



# CYBERSECURITY AND YOU (WHY IS IT IMPORTANT AND WHAT IS MY ROLE?)



*Presented by Rutgers WIT+ members of the  
Information Security Office,  
Compliance and Training Team*





- 01. INTRODUCTIONS
- 02. IMPORTANCE OF CYBERSECURITY IN HIGHER ED
- 03. CHALLENGING THE NARRATIVE: CYBERSECURITY IS EVERYONE'S RESPONSIBILITY
- 04. THE HUMAN ELEMENT: THE IMPORTANCE OF AWARENESS, CULTURE & COMPLIANCE
- 05. KEY TAKEAWAYS & FINAL THOUGHTS
- 06. Q&A

# AGENDA



# INTRODUCTIONS



## Sharkirah Foote



- Compliance and Training Manager at Rutgers since 2021
- Over 14 years of Cybersecurity experience in Higher Education
- Current role includes research data security, data loss prevention, IT policy development and security awareness and training strategy



## Catharine Tarquinio

- Information Security Awareness & Training Analyst at Rutgers since January 2023
- 7 years of cybersecurity experience in Higher Education
- Current role includes awareness campaigns, events, training, compliance, and community outreach

02.

# The Importance of Cybersecurity in Higher Ed



# THE IMPORTANCE OF CYBERSECURITY IN HIGHER EDUCATION

**Protecting Sensitive Data:** Higher education institutions store vast amounts of sensitive data, including student records, research data, and financial information. Institutions hold the responsibility for preventing identity theft, fraud, etc.

**Maintaining Trust:** Implementing robust security controls and facilitating a security-first mindset helps maintain the trust of staff, faculty, students, their families, and other stakeholders. A data breach can severely damage an institution's reputation and erode this trust.



# A FEW RECENT EXAMPLES:

**August 2023:** A significant cyber attack at a university during the first week of classes halted internet services and affected approximately 230,000 students.

**September 2023:** At another university, three decades' worth of sensitive information about applicants, students, and employees was accessed in a data breach, leading to multiple lawsuits.



# THE IMPACT

**Operational Disruption:** Cyber attacks disrupt educational processes, leading to downtime and loss of productivity.

**Financial Costs:** The average cost of recovering from a data breach is nearing \$4 million\*, including expenses related to data recovery, legal fees, fraud protection for affected individuals, and potential fines.

**Reputational Damage:** A breach harms the institution's reputation, affecting student enrollment and impacting important relationships like research and funding partnerships.



\*2024 Splunk State of Security Report

# KEY CHALLENGES



## THIRD-PARTY RISKS

Universities rely on third-party applications to deliver an increasing number of services, widening the attack surface



## DIVERSE USER POPULATION

Students, faculty and staff with differing levels of awareness, plus high turnover, increases the risk of human error



## DECENTRALIZED IT INFRASTRUCTURE

Universities may have multiple campuses with varying policies and security protocols

## FREEDOM VS. SECURITY

Universities thrive on research and collaboration, which can conflict with strict access control and security policies



## BUDGET CONSTRAINTS

Budget limitations and fund prioritization frequently restricts the ability to invest in advanced cybersecurity tools and personnel



## REGULATORY COMPLIANCE

Universities have a plethora of federal and state regulations to comply with, which can be complex or vague and may change frequently



## LACK OF CYBERSECURITY SKILLS

Professionals that have the diverse set of skills universities need to address problems aren't easy to find, leading to universities going without





03.


# Challenging the Narrative: Cybersecurity is Everyone's Responsibility



# UNIVERSITIES ALREADY IMPLEMENT A VARIETY OF TECHNICAL CONTROLS TO PROTECT THEIR DATA, LIKE...


- Multi-factor authentication (MFA)
- Firewalls
- Encryption
- Network segmentation
- Endpoint protection
- Access controls
- Data loss prevention (DLP)
- Software updates and patching



- 
01. TARGET IDENTIFICATION & RESEARCH
  02. WEAPONIZATION
  03. DELIVERY & DECEPTION
  04. EXPLOITATION
  05. INSTALLATION & CONTROL
  06. ACT ON OBJECTIVE
  07. DISENGAGEMENT/EXIT

# COMMON ATTACK CHAIN



- 
01. TARGET IDENTIFICATION & RESEARCH
  02. WEAPONIZATION
  03. DELIVERY & DECEPTION
  04. EXPLOITATION
  05. INSTALLATION & CONTROL
  06. ACT ON OBJECTIVE
  07. DISENGAGEMENT/EXIT

**Which step in the chain can be thwarted by a human when technical controls fail?**

# COMMON ATTACK CHAIN



01. TARGET IDENTIFICATION & RESEARCH



02. WEAPONIZATION

03. DELIVERY & DECEPTION



04. EXPLOITATION



05. INSTALLATION & CONTROL



06. ACT ON OBJECTIVE



07. DISENGAGEMENT/EXIT



**Nearly ALL of them!**

**COMMON  
ATTACK CHAIN**



# THE DYNAMIC IS CHANGING...


Universities are increasingly being targeted by sophisticated cyber attacks aimed at stealing valuable student, research, and even medical data (for institutions operating healthcare facilities). These attacks, known as **advanced persistent threats (APTs)**, use ransomware (malware that demands a ransom) to steal or encrypt data.

Historically, malware was easily executable via a link or attachment. Because technological security controls are getting more advanced, attackers are now investing heavily in targeting the human element via **social engineering**. Therefore, we need to understand how humans can be hacked, as well as technology.

04.

# The Human Element: The Importance of Awareness, Culture & Compliance





“A cybersecurity culture refers to the collective mindset, behavior, and practices of individuals within an organization regarding their approach to cybersecurity. It is about fostering an environment where every single person – from top management to employees at all levels – understands the importance of cybersecurity. Plus, where every individual actively helps protect the organization's digital assets and information from cyberthreats.”

–Michel Sahli, Adnovum





A

## AWARENESS

Awareness begins with communication and understanding. Conveying the importance of cybersecurity to a diverse university community requires taking creative and hands-on approaches to ensure everyone is prepared.

Departments should incorporate cybersecurity controls into internal procedures that reflect the diverse needs of the university community. Avoid focusing on "checking the box" and address why we need to security in the first place.

## COMPLIANCE



C




T

## TRAINING

Training programs should use real-world scenarios incorporating a variety of examples to make the content more relatable and should be focused on providing the appropriate tools for your team's toolbox, NOT as a punishment.

Managers must prioritize cybersecurity and demonstrate commitment by "walking the walk", regularly communicating the importance of cybersecurity to the community while also displaying the behaviors they want to see.

## LEADERSHIP



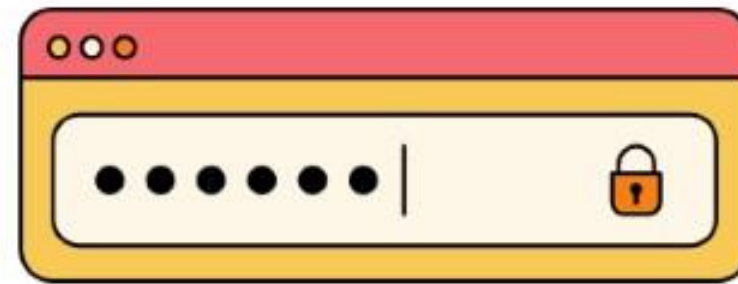
L



# PRACTICAL STEPS YOU CAN ACT ON TODAY!



- **Practicing safe browsing habits**
  - Get in the habit of hovering before clicking
  - Verify website authenticity before entering your password
  - Use secure connections (Rutgers Secure WiFi or VPN)



- **Password management**
  - Create strong passphrases
  - Avoid anything pertaining to you than can be found out online
  - Don't reuse them!
  - Use a password manager



- **Recognizing social engineering attempts**
  - Keep up to date on common red flags; they change constantly
  - **If you see something, say something**; report immediately and share your concerns with your manager or local IT!



05.

# Key Takeaways & Final thoughts



# WHY DOES CYBERSECURITY MATTER TO ME?

## High levels of staff awareness results in:

- Faster reporting of cyber threats and less successful attacks, leading to a more secure organization
- Lower cyber-insurance costs
- Compliance with regulatory mandates and best practices
- Lowered personal risk! Data shows that employees who practice secure habits at work tend to use them in their personal lives, and vice versa

*Why does it*  
**MATTER?**

**Because cybercriminals are now directly attacking humans, not computers, our awareness MUST complement technical approaches!**



# Q&A





# THANK YOU

OIT–Information Security Office  
Compliance and Training Team

Sharkirah Foote & Catharine Tarquinio

[iso\\_compsat@oit.rutgers.edu](mailto:iso_compsat@oit.rutgers.edu)

Report phishing attempts to [abuse@rutgers.edu!](mailto:abuse@rutgers.edu)

