

**August 27, 2024**

# **“What is the Weakest Link in Cybersecurity?”**

**Foundations of Cybersecurity - CYBS 3213**

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



# Checking In

- Last time, we discussed the question, “What is Cybersecurity?” (Cybercrime; Definitions; CIA Triad; AAA)
  - “Protection of connected systems and applications from cyberattacks and cybercrime.”
- What was the most important concept that you learned in the last class?
- What was the muddiest (most unclear) point during the last class?

The logo for the game show 'Weakest Link' is centered. It features the words 'WEAKEST' and 'LINK' in a bold, blue, sans-serif font, stacked vertically. A large, metallic key is positioned diagonally across the text, with its head pointing towards the top left and its shaft extending towards the bottom right. The background is a vibrant blue and purple gradient, with a large, glowing yellow ring at the top and bottom. The overall design is dynamic and futuristic.

# WEAKEST LINK

# Humans as the Weakest Link

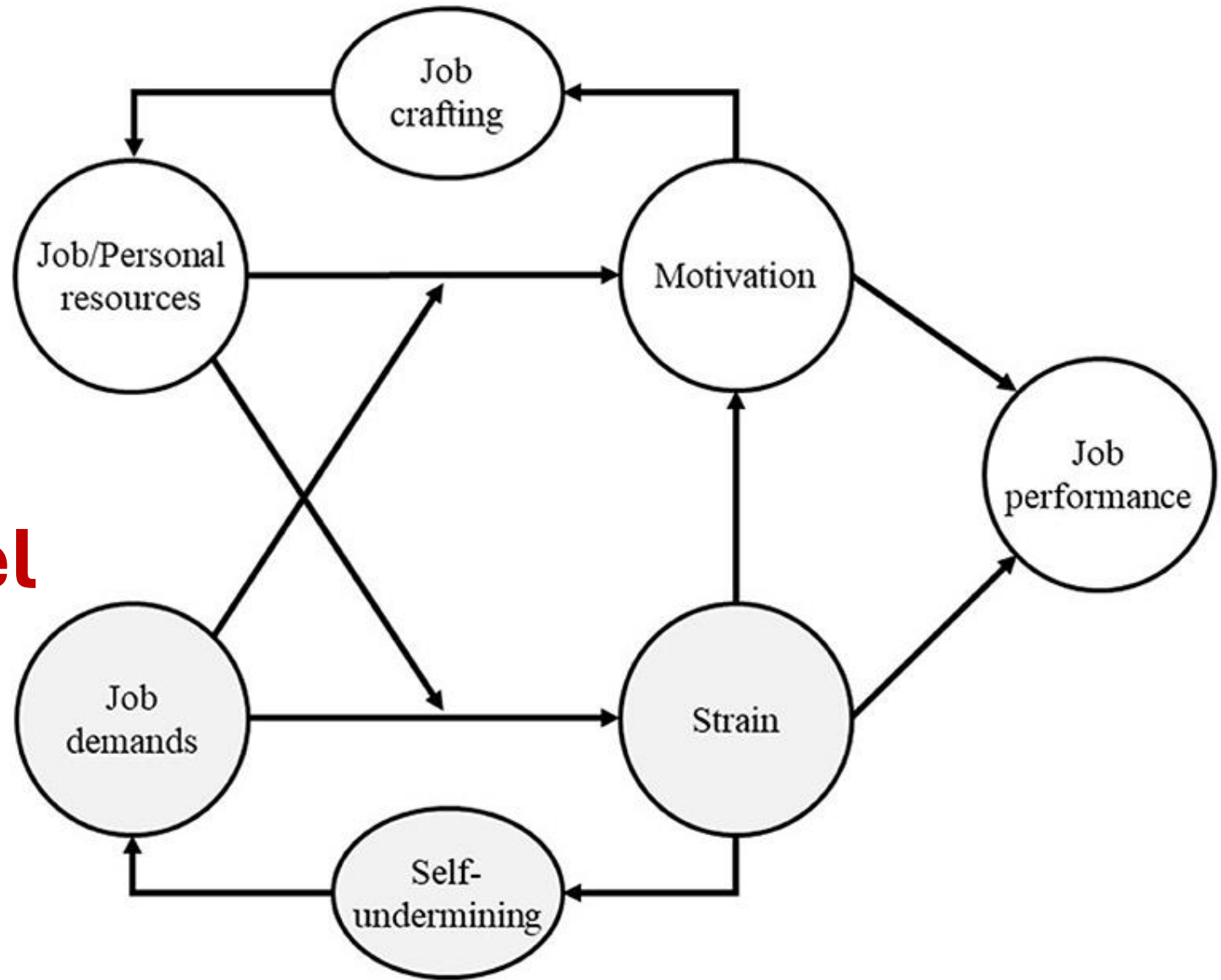
## JD-R:

- Imbalance of job demands and personal and organizational resources to cope with the demands of the job.

## Protection Motivation Theory (PMT):

- Individuals are motivated to protect themselves based on their assessment of a threat and ability to cope with it.

# Job Demands – Resource Model



## Risk cognitions

Severity

Vulnerability

=

Threat appraisal

Response  
efficacy

Self-efficacy

=

Coping appraisal

Protection  
Motivation



# Security Terminology

- |                          |   |
|--------------------------|---|
| a. Asset                 | a. Something of value.  |
| b. Vulnerability         | b. Weakness in system, process, or management that can be exploited.                            |
| c. Threat                | c. Action that could cause harm, not the actual compromise.                                     |
| d. Threat actor or agent | d. Person who can carry out a threat or exploit the vulnerability causing an actual compromise. |

# Security Terminology

- |                      |  |
|----------------------|--|
| d. Attack vector     | d. Pathway used by attacker to access the system.                |
| e. Attack surface    | e. All the points on a system where vulnerability could happen.  |
| f. Threat likelihood | f. Probability that a threat agent will exploit a vulnerability. |
| g. Risk              | g. Exposure to some type of danger.                              |



# Cybersecurity Risk - 3 Aspects (IAE)

## 1. Identification –

- Identify and prioritize assets, events, vulnerabilities, and controls.

## 2. Analysis –

- Determine likelihood of event and its impact.

## 3. Evaluation –

- Determine, prioritize, and understand the significance of the risk level; recommend actions; document results.

# The Four Choices of Risk - AATM

1. Acceptance: Low risk, not worth the cost, remote possibility.
2. Avoidance: Assess zero chance of risk; no USBs.
3. Transference: Transfer risk for damages; cyber-insurance.
4. Mitigation: Most common approach; reduce likelihood of event occurring or the impact.

In cybersecurity, what is a flaw or weakness that allows an attacker to bypass security protections?

---

- a. Access
- ☒ b. Vulnerability
- c. Threat
- d. Risk

# Results of Cybersecurity Attack

- a. Data breach – data is exposed to compromise.
- b. Data loss – actual loss of the data.
- c. Data exfiltration – unauthorized transfer of the data.

# What do we call the people who act as threat actors?

1. Hackers
2. Script kiddies
3. Brokers
4. Insiders
5. Cyberterrorists
6. Hacktivists
7. State Actors

Which of the following is NOT  
classified as an insider?

---

- a. Business partners
- b. Contractors
- ☒ c. Cybercriminals
- d. Employees

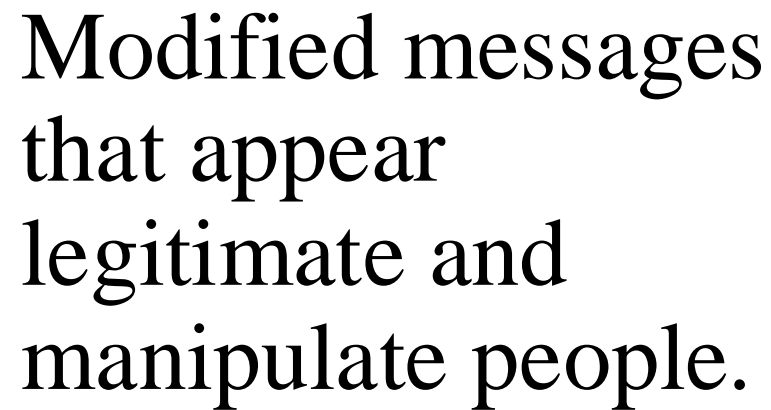
## Significance of Cyber-attacks:





# World's Biggest Data Breaches and Hacks

- <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



- Phishing – usually done by email.
- Vishing – via phone
- Smishing – SMS text
- Spear phishing – aimed at specific group
- Whaling – High value CEOs

# Personal Influence Principles - AFIT

**Authority** - A target believes the attacker is in a position of power over the target.

**Familiarity** - A target believes the attacker is a known individual or associated with a known organization.

**Intimidation** - A target believes the attacker can inflict harm.

**Trust** - A target believes the attacker is trustworthy because the attacker has built a connection with the target.

# Social Influence Principles – CSU

**Consensus** - A target believes the attacker's suggested action has been done by others.


**Scarcity** - A target believes the attacker's suggested action has limited availability.

**Urgency** - A target believes the attacker's suggested action has a time constraint.

CNN Money



# Whaling Attack

 **Hitachi Systems Security Inc.**

<https://www.youtube.com/watch?v=BU8h9GzdlSw>



# 72% of Senior Executives Targeted by Cyberattacks in the Last 18 Months

GetApp's survey of cybersecurity professionals reveals US senior executives are the most at risk for cyberattacks, and businesses must prepare against more persistent, advanced threats

August 19, 2024 08:00 AM Eastern Daylight Time

STAMFORD, Conn.--(BUSINESS WIRE)--72% of surveyed cybersecurity professionals in the past 18 months. This trend, however, is growing sophistication of attacks, with 27% of the attacks.

## INSIGHT: US technology executive tricked into sending \$400,000 to scammers while trying to buy \$1.6m home

AML, FINANCIAL CRIME, US

★ PREMIUM

July 24, 2024

World / Asia

### Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'



By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024






2023 CRIME TYPES

By Complaint Count				
Crime Type	Complaints		Crime Type	Complaints
Phishing/Spoofing	298,878		Other	8,808
Personal Data Breach	55,851		Advanced Fee	8,045
Non-payment/Non-Delivery	50,523		Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223		Overpayment	4,144
Investment	39,570		Data Breach	3,727
Tech Support	37,560		Ransomware	2,825
BEC	21,489		Crimes Against Children	2,361
Identity Theft	19,778		Threats of Violence	1,697

# What is the goal of a phishing attack?

- a. To capture keystrokes.
- b. To send a fraudulent email to a user.
- c. To duplicate a legitimate service.
-  d. To trick a user into surrendering personal information.

Which of the following principles is NOT used in a social engineering attack?

a. Intimidation

b. Consensus



c. Unfamiliarity

d. Authority

Which of the following principles is NOT a risk associated with using a social media/networking account?

- ☒ a. Users may not be trusting of others.
- b. Accepting friends may have unforeseen consequences.
- c. Social media and networking security is confusing.
- d. Personal data can be used maliciously.

## Key Take-Aways:

1. Humans are the weakest link in cybersecurity
2. Being a good cybersecurity analysts requires identifying, analyzing, and evaluating risk.
3. The various ways criminals use social engineering must be understood and mitigated.

# Prepare Media Article and Presentation

---

- Relevance to class topic (20%):
- Understanding of the issue (30%):
- Clear and organized summary (30%)
- Engagement with class (20%):
- **IMPORTANT:** Upload your article before the next class and provide a few sentences to answer each of the first three questions. (1 page max)
- Think about teaching the topic.





**August 29, 2024**

# **Presentations**

**Foundations of Cybersecurity - CYBS 3213**

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

