THE UNIVERSITY OF
TENNESSEE
HEALTH SCIENCE CENTER

Faculty Senate
faculty@uthsc.edu

Memphis
Knoxville
Chattanooga
Nashville

FACULTY SENATE MINUTES

UTHSC Faculty Senate Meeting

Zoom Monthly Meeting
January 14th, 2025

Attendance: (senators, administrators, and faculty)

Attending: Anna Bukiya, April Hilsdon, April Hilsdon, Ashton Brooks, Ayman Abdul H Aldayeh, Ben Maddox, Brett Wilson, Carrie Harvey, Chalet Tan, Cheran Elangovan, Chris Madeksho, Chris Wood, Cindy Russell, Dan Young, David W Petersen, Dina Filiberto, Donna Lynch-Smith, Fuming Zhou, Hassan Almoazen, Helmut O Steinberg, Hitesh Sandhu, Imran Quraishi, Ioannis Dragatsis, James M. Lewis, Jaqueline D Venturin, Jason Yaun, Jayc Sedlmayr, Jeff Kalmowicz, Jeffry Bieber, Jess Wesberry, Jill M. Maples, Karen J Derefinko, Karine Guerrier, Katherine L March, Kevin William Freeman, Kim Carter, Kimberly Morris, Kristen Bettin, Laura T Reed, Laurentia Nodit, Laxmichaya Sawant, Lisa Beasley, Mahmoud Hassouba, Maria Carrillo, Mary Erickson, Michelle Lynn Abramovitz, Molly Erickson, Nabajit Choudhury, Nina K Sublette, Paul J Koltnow, Peter Buckley, Phyllis Richey, Ramesh Krishnan, Ranjit Philip, Rebecca Reynolds, Rima Zahr, Ron Espinal, Sandeep Chilakala, Scott Hollis, Shaunta' Chamberlin, Shelley White-Means, Stephen Pishko, Stephen Rauls, Steven M Doettl, Tauheed Ishrat, Tayebeh Pourmotabbed, Ted Cory, Terrance G Cooper, Thaddeus A Wilson, Tracy McClinton, Tyler Melton, Valarie Fleming, Vickie Baselski, Yanhui Zhang, Yi Lu

Faculty Senate Meeting

Meeting was called to order at 4:01 pm CST/5:01 pm EST

Presiding: Dr. Tracy McClinton, President

Business Discussion with Dr. Tracy McClinton
Discussion and Approval of the December 10, 2024 minutes

- The floor was opened for discussion of the December 10, 2024 meeting minutes. Two edits were recommended. Dr. Anna Bukiya motioned to accept the minutes as written. Motion was seconded by Dr. Terry Cooper
- Poll Everywhere Vote:
  - Approve: 46
  - Do not approve: 0
  - Abstain: 2

Discussion on Cybersecurity with Chris Madeksho, Office of Cybersecurity (appendix A)

- Targeted training for higher education is necessary, with activities for specific groups
- Have been working to develop UT Health Science Center training, rather than generic videos that we currently use
- Human risk is the largest factor for data breaches, number of data breaches is exploding.
  - Can include misuse of access, stolen credentials
- Training is boring and repetitive, lack of retention of details, and fear and confusion on the topic
- .edu domain address is perceived as highly trusted and safe, which bypasses spam filters and leads to greater email deliverability
  - Makes .edu accounts especially desirable for attacks
- Credentials/emails are worth a lot more from .edu rather than other email domains
- Tailored training approaches
  - Students: Securing personal devices, social media risks
  - Faculty: protecting research and intellectual property, better data handling

  - Researchers: collaboration practices and safeguarding information
  - Staff: Data handling, secure system access controls to ensure data integrity
- Targeted training
  - Risk assessments
  - Develop content for these risks
  - Deliver training to people
  - Measure the impact of the training
- What types of things are being investigated right now?
  - Personal laptops stolen and HIPAA protected information that was on the laptop.
  - Education opportunity that there are better ways to store/share data
- Thousands of failed foreign logins every quarter for the university, from a variety of countries
  - Underscores the importance of strong passwords, 2 factor authentication
- Phishing emails
  - 100,000 phishing emails received at the University for month, but spam filters catch 98% of them. This is a significant improvement over the last year.
- Need support from the faculty senate on developing targeted training specific to the University
- Senate computing committee is going to be working with Chris Madeksho on the early stages of this
- Questions/Discussion
  - Suggestion on tailoring training for people who have higher need/access for protected data/materials
    - Currently students are not part of training due to HIPAA requirements
    - Employee training is through the KATE system, which students do not have access to
  - Is it possible to identify specific risk groups, where failed log-ins were, etc?

  - Data that is collected provides some of this information: data leakage, personal, etc.
- What can be done to make sure that students have access to the training that they need?
  - Working to develop training for Colleges/students, especially during orientation, as well as annual refreshers
- Where could information for students be held?
  - Course syllabi could be a potential source for language
    - May be some new software/policies for syllabi in the future
  - Making sure material is easily visible, put on one screen for previews
  - Meet with students through SGAEC
- Encryption of data/emails what needs to be done?
  - Need to be concerned due to the risk of stolen credentials, even if it is kept within UTHSC
  - Can use Vault, or type encrypt in the subject line of the email.
- Discussion on the UT Vault
  - Original encryption approach for the UT system
  - Highly recommended for large files
- What if you are working with other universities on projects?
  - Depends on the data, some may need to be encrypted for transit, or use UT Vault
- Onedrive/sharepoint
  - Secure and HIPAA compliant per Microsoft, but there has not been an internal audit
- Do emails to students need to be encrypted depending on what is included?
  - UT Health Science Center is a covered entity, so we need to be HIPAA compliant

New Business

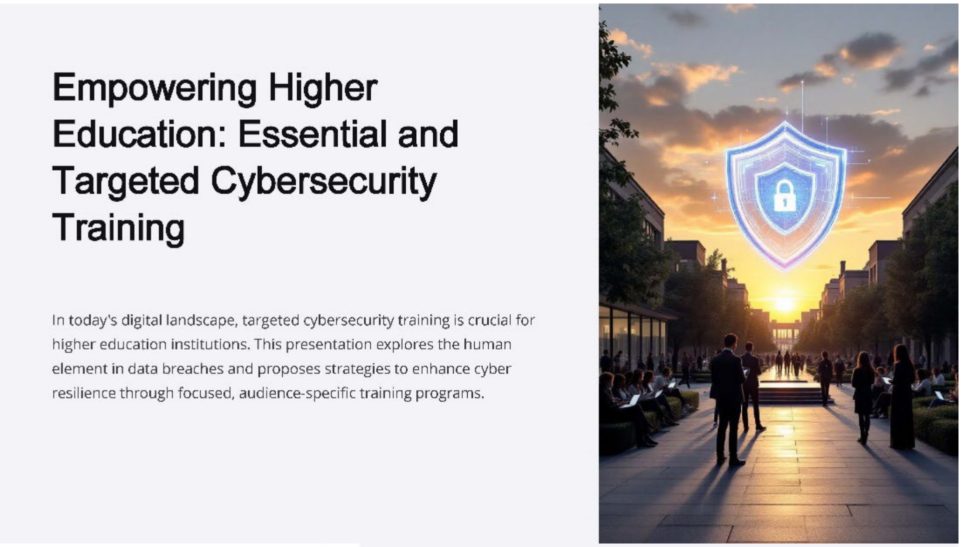
- **Infographic for UT Health Science Center Faculty**
    - Way to promote the faculty
    - Is being done by other parts of the UT system
    - Infographic from UT Knoxville shared on what they are doing as a University
    - Goal is to develop something that is unique for the Health Science Center, as well as our reach
    - Much of this data is available in the office of Faculty affairs, digital measures, etc.
- **Honor code**
    - FSEC has been working with Vice Chancellor Charlie Snyder on revising the honor code, more details to come

Announcements

The meeting was adjourned at 4:58 pm CST/5:58 pm EST.

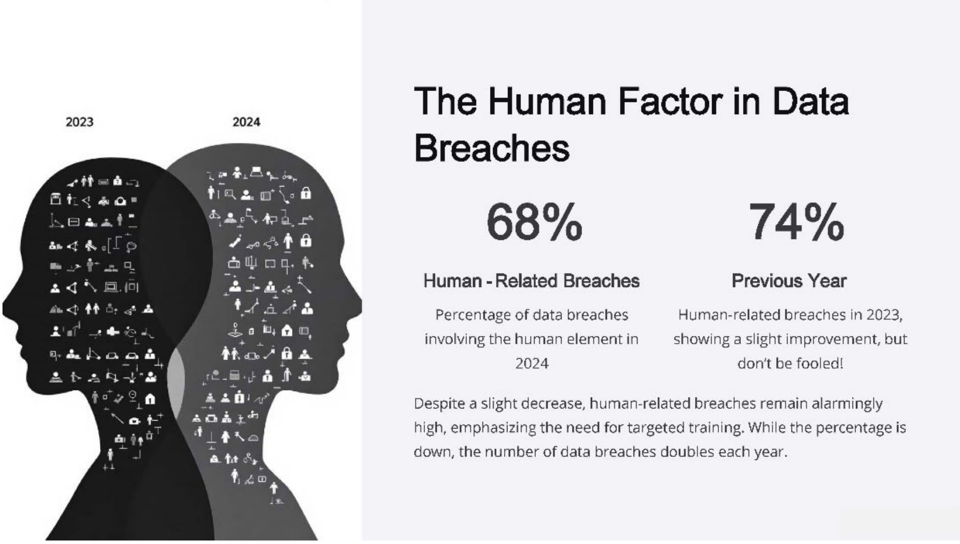
Respectfully Submitted,
Dr. Ted Cory
Faculty Senate Secretary

Appendix A: Presentation on cybersecurity



Empowering Higher Education: Essential and Targeted Cybersecurity Training

In today's digital landscape, targeted cybersecurity training is crucial for higher education institutions. This presentation explores the human element in data breaches and proposes strategies to enhance cyber resilience through focused, audience-specific training programs.



The Human Factor in Data Breaches

68%

Human - Related Breaches

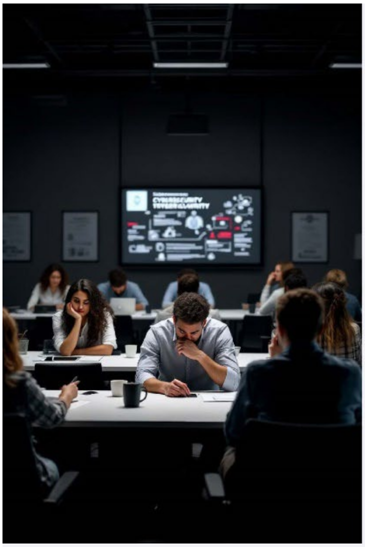
Percentage of data breaches involving the human element in 2024

74%

Previous Year

Human-related breaches in 2023, showing a slight improvement, but don't be fooled!

Despite a slight decrease, human-related breaches remain alarmingly high, emphasizing the need for targeted training. While the percentage is down, the number of data breaches doubles each year.



Current Training Challenges

Boring and Repetitive

Employees often find cybersecurity training unengaging and monotonous.

Lack of Retention

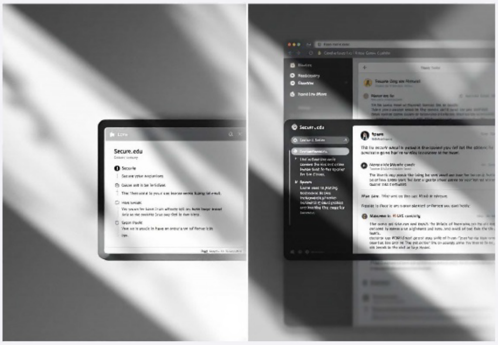
Even security professionals struggle to recall specific training content.

Fear and Confusion

Many people can feel overwhelmed or scared by cybersecurity topics.

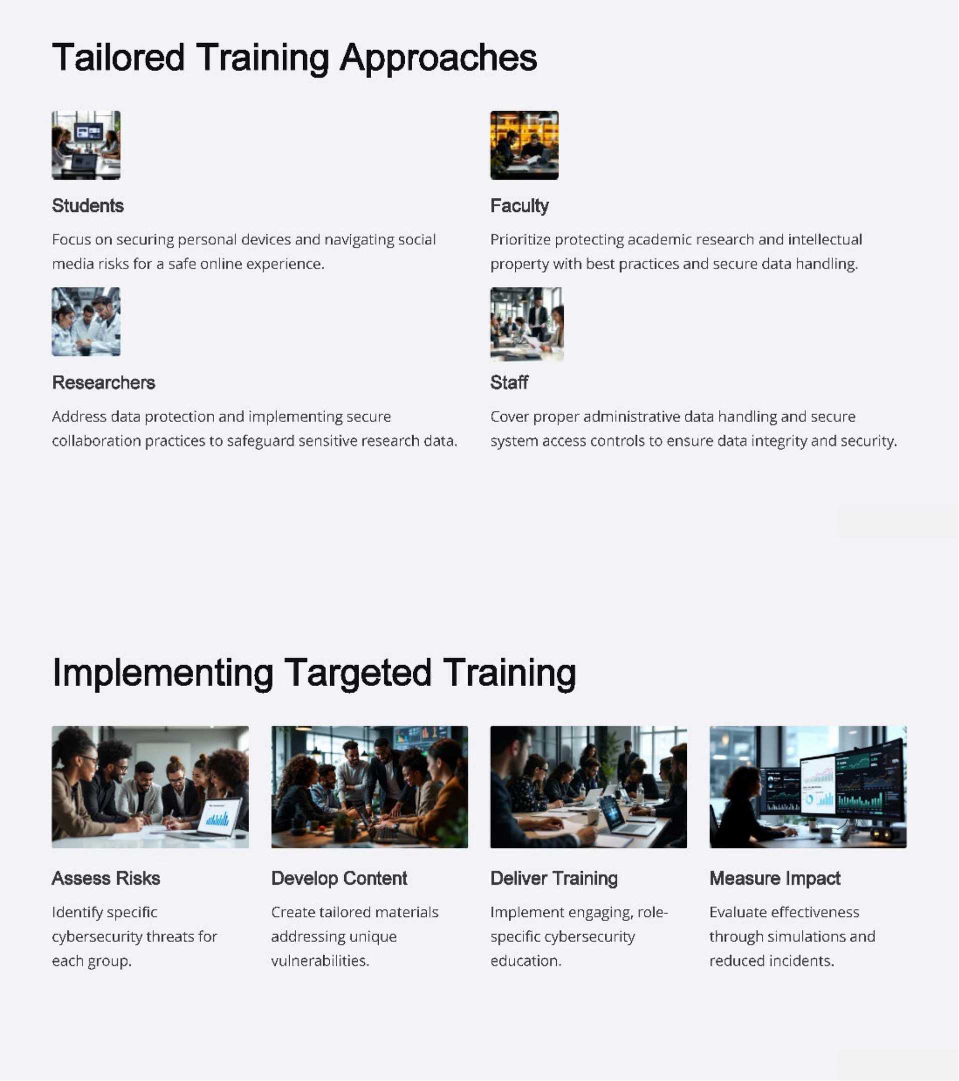
The .edu Email Vulnerability

An example of a high risk



Accredited institutions' exclusive access to .edu domain addresses creates a perception of inherent trust and safety. This often bypasses spam filters and leads to greater email deliverability, which can be both a benefit and a security vulnerability.

This high level of perceived trust makes .edu emails especially desirable to phishing attacks and other malicious activities. As users are more likely to trust messages from these domains, these attacks often result in higher success rates.



Tailored Training Approaches

Students

Focus on securing personal devices and navigating social media risks for a safe online experience.

Faculty

Prioritize protecting academic research and intellectual property with best practices and secure data handling.

Researchers

Address data protection and implementing secure collaboration practices to safeguard sensitive research data.

Staff

Cover proper administrative data handling and secure system access controls to ensure data integrity and security.

Implementing Targeted Training

Assess Risks

Identify specific cybersecurity threats for each group.

Develop Content

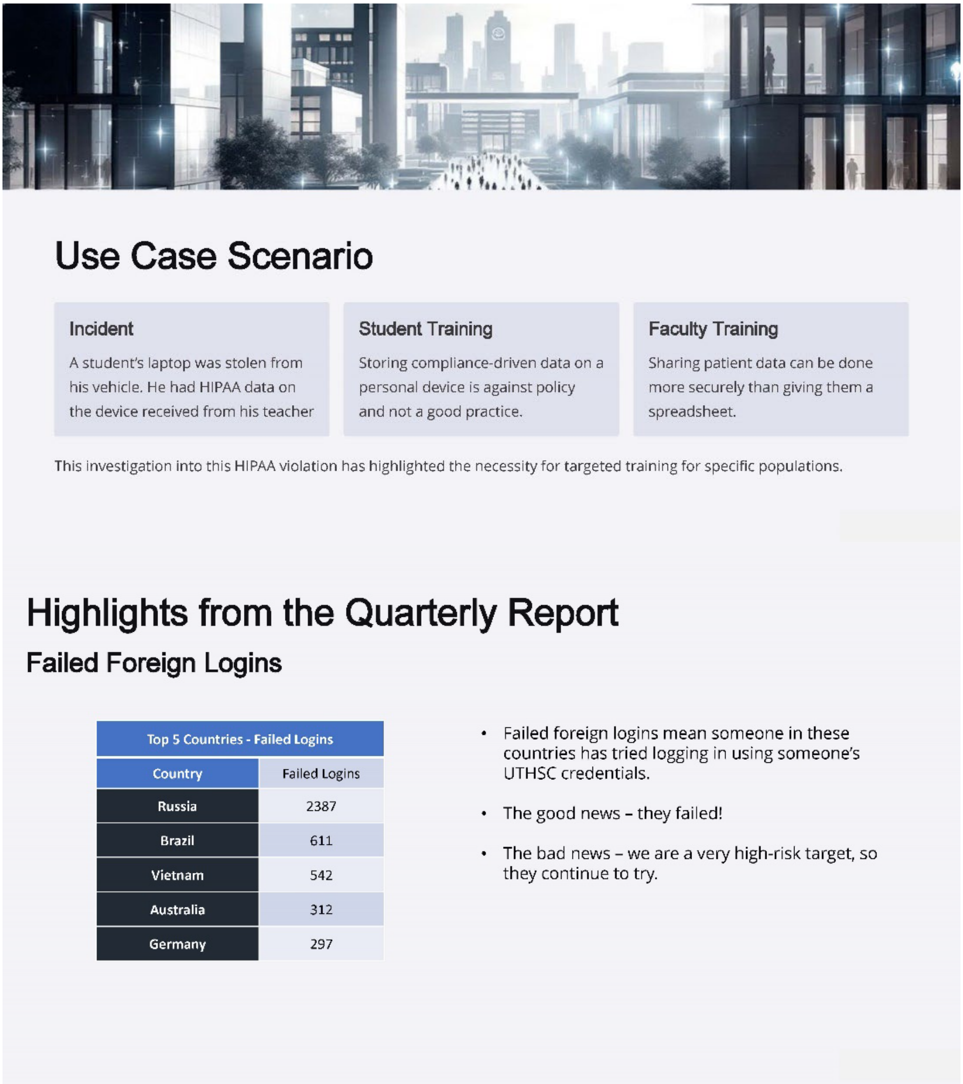
Create tailored materials addressing unique vulnerabilities.

Deliver Training

Implement engaging, role-specific cybersecurity education.

Measure Impact

Evaluate effectiveness through simulations and reduced incidents.



Use Case Scenario

Incident

A student's laptop was stolen from his vehicle. He had HIPAA data on the device received from his teacher

Student Training

Storing compliance-driven data on a personal device is against policy and not a good practice.

Faculty Training

Sharing patient data can be done more securely than giving them a spreadsheet.

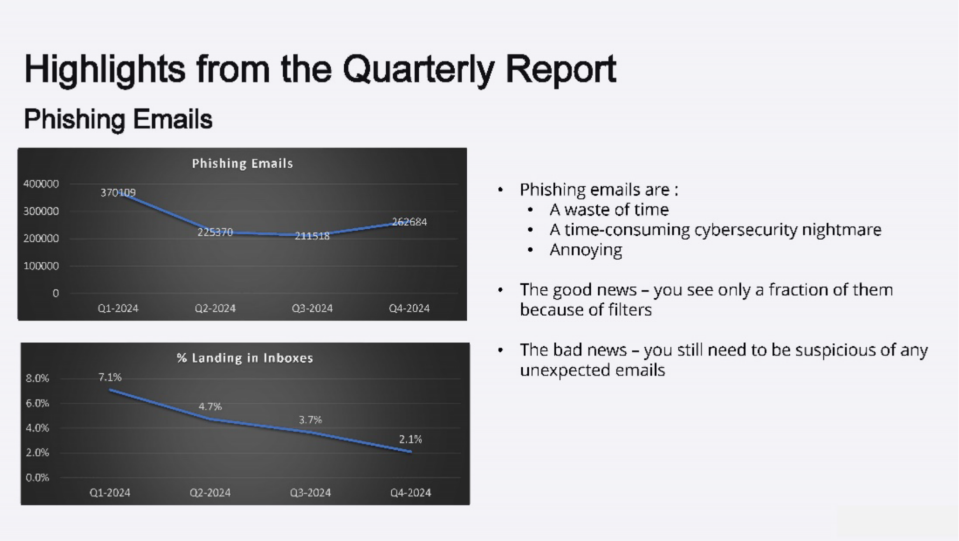
This investigation into this HIPAA violation has highlighted the necessity for targeted training for specific populations.

Highlights from the Quarterly Report

Failed Foreign Logins

Top 5 Countries - Failed Logins	
Country	Failed Logins
Russia	2387
Brazil	611
Vietnam	542
Australia	312
Germany	297

- Failed foreign logins mean someone in these countries has tried logging in using someone's UTHSC credentials.
- The good news – they failed!
- The bad news – we are a very high-risk target, so they continue to try.



Highlights from the Quarterly Report

Phishing Emails

- Phishing emails are :
  - A waste of time
  - A time-consuming cybersecurity nightmare
  - Annoying
- The good news – you see only a fraction of them because of filters
- The bad news – you still need to be suspicious of any unexpected emails