Module 1: IT and Security Principles

Frank Asamoah

MBA| MSC | BSC | CEH | Security + | CYSA+|CISM |CASP+| GCP Architect

@kingphranky

https://www.linkedin.com/in/frank-asamoah

All Rights © Reserved Schnell Academy 2024

Information Technology and Security Principles: Threats

Understanding Cybersecurity Threats, Types, and Best Practices

All Rights © Reserved Schnell Academy 2024

Overview of Threats

Definition of threats in cybersecurity: Events or circumstances that could harm an organization's assets, networks, or operations.

Types of threats: Intentional (e.g., cyberattacks by hackers) and unintentional (e.g., natural disasters or human error).

All Rights © Reserved Schnell Academy 2024

Categories of Threats

01

Human Threats: External (hackers, cybercriminals) and internal (disgruntled employees, accidental breaches).

02

Natural Threats: Disasters like earthquakes, floods, and hurricanes.

03

Technological Threats: System failures, hardware malfunctions, outdated software.

04

Physical Threats: Unauthorized access, theft, and sabotage.

All Rights © Reserved Schnell Academy 2024

Types of Cybersecurity Threats

Brief descriptions of common cyber threats.

Phishing: Deceptive emails to steal sensitive info.

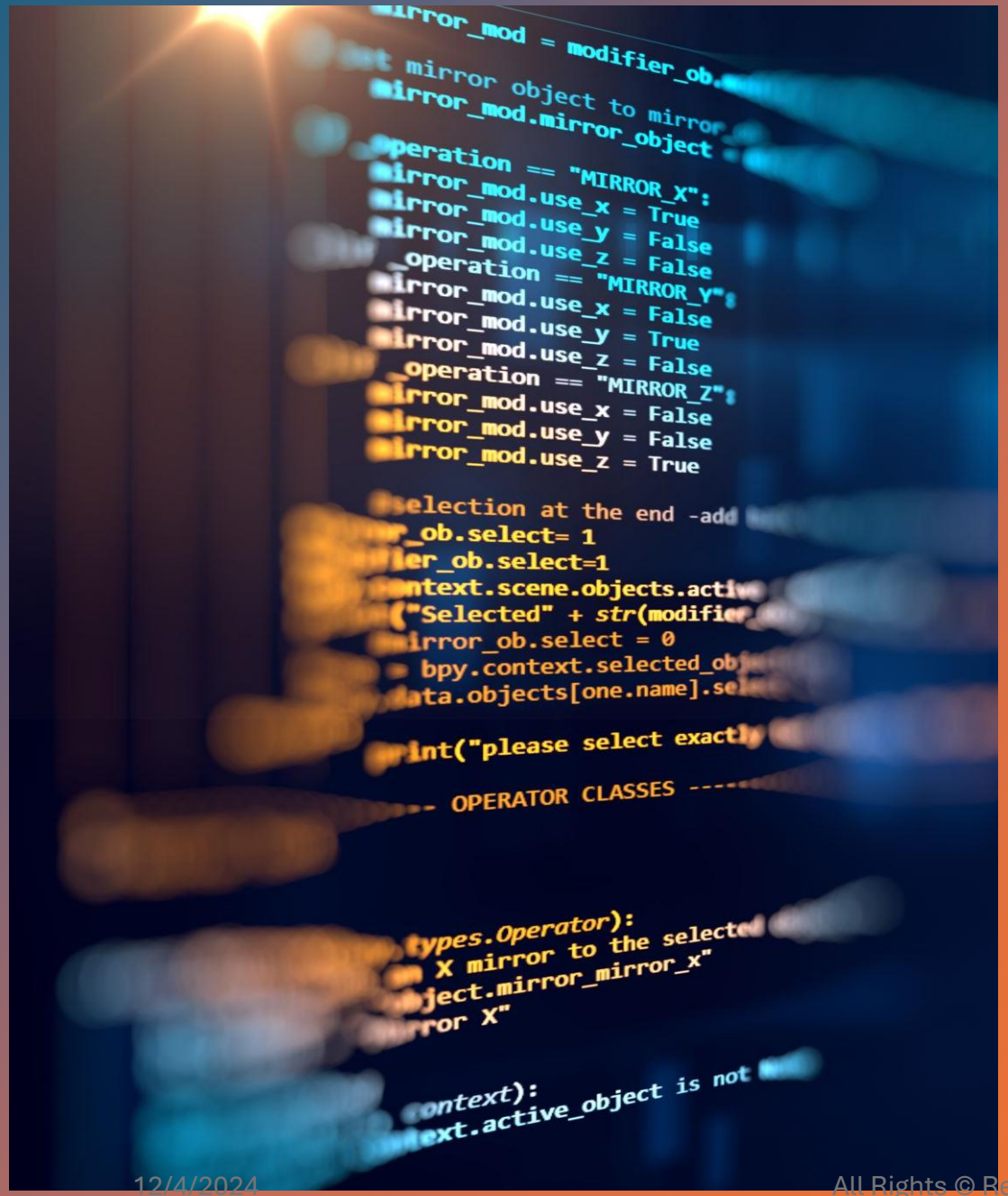
Ransomware: Malware demanding ransom for data access.

DDoS: Overloading systems to disrupt access.

Insider Threats: Internal personnel causing harm.

APTs: Long-term attacks by skilled attackers.

All Rights © Reserved Schnell Academy 2024



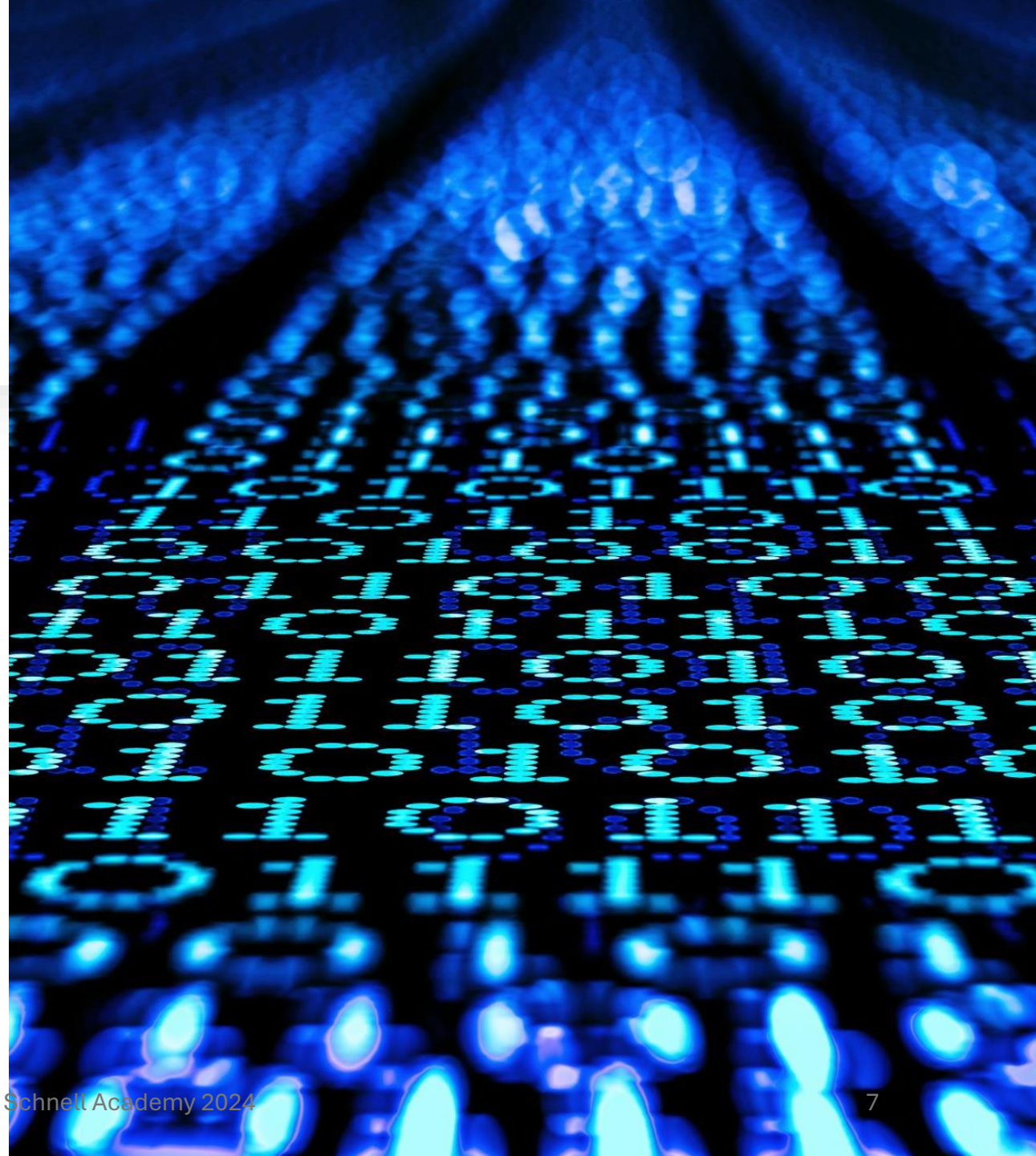
Phishing

- **Definition**: Fake emails/messages designed to steal info.
- **Example**: 2016 DNC phishing attack that compromised sensitive data.

All Rights © Reserved Schnell Academy 2024

Ransomware

- **Definition**: Malware that encrypts data and demands a ransom.
- **Example**: WannaCry ransomware attack in 2017.



All Rights © Reserved Schnell Academy 2024

Distributed Denial-of-Service (DDoS)

- **Definition**: Overloading a system with traffic to make it unavailable.
- **Example**: 2016 Dyn DNS DDoS attack that affected major websites.

All Rights © Reserved Schnell Academy 2024

Insider Threats

Definition: Threats from individuals within the organization, like employees or contractors.

Example: Edward Snowden’s data leak of classified NSA information.

All Rights © Reserved Schnell Academy 2024

Advanced Persistent Threats (APTs)

- **Definition**: Targeted, long-term cyberattacks, often by skilled and well-funded attackers.

- **Example**: SolarWinds attack in 2020 affecting government agencies and corporations.

All Rights © Reserved Schnell Academy 2024

Common Threat Actors

- **Cybercriminals**: Financially motivated.
- **Hacktivists**: Politically or socially motivated.
- **State-Sponsored Actors**: Government-backed for espionage.
- **Insiders**: Malicious employees or contractors.

All Rights © Reserved Schnell Academy 2024

Threat Modeling and Risk Assessment

- **Threat Modeling**: Identifying and understanding threats using methods like STRIDE and PASTA.
- **Risk Assessment**: Evaluating likelihood and impact of threats.
- Steps: Identify assets, threats, assess vulnerabilities, analyze impact, and develop mitigation strategies.

All Rights © Reserved Schnell Academy 2024

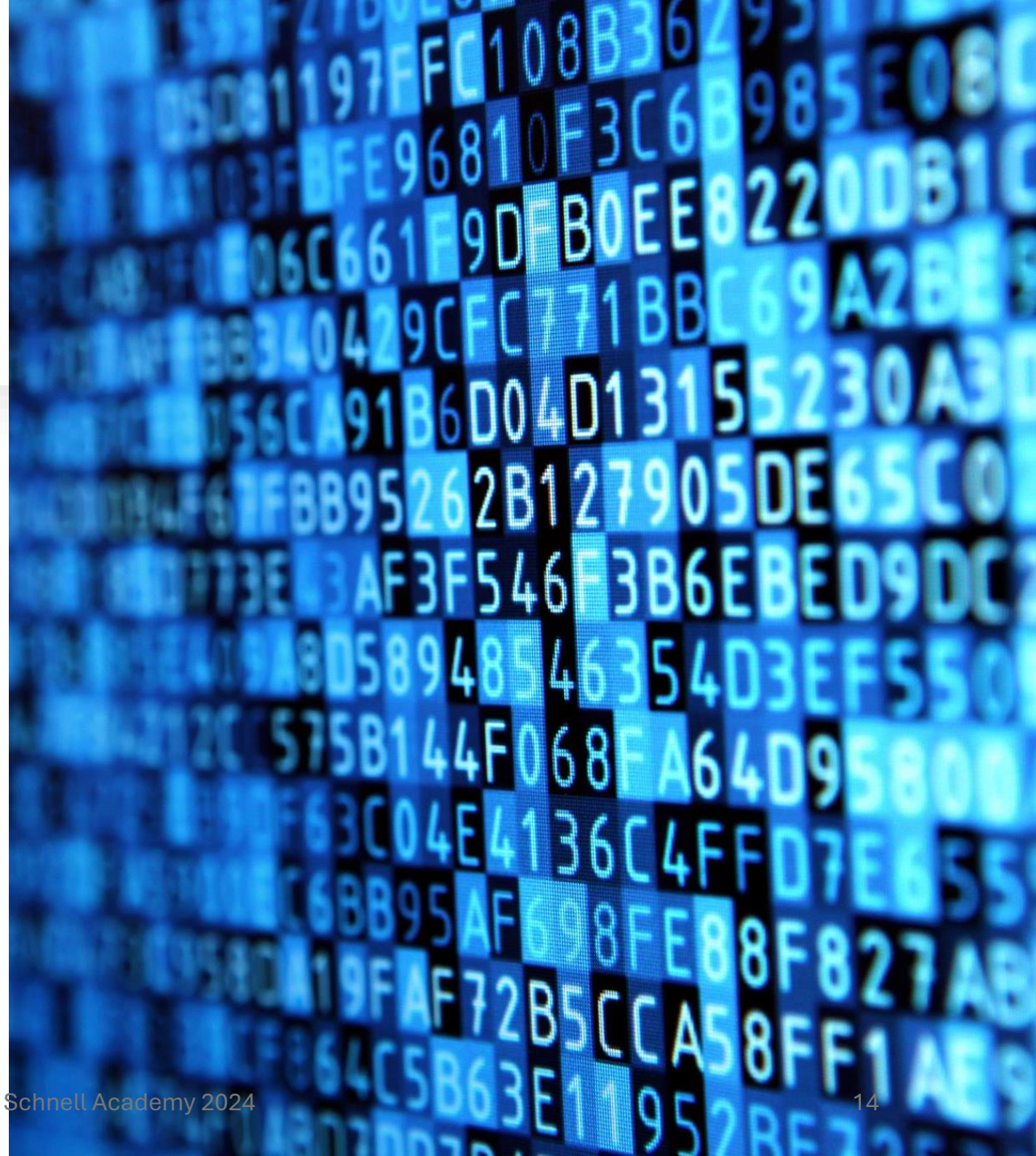
Best Practices for Threat Management

- **Access Controls**: Use MFA and Principle of Least Privilege.
- **Regular Updates**: Implement patch management.
- **Employee Training**: Educate on phishing and social engineering.
- **Network Security**: Use firewalls, IDS, and IPS.
- **Incident Response Planning**: Prepare and test response plans.

All Rights © Reserved Schnell Academy 2024

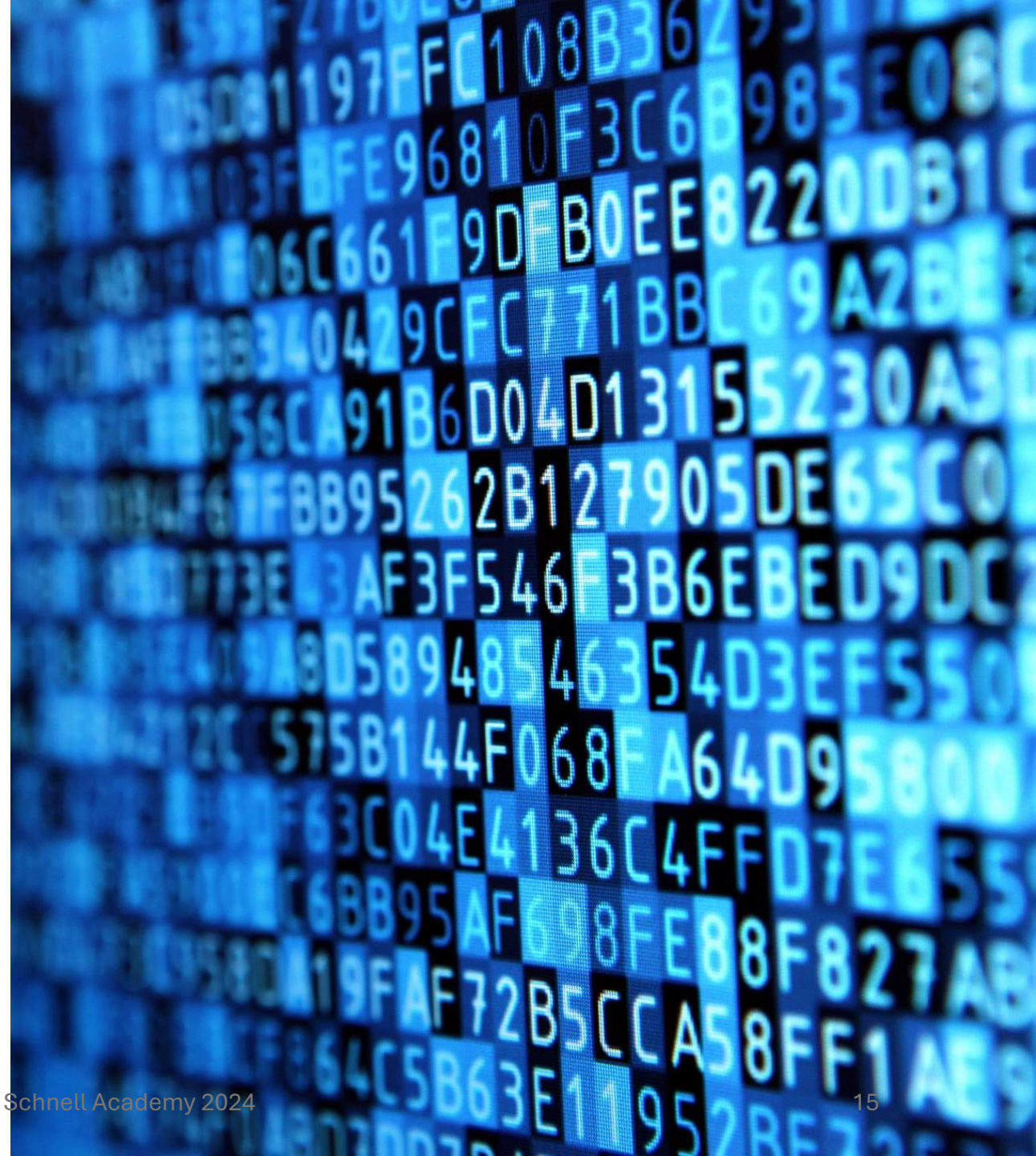
Case Study 1: Equifax Data Breach (2017)

- **Background**: Unpatched vulnerability in Apache Struts exploited.
- **Impact**: Exposed data of 147 million individuals.
- **Lesson Learned**: Importance of timely patch management.



All Rights © Reserved Schnell Academy 2024

Case Study 2: Target Data Breach (2013)



- **Background**: Credentials stolen from third-party HVAC vendor used to access data.
- **Impact**: 40 million credit and debit card records compromised.
- **Lesson Learned**: Importance of third-party security assessments.

All Rights © Reserved Schnell Academy 2024

Assignments

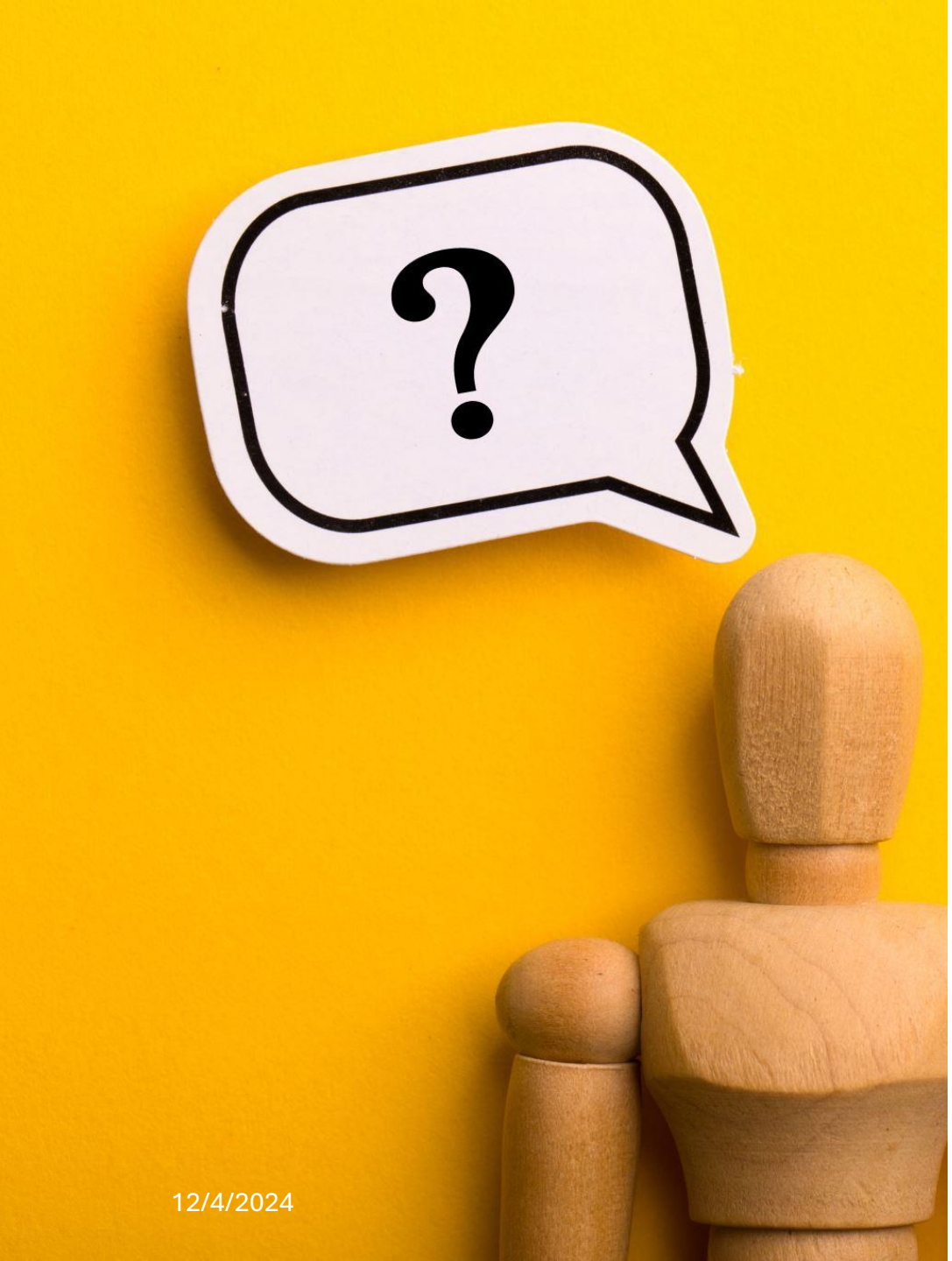
- **Research Assignment**: Report on a recent cyber threat affecting a major organization.
- **Practical Assignment**: Conduct a basic threat modeling exercise for a small business.
- **Group Assignment**: Present on common cyber threats in a specific industry.

All Rights © Reserved Schnell Academy 2024

Recommended Resources

- **YouTube**:
  - "Cyber Threats Overview: Understanding Cybersecurity Threats"
  - "Threat Modeling Explained"
- **Books**:
  - *Cybersecurity Essentials* by Charles J. Brooks
  - *Threat Modeling: Designing for Security* by Adam Shostack

All Rights © Reserved Schnell Academy 2024



Thank You!

Questions?

All Rights © Reserved Schnell Academy 2024