ref: https://www.cisa.gov/news-events/directives/binding-operational-directive-19-02

Recover from an IAS Attack

Remediation planning tips:

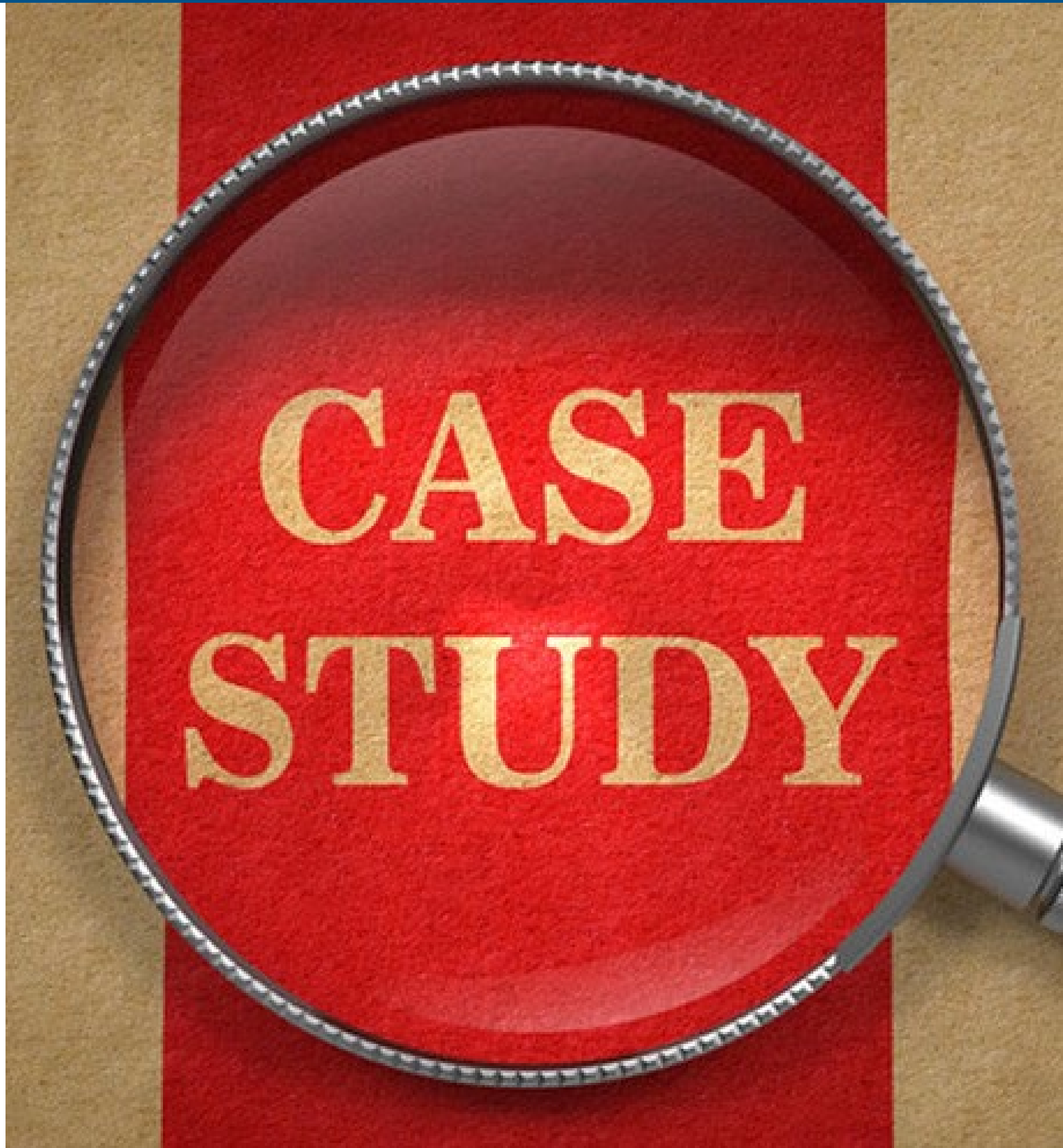
- Ask for help, contact CISA, the FBI or the Secret Service
- Work with experienced Cybersecurity advisor to help identify the extend of damage and recover from the attack
- Isolate the infected system
- Inform all stakeholders (employees, customers, partners, vendors) through a coordinated POC for the organization
- Apply impact assessment findings to prioritize recovery actions
- Implement a vulnerability and configuration management program to enforce consistent patch management and remove end of life systems.

Ref: https://www.cisa.gov/news-events/directives/binding-operational-directive-19-02

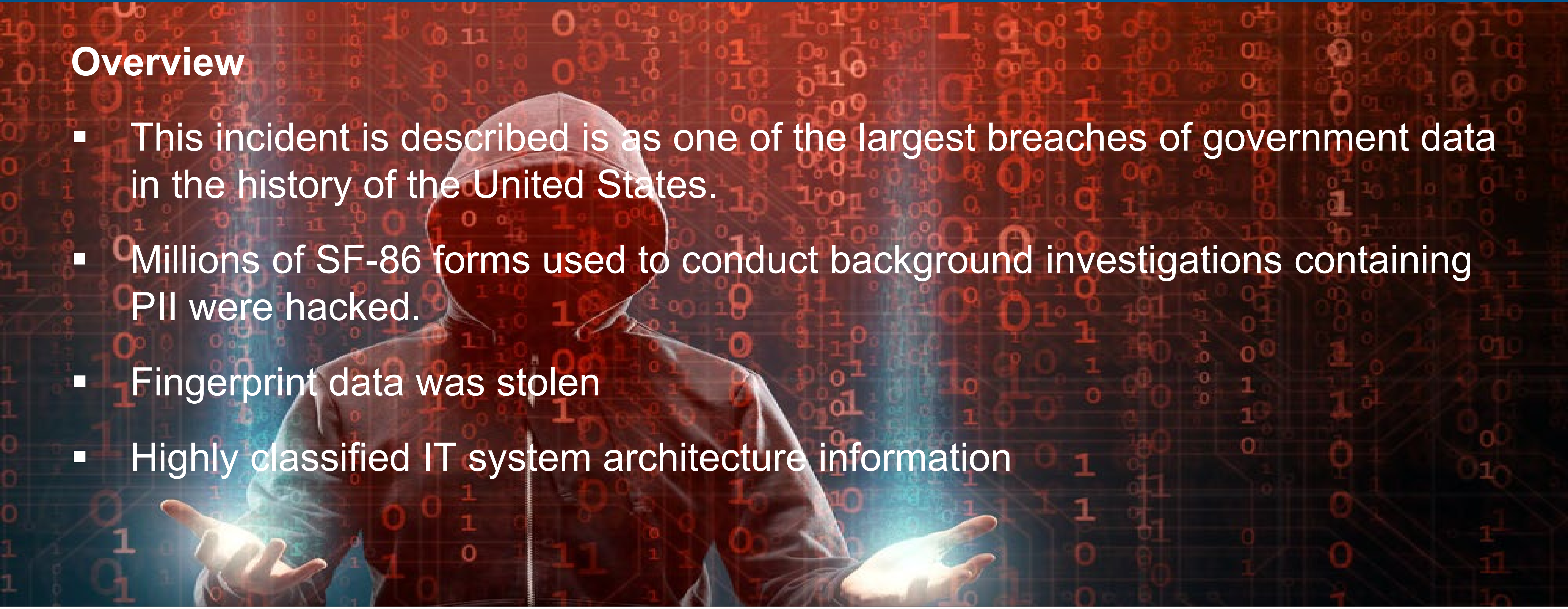
Case Studies

The following slides provide selected real-world examples of internet accessible system attacks, the impacts, and how the organizations responded to these attacks.

- Office of Personnel Management (OPM)
- University of Washington (UW)
- Oklahoma Department of Securities (ODS)



Office of Personnel Management (OPM) Breach



Overview

- This incident is described is as one of the largest breaches of government data in the history of the United States.
- Millions of SF-86 forms used to conduct background investigations containing PII were hacked.
- Fingerprint data was stolen
- Highly classified IT system architecture information

https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

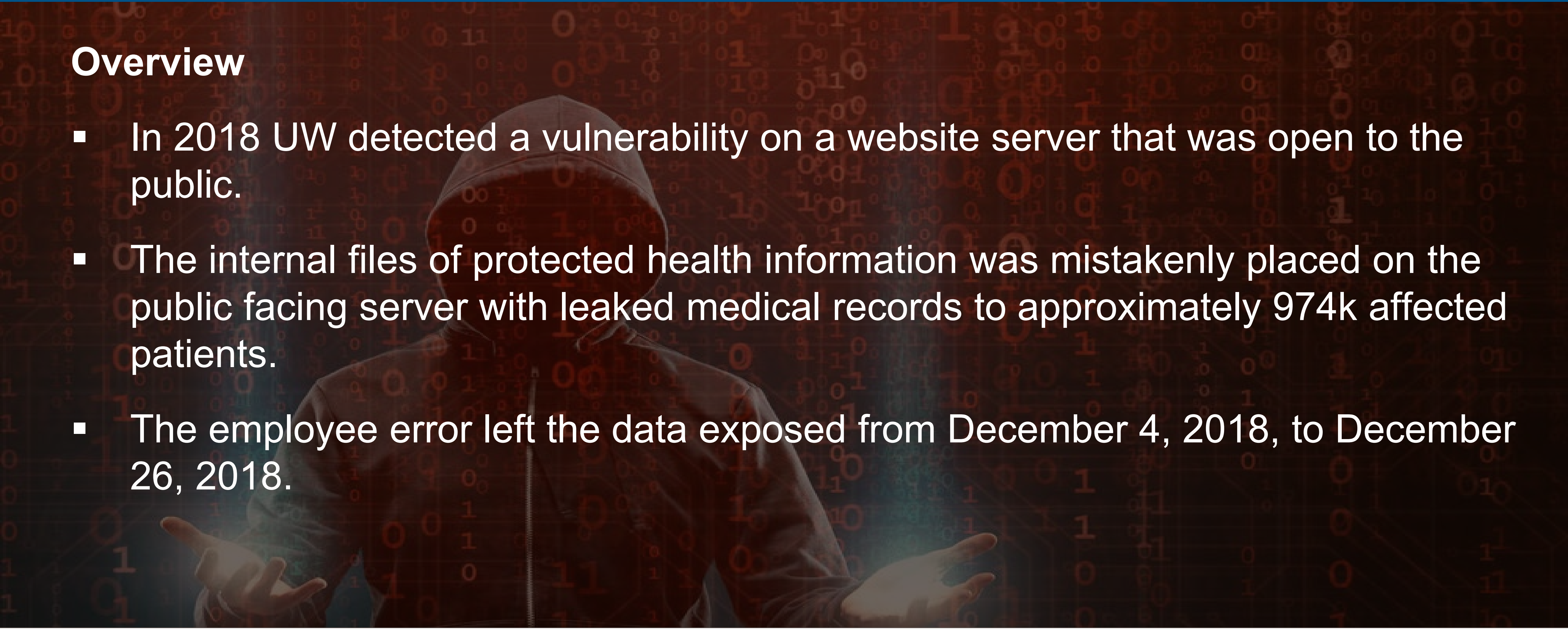
Office of Personnel Management (OPM), Cont.

Incident Response

- Isolate the attack
- Perform a system reset
- Implement two-factor authentication
- US-CERT Emergency team

https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

University of Washington (UW)

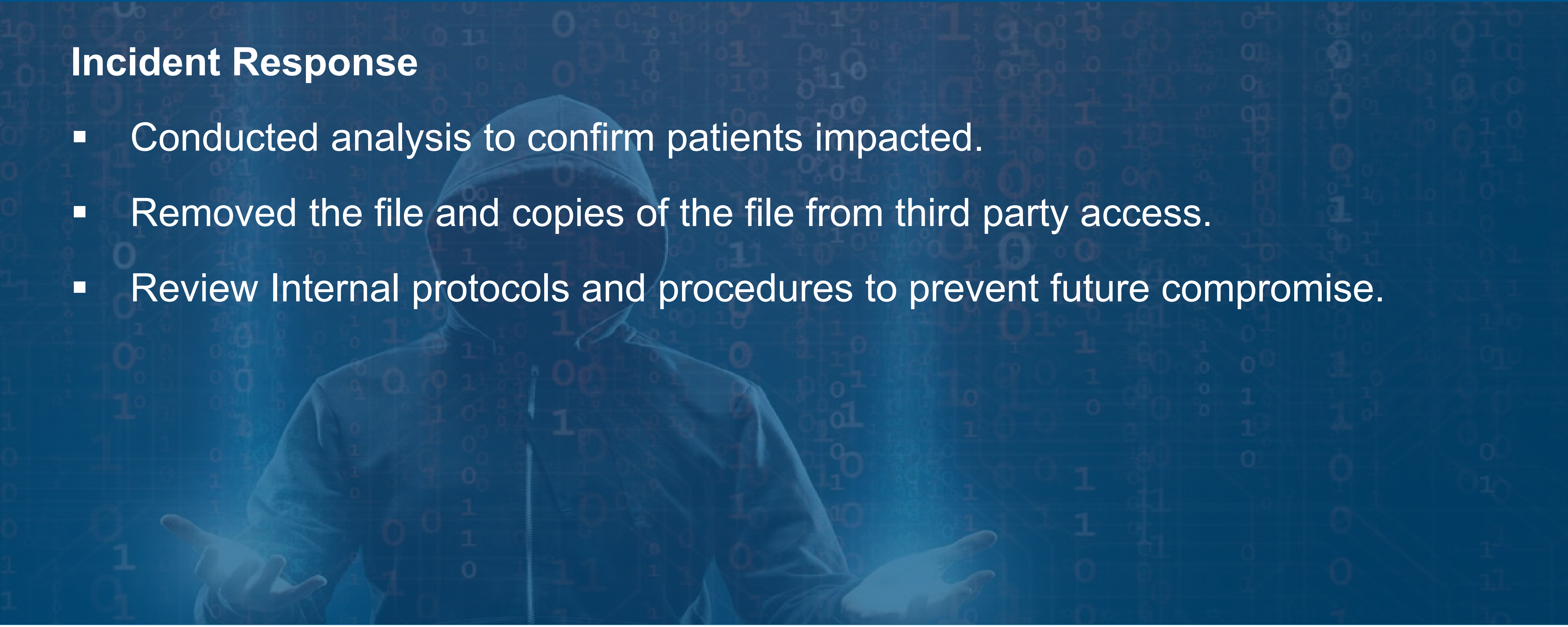


Overview

- In 2018 UW detected a vulnerability on a website server that was open to the public.
- The internal files of protected health information was mistakenly placed on the public facing server with leaked medical records to approximately 974k affected patients.
- The employee error left the data exposed from December 4, 2018, to December 26, 2018.

https://newsroom.uw.edu/news/data-error-exposes-patient-information

University of Washington (UW), Cont.

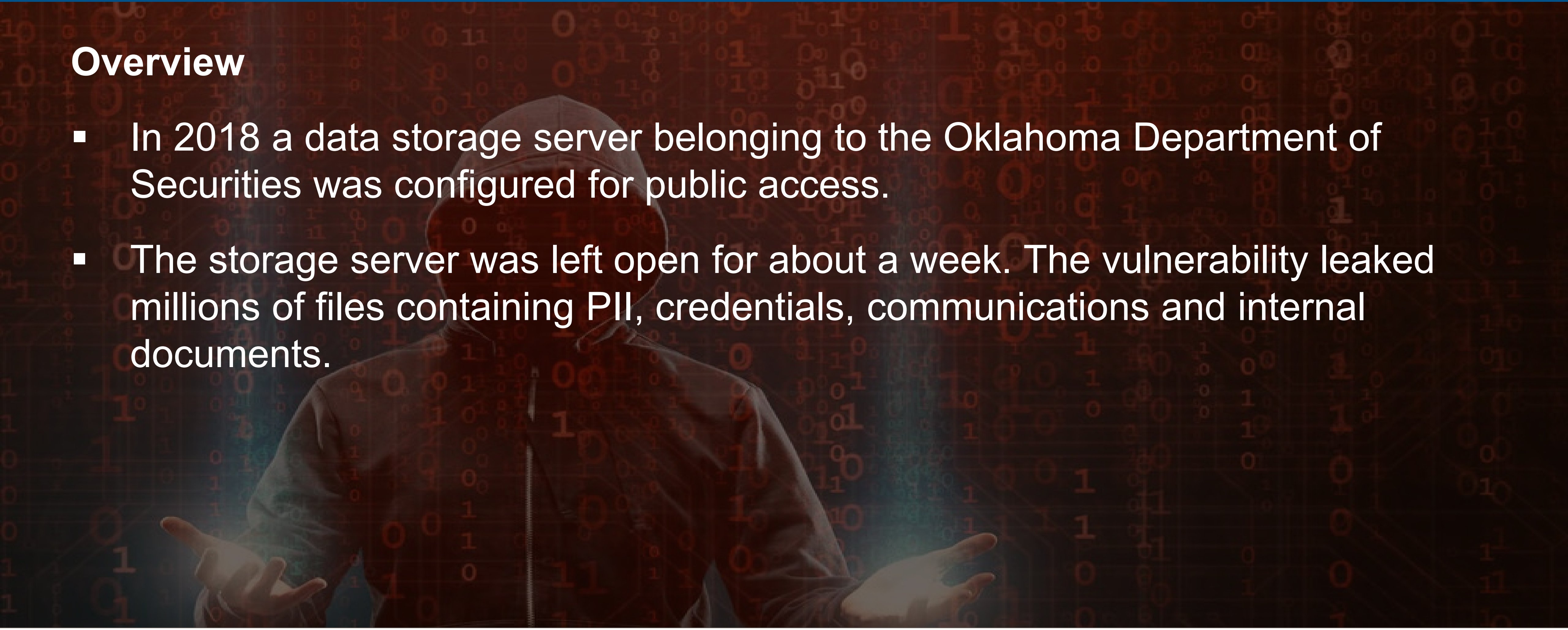


Incident Response

- Conducted analysis to confirm patients impacted.
- Removed the file and copies of the file from third party access.
- Review Internal protocols and procedures to prevent future compromise.

https://newsroom.uw.edu/news/data-error-exposes-patient-information

Oklahoma Department of Securities (ODS)



Overview

- In 2018 a data storage server belonging to the Oklahoma Department of Securities was configured for public access.
- The storage server was left open for about a week. The vulnerability leaked millions of files containing PII, credentials, communications and internal documents.

https://www.upguard.com/breaches/rsync-oklahoma-securities-commission

Oklahoma Dept of Securities (ODS), Cont.

Incident Response

- Conducted analysis to identify breach
- Remove public access
- Hired investigator
- Report to FBI

https://www.upguard.com/breaches/rsync-oklahoma-securities-commission

Summary

- ✓ Define Internet Accessible System Vulnerabilities
- ✓ Understand cyber hygiene best practices that prevent threat attempts from succeeding
- ✓ Potential impacts of Internet Accessible System exploits and what an effective organizational response looks like
- ✓ Understand the steps to identify, mitigate, and recover from IAS attacks

Resources

Vulnerability Remediation Requirements For Internet-Accessible Systems

https://www.cisa.gov/news-events/directives/binding-operational-directive-19-02

Understanding Denial-of-Service Attacks

https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

Wireless Network and Wi-Fi Security Issues to Look Out For

https://cybersecurity.att.com/blogs/security-essentials/security-issues-of-wifi-how-it-works

Remediate Vulnerabilities for Internet-Accessible Systems

https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-RemediateVulnerabilitiesforInternetAccessibleSystems_S508C.pdf

OPM Hack Article

https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-America.html

Additional Resources

CISA Website

- https://www.cisa.gov

IR Training Website

- https://www.cisa.gov/resources-tools/programs/Incident-Response-Training

CISA GitHub

- https://www.cisa.gov/cisa-github

CISA YouTube Channel

- https://www.youtube.com/channel/UCxyq9roe-npgzrVwbpoAy0A

FedVTE

- https://fedvte.usalearning.gov

CISA Commenting Policy

- https://www.cisa.gov/cisa-moderation-comment-policy

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA