



December 3, 2024

**“Rules of Engagement:
Navigating the World of Security
Standards”**

Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

 **Tulsa**
SCHUSTERMAN CENTER

1

Checking In

- What’s the top takeaway from last class or classes that’s sticking with you? (Guards, Guns, and Gates; Real-Time Security: How to SOAR Above the Threats)
- Was there anything from last class or classes that didn’t fully click? Anything you’re still a little fuzzy on?

2

Learning Outcomes

1. Identify key security laws, regulations, and standards (e.g., GDPR, PCI DSS, HIPAA) and explain their significance in achieving effective security governance.
2. Evaluate comprehensive IT security policies, including data classification, change management, access control, personnel policies, and incident response procedures, while demonstrating understanding of their role in organizational security.
3. Assess security awareness training programs that address both technical and non-technical personnel needs, incorporating various training methods (CBT, ILT, role-based) and focusing on practical threat recognition and response.

3



4

General Data Protection Regulation (GDPR)

The GDPR grants EU residents **eight privacy rights**:

- **Right to be informed:** Know how personal data is collected and used.
- **Right of access:** View their personal data.
- **Right to rectification:** Correct inaccurate or incomplete data.
- **Right to be forgotten:** Request deletion of personal data.
- **Right to restrict processing:** Limit how data is used.
- **Right to data portability:** Transfer their data between services.
- **Right to object:** Refuse data processing under specific circumstances.
- **Rights related to automated decision-making and profiling:** Challenge decisions made without human input.

5

Payment Card Industry Data Security Standard (PCI DSS)

The **PCI Security Standards Council (PCI SSC)** develops standards to protect card data, including the **PCI Data Security Standard (PCI DSS)**.

PCI DSS has 12 compliance requirements to safeguard cardholder data:

- a. Use secure network controls.
- b. Configure systems securely.
- c. Protect stored account data.
- d. Encrypt cardholder data during transmission over public networks.
- e. Defend systems against malware.
- f. Keep systems and software secure.

6

Frameworks

- **Center for Internet Security (CIS):** Focuses on developing best practices to defend against cyber threats.
- **National Institute of Standards and Technology (NIST):** A US government agency advancing standards and technology for federal systems.
- **International Organization for Standardization (ISO):** Develops global standards through member countries.
- **International Electrotechnical Commission (IEC):** Creates international standards for electrical and electronic technologies.
- **American Institute of Certified Public Accountants (AICPA):** Provides resources to ensure public accountability and protect public interest.
- **Cloud Security Alliance (CSA):** Specializes in best practices for secure cloud computing.

7

ISO/IEC Standards and Frameworks

- ISO and IEC often collaborate to develop global standards. Co-developed standards are labeled ISO/IEC. Notable examples:
- **ISO/IEC 27001:** Guidelines for the creation of an information security management system (ISMS) (e.g., CIA Triad).
- **ISO/IEC 27002:** Details for implementation of security controls within an ISMS.
- **ISO/IEC 27701:** Focuses on building a privacy information management system (PIMS).
- **ISO/IEC 31000:** Provides a framework for risk management.

8

System and Organization Control (SOC)

- Developed by the AICPA, SOC reports ensure service entities securely manage financial data
- **SOC 1:** Focuses on internal controls related to financial reporting, requested only by the user entity
- **SOC 2:** Assesses security, availability, processing integrity, confidentiality, and privacy.
 - *Type 1:* A point-in-time assessment of controls.
 - *Type 2:* A periodic (usually annual) review to evaluate ongoing effectiveness. Type 1 results often guide improvements before Type 2 audits.
- **SOC 3:** Summarizes SOC 2 results in a high-level report available to the public.

9



10

IT Asset Disposal and Decommissioning

1. **Sanitization:** Completely erases data from storage devices, using methods like overwriting or cryptographic erasure, based on the sensitivity of the data.
2. **Destruction:** Physically destroys the device (e.g., shredding or pulverizing) to make data retrieval impossible, often used for highly sensitive assets or when sanitization isn't sufficient.
3. **Data Retention:** Before disposal, organizations must back up or archive data that requires long-term storage for legal or regulatory reasons.
4. **Certification:** Certifications validate that sanitization or destruction processes were performed correctly and meet compliance standards, ensuring no data leaks.

11

Change Management

Its main goal is to protect the **confidentiality, integrity, and availability** of systems while maintaining smooth business operations.

This process applies to all changes, from simple updates to major system upgrades, and emphasizes clear communication with stakeholders and users.

Change management includes controls to mitigate risks and protect system security during changes.

1. **Mitigating Risks:** Temporary restrictions like allow/deny lists ensure only authorized access during updates. Planning includes analyzing downtime impacts and addressing dependencies, especially in legacy systems.
2. **Automation** streamlines change management processes, improving security and efficiency by reducing manual errors and downtime.
 - a. Automates change request submissions and tracks approvals systematically.
 - b. Schedules updates with minimal interruptions.
 - c. Ensures compliance with policies and generates detailed audit trails for all changes.

12

Business Continuity

1. **Business continuity (BC)** is an organization's ability to keep operating during and after a disaster or incident.
2. Key events affecting BC:
 1. **Disaster Recovery (DR)**: The ability to restore normal operations after a disaster.
 2. **Incident Response (IR)**: The ability to identify and address an incident effectively.
3. Organizations use three plans to handle disasters or incidents:
 - a. **Business Continuity Plan (BCP)**: Procedures for staying operational during disruptions. (Includes all business areas)
 - b. **Disaster Recovery Plan (DRP)**: Steps to restore normal operations after a disaster.
 - c. **Incident Response Plan (IRP)**: Steps to detect, respond to, and recover from an incident.

13

Aspect	Business Continuity Plan (BCP)	Disaster Recovery Plan (DRP)	Incident Response Plan (IRP)
Primary Goal	Keep critical operations running	Recover IT systems and data	Manage and contain cyber incidents
Scope	Broad (entire organization)	Narrow (IT systems)	Narrow (cybersecurity threats)
Timeline	During and after disruption	After disruption	Immediate response and resolution
Focus Areas	People, processes, resources	Technology infrastructure	Threat identification and mitigation
Example Scenario	Maintaining customer service during a ransomware attack	Restoring servers after a data breach	Investigating and stopping malware
Involves	All departments	IT/technical teams	Incident response team

14

Security Policies

1. **DLP Policy:** Outlines strategies to prevent data breaches.
2. **Password Policy:** Specifies password complexity and expiration rules.
3. **Acceptable Use Policy (AUP):** Details valid use of network resources.
4. **BYOD Policy:** Defines how personal devices connect to the network.
5. **Remote Access Policy (RAP):** Covers remote access to resources.
6. **Onboarding Policy:** Defines how new employees gain access to resources.
7. **Offboarding Policy:** Ensures terminated employees lose access to resources.
8. **Retention Policy:** Details how data and documents are archived.
9. **Credential Policy:** Manages identity verification and authentication

15

Personnel Policies

1. **Background Check Policy:** Requires checks on employees to verify trustworthiness.
2. **Job Rotation Policy:** Rotates employees to identify security gaps or procedural issues.
3. **Mandatory Vacation Policy:** Enforces employee leave to uncover hidden risks or fraud.
4. **Separation of Duties Policy:** Splits critical tasks among employees to maintain integrity.
5. **Least Privilege Policy:** Ensures employees only access data necessary for their role.
6. **Clean Desk Policy:** Requires workspaces to be free of sensitive documents.
7. **Social Media Policy:** Governs business-related use of social media.

16

Security Awareness

Anomalous Behavior Recognition

1. Security awareness also teaches employees to detect **anomalous behaviors**, which may indicate security risks:
 - a. **Risky**: Potentially harmful actions, such as accessing sensitive data without authorization.
 - b. **Unexpected**: Unusual activity, like logins from unknown locations or odd behavior patterns.
 - c. **Unintentional**: Mistakes by legitimate users, such as accidentally deleting important files.
 - d. **Situational awareness** is key to recognizing and responding to these behaviors, helping mitigate threats and improve organizational security.

17

An accounting employee changes roles with another accounting employee every 4 months. What is this an example of?

- a. Separation of duties
- b. Mandatory vacation
- ☒ c. Job rotation
- d. Onboarding

18

Gurvinder's corporate data center is located in an area that FEMA has identified as being part of a 100-year flood plain. He knows that there is a chance in any given year that his datacenter could be completely flooded and underwater, and he wants to ensure that his organization knows what to do if that happens. What type of plan should he write?

- a. A Continuity of Operations Plan
- b. A business continuity plan
- c. A flood insurance plan
- ☒ d. A disaster recovery plan

19

Caroline has been asked to find an international standard to guide her company's choices in implementing information security management systems. Which of the following would be the best choice for her?

- ☒ a. ISO 27002
- b. ISO 27701
- c. NIST 800-12
- d. NIST 800-53

20

Eric's organization has created a policy document that describes how users can and cannot use the organization's network, systems, and services. What type of policy has he created?

-
- a. Business continuity policy
 - ☒ b. An acceptable use policy
 - c. An incident response policy
 - d. This is a standard, not a policy

21

Susan has discovered evidence of a compromise that occurred approximately five months ago. She wants to conduct an incident investigation but is concerned about whether the data will exist. What policy guides how long logs and other data are kept in most organizations?

-
- a. The organization's data classification policy
 - b. The organization's backup policy
 - ☒ c. The organization's retention policy
 - d. The organization's legal hold policy

22

What standard is used for credit card security?

-
- a. GDPR
 - b. COPPA
 - ☒ c. PCI-DSS
 - d. CIS

23

Which of the following principles stipulates that multiple changes to a computer system should not be made at the same time?

-
- a. Due diligence
 - b. Acceptable use
 - ☒ c. Change management
 - d. Due care

24

Which of the following rights is not included in the GDPR?

-
- a. The right to access
 - b. The right to be forgotten
 - c. The right to data portability
 - ☒ d. The right to anonymity

25

Mark is responsible for the execution of his organization's security awareness program. Why might he deploy multiple training methods like workshops, online training, and simulations as part of the training?

-
- a. To meet compliance requirements
 - ☒ b. To address learning preferences
 - c. To decrease costs for training
 - d. To meet KPIs

26

Mikayla is working remotely in a public space and has been trained to make sure that others cannot see her screen or keyboard. What term is used to describe this?

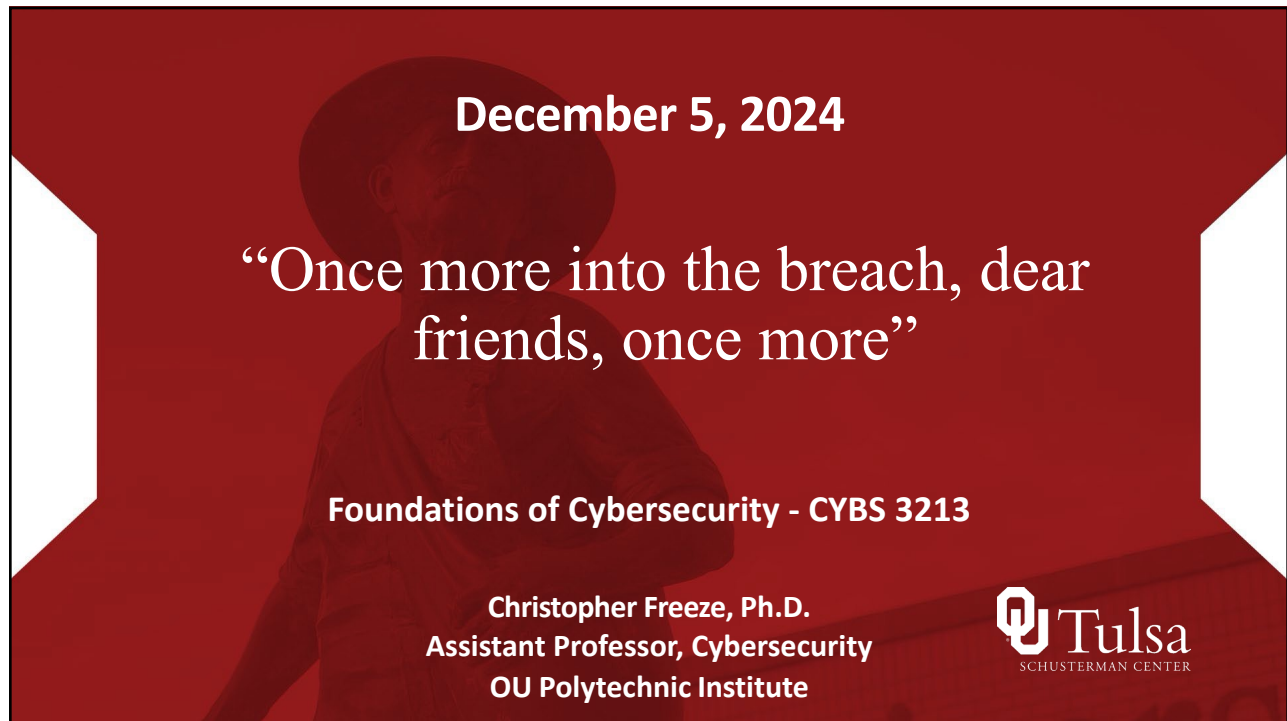
-
- a. Insider threats
 - ☒ b. Situational awareness
 - c. Social engineering
 - d. Unintentional risky behavior

27

What common terms are used to categorize anomalous behavior?

-
- ☒ a. Risky, unexpected, and unintentional
 - b. Recurring, occasional, and unique
 - c. Unintentional, insider, and accidental
 - d. Active, passive, and integrated

28




December 5, 2024

“Once more into the breach, dear friends, once more”

Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

 **Tulsa**
SCHUSTERMAN CENTER