Federal Information Security Educators (FISSEA)

Winter Forum

February 11, 2025

1:00pm – 4:00pm ET

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Notes and Reminders

Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.

Webinar Recording: This webinar and the engagement tools will be recorded. An archive will be available at www.nist.gov/fissea.

Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.

CE/CPE credits: The CEU form will be available on the event page after the event.

Welcome and Opening Remarks

Marian Merritt
Deputy Director of NICE/FISSEA Lead
National Institute of Standards and Technology

Frauke Steinmeier
FISSEA Co-Chair

Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates+subscribe@list.nist.gov

Volunteer for the Planning Committee
https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee

Serve on the Contest or Award Committees
Email fissea@nist.gov

Submit a presentation proposal for a future FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations

EXCITE: EXploring the enhancement of Cyber security training through Immersive TEchnology

Dr. Sandra Scott-Hayward

QUB ACE-CSE Director

Queen's University Belfast

QUEEN'S
UNIVERSITY
BELFAST

EXCITE: EXploring the enhancement of Cyber security training through Immersive TEchnology

Dr. Sandra Scott-Hayward, QUB ACE-CSE Director

FISSEA Winter Forum – 11 February 2025

What is the ACE-CSE?

https://www.qub.ac.uk/ace-cse/

QUB | ACE-CSE: WHO WE ARE

Queen's is an ACE-CSE. An ACE-CSE is awarded from the National Cyber Security Centre (NCSC) to universities demonstrating excellence in cyber security education.

Our diverse ACE-CSE team is led by Dr Sandra Scott-Hayward from the School of Electronics, Electrical Engineering and Computer Science (EEECS), and is made up of staff from each faculty and professional services including Information Services, People and Culture, and Careers.

Together, we are delivering Queen's cyber security strategy to strengthen cyber security awareness and knowledge across all education pathways, operational areas of the institution and the wider community.

WHAT WE DO

We teach a range of cyber security modules to undergraduate students in the School of EEECS. Our certified Master's degree in Applied Cyber Security has been running since 2014. As part of developing cyber security expertise across degree pathways, we offer joint courses between Cyber Security and Law at Master's level, and offer guest cyber security lectures in multiple disciplines. Within our Leverhulme Interdisciplinary doctoral training programmes (LINCS and LINAS), postgraduate scholars explore cyber security challenges from a societal, economic and governmental perspective.

Since its foundation in 2000, the Centre for Secure Information Technologies (CSIT) at Queen's has developed a strong reputation in this critical technology area. We have been recognised as an ACE-CSR since 2011. CSIT played a leading role in the formation and evolution of the local cyber security cluster, NI Cyber. Our strong industry engagement enables us to offer our students access to a vibrant cyber security cluster, and to provide a pipeline of high-quality graduates with skills that are relevant for the future.

Find out more about what we've been up to over the last few months in our newsletter.

Gold Award

in association with National Cyber Security Centre

Department for Science, Innovation & Technology

Academic Centre of Excellence in **Cyber Security Education**

QUEEN'S UNIVERSITY BELFAST

Gold Award

in association with National Cyber Security Centre

Department for Science, Innovation & Technology

Academic Centre of Excellence in **Cyber Security Education**

QUEEN'S UNIVERSITY BELFAST

ACE-CSE Student Cyber Security Awareness Training

Aim: To develop your understanding and awareness of cyber security

Why? As an Academic Centre of Excellence in Cyber Security Education (ACE-CSE), we believe that each student should have the opportunity to learn good cyber security practices that will benefit them in their student, work, and social lives.

What? A suite of cyber security immersive experiences presented in virtual 3D student-oriented scenarios (web application) supported with a set of resources to read/watch/do to learn more about good cyber security practices.

Gold Award

in association with National Cyber Security Centre

Department for Science, Innovation & Technology

Academic Centre of Excellence in **Cyber Security Education**

QUEEN'S UNIVERSITY BELFAST

EXCITE – Overall Objective

The specific aim of EXCITE is to explore the potential to increase the efficacy of cyber security training for students through the use of immersive experiences supported by augmented and virtual reality (AR/VR) design.

Motivated by:

- Gap in provision of cyber security awareness training to 3rd-level students
- Low efficacy of 1-D/2-D training materials

QUEEN'S UNIVERSITY BELFAST

EXCITE – Phase 1

Explored the cyber security experience of a diverse, multi-disciplinary group of third-level students, and the suitability and effectiveness of a range of cyber security training materials.

Format/Presentation/Structure (FPS)

FPS1	Case studies or characters that bring the scenario to l
FPS2	The capability for the student to self-check their knowl example, the inclusion of quizzes with explanations pr enhance learning.
FPS3	The opportunity for the student to apply the knowledg 3D technology to recreate conditions, which mirror rea is likely to encounter in their daily lives. In particular, i used to provide an opportunity for the student to apply stressful conditions.

Content

C1	Content which is directly relevant and relatable to student life. For example, the importance of backing up student work.
C2	Coverage of the "Digital Footprint".
C3	Coverage of best cyber security practice with social media.
C4	Coverage of cyber security at home/in student accommodation.
C5	Specific information for international students who may be especially vulnerable to cyber security attack due to their lack of familiarity with existing practices in the UK and/or use of multiple devices across different networks and regions.
C6	Practical guidance as to how to respond to a cyber security incident or how to apply cyber security best practices. For example, how to minimise exposure to cyber security attacks, what tools to use (e.g., password manager), what technical actions to take, and what to do if subjected to an attack.
C7	Training and guidance about use of tools such as Microsoft Teams, Zoom, TeamViewer etc.

EXCITE Phase 2 - Objective

Phase 2 focused on the **design and development** of a suite of cyber security immersive experiences presented in virtual 3D student-oriented scenarios e.g., student residence, university computer lab, coffee shop.

Two versions of the immersive experiences have been developed:

- A desktop application available for students to download and run on their own device supports broad accessibility of the training
- A VR headset application provides the fully immersive environment for focused, small group training.

QUEEN'S UNIVERSITY BELFAST

EXCITE Phase 2 – Study Design

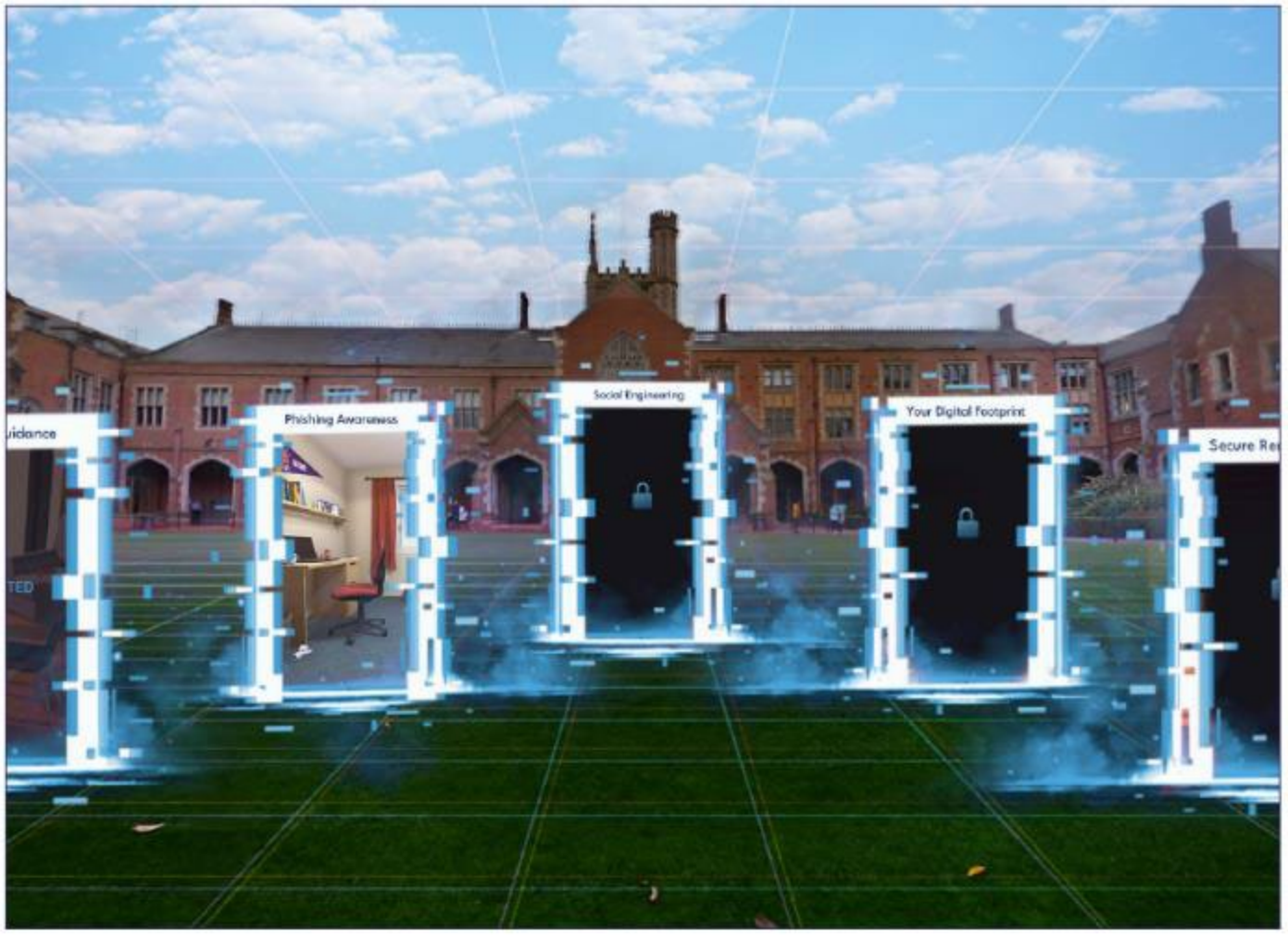
- Interdisciplinary - Faculty of Arts, Humanities, and Social Sciences (AHSS), Faculty of Medicine, Health, and Life Sciences (MHLS), and the Faculty of Engineering and Physical Sciences (EPS))
- Student-oriented – input from Phase 1 plus three stages of feedback – storyboards, initial version of 3 experiences, full VR suite of experiences.
- Partnership with Zubr Virtual Reality (https://zubr.co), an organization experienced in immersive digital content creation for training/learning.

QUEEN'S UNIVERSITY BELFAST

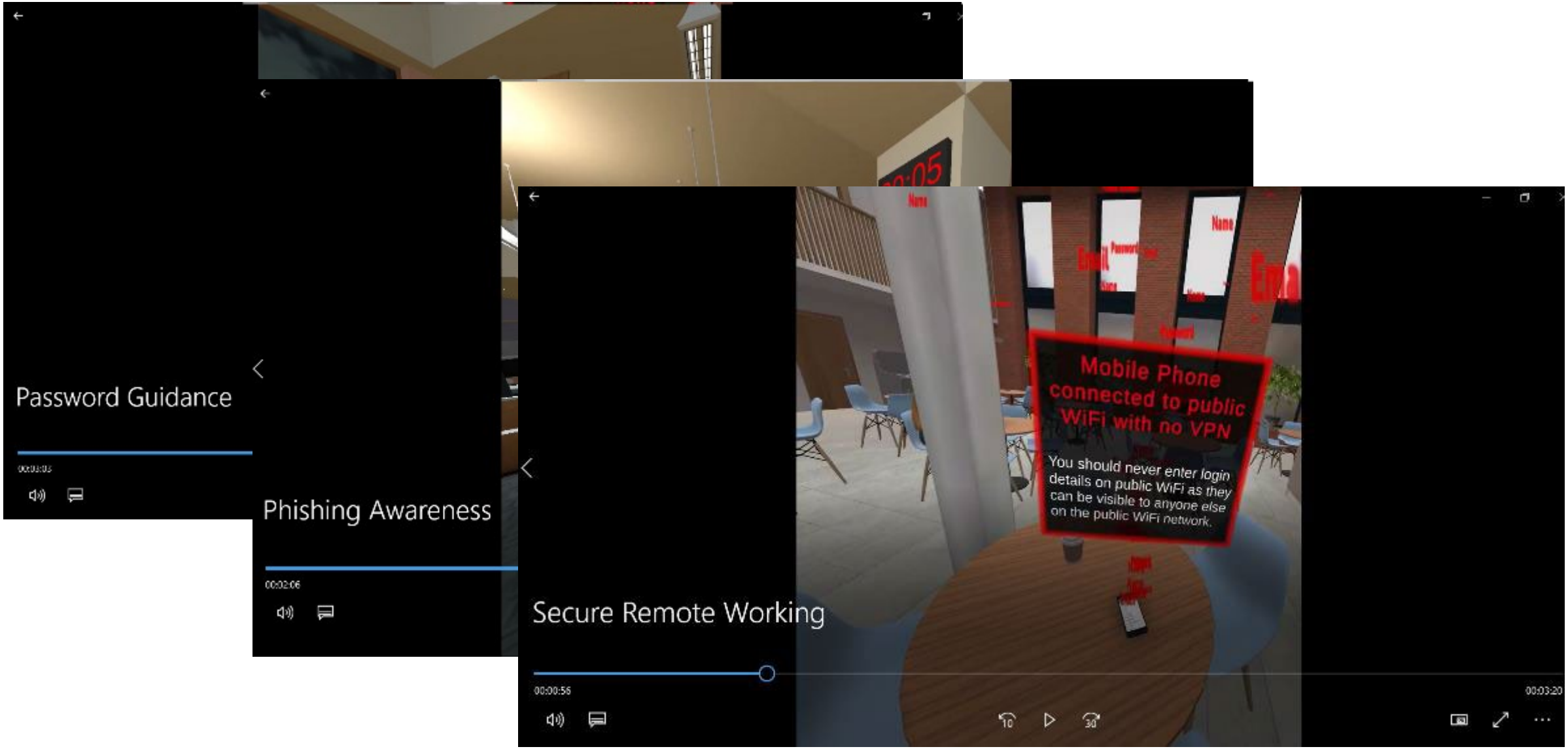
Stage 1 – Design – Storyboard Development

Moodboard

Student room, library and cafe



Stage 2 – Prototype experiences



Stage 3 - VR Focus Groups

QUEEN'S UNIVERSITY BELFAST

Satisfaction of requirements:

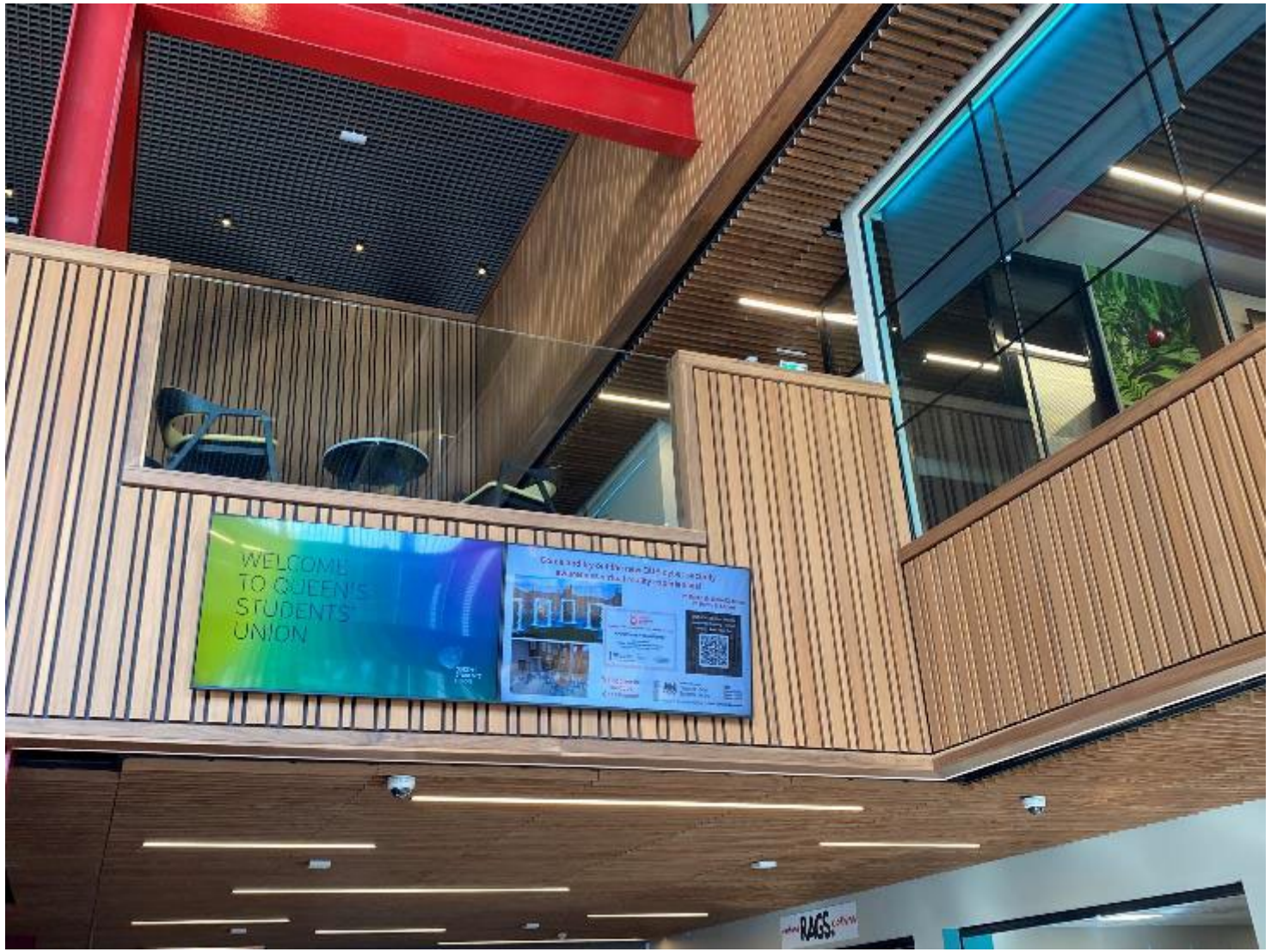
Req. No.	Requirement Description	Phase 2 design element
FPS1	Case studies or characters that bring the scenario to life.	✓ Use of QUB locations – library, café, student room. ✓ Use of QUB branding within these scenarios e.g., posters, merchandise etc. ✓ Use of student characters in relevant scenarios e.g., *Social Engineering*, *Social Media Use* etc.
FPS2	The capability for the student to self-check their knowledge/understanding. For example, the inclusion of quizzes with explanations provided for incorrect answers to enhance learning.	✓ Inclusion of topic-related question pre- and post-experience. ✓ Gamified experiences to practice and then test knowledge/understanding e.g., *Password Guidance*, *Phishing Awareness*. ✓ Inclusion of feedback at the end of each gamified experience.
FPS3	The opportunity for the student to apply the knowledge. For example, by using 2D and 3D technology to recreate conditions, which mirror real world situations that the student is likely to encounter in their daily lives. In particular, immersive technology could be used to provide an opportunity for the student to apply knowledge in distracting and/or stressful conditions.	✓ Gamified experiences to practice and then test knowledge/understanding e.g., *Password Guidance*, *Phishing Awareness*. ✓ Use of QUB locations – library, café, student room. ✓ Use of student characters in relevant scenarios e.g., *Social Engineering*, *Social Media Use etc.* ✓ Timed experiences to create an element of pressure.

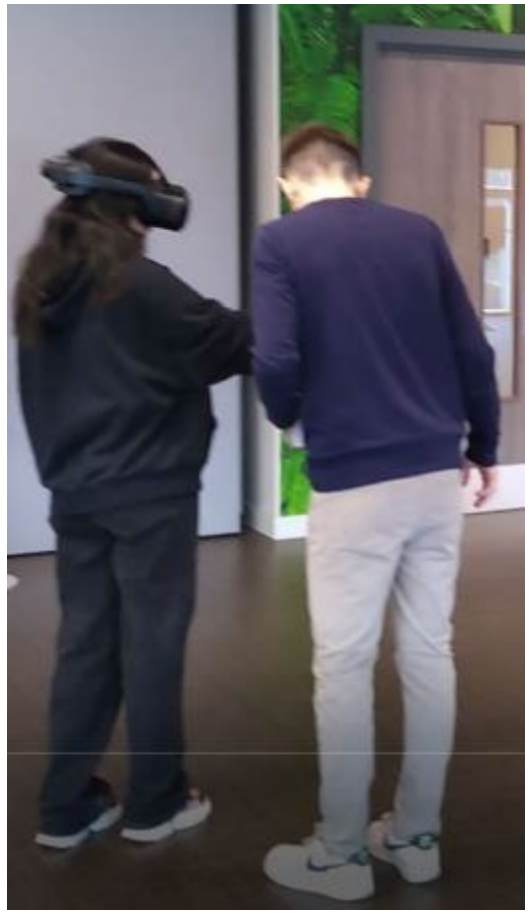
QUEEN'S UNIVERSITY BELFAST

Satisfaction of requirements:

C1	Content which is directly relevant and relatable to student life. For example, the importance of backing up student work.	✓ Use of student characters in relevant scenarios e.g., *Social Engineering, Social Media Use etc.* ✓ Inclusion of devices/services used by students throughout Canvas/Microsoft
C2	Coverage of the "Digital Footprint".	✓ Specific experienc *Footprint*) focused
C3	Coverage of best cyber security practice with social media.	✓ Specific experienc focused on this to
C4	Coverage of cyber security at home/in student accommodation.	✓ Inclusion of a student room scenario. ✓ Experiences linked to cyber security in the student accommodation e.g., *Social Engineering, Protecting your Data and Devices.*
C5	Specific information for international students who may be especially vulnerable to cyber security attack due to their lack of familiarity with existing practices in the UK and/or use of multiple devices across different networks and regions.	✓ Specific experience (*Social Engineering*) focused on this topic. ✗ Use of multiple devices across different networks/regions is not covered. However, services used by international students e.g., WeChat included.
C6	Practical guidance as to how to respond to a cyber security incident or how to apply cyber security best practices. For example, how to minimise exposure to cyber security attacks, what tools to use (e.g., password manager), what technical actions to take, and what to do if subjected to an attack.	✓ Specific experience (*Incident Reporting*) focused on this topic. ✓ Feedback, recommended tools and best practices included in all experiences.
C7	Training and guidance about use of tools such as Microsoft Teams, Zoom, TeamViewer etc.	✓ Information sheet shared on completion of training to cover links to guidance on use of common QUB tools.

Full experience - Training





QUEEN'S UNIVERSITY BELFAST

Some student comments:

"Impressive!"

"I'm going to change my password now!"

"Excellent!"

"Very interactive"

"Really engaging, rather than Canvas training"

"It gamifies the experience of learning increasing the learning rate of the topic."

"Have learned more and is more engaging than watching a video or reading text."

"Pay attention a lot more."

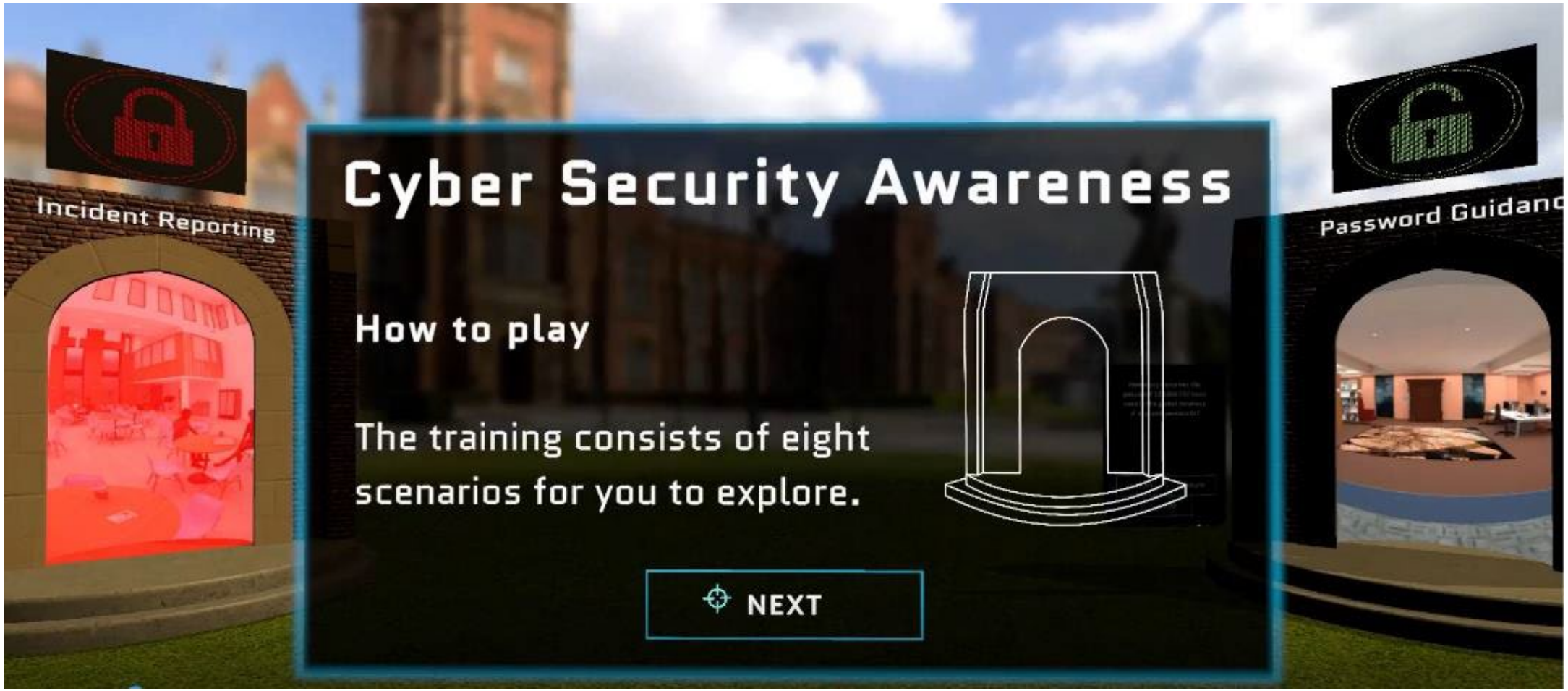
"Cybersecurity is often taught to be boring. This experience shows that it need not be. I have not come across any other platform trying to teach cybersecurity through VR … brings an element of excitement to an otherwise boring topic. Young people and students will have fun with this simply because of the way it is designed. They learn by doing rather than simply being told to do something."

QUEEN'S UNIVERSITY BELFAST

ACE-CSE Student Cyber Security Awareness Training

This training is designed to develop your understanding and awareness of cyber security.

ACE-CSE Student Cyber Security Awareness Training



QUEEN'S UNIVERSITY BELFAST

ACE-CSE Student Cyber Security Awareness Training

QUEEN'S UNIVERSITY BELFAST

Trial - Certificate of Completion

QUEEN'S UNIVERSITY BELFAST

EXCITE Phase 3 - Objective

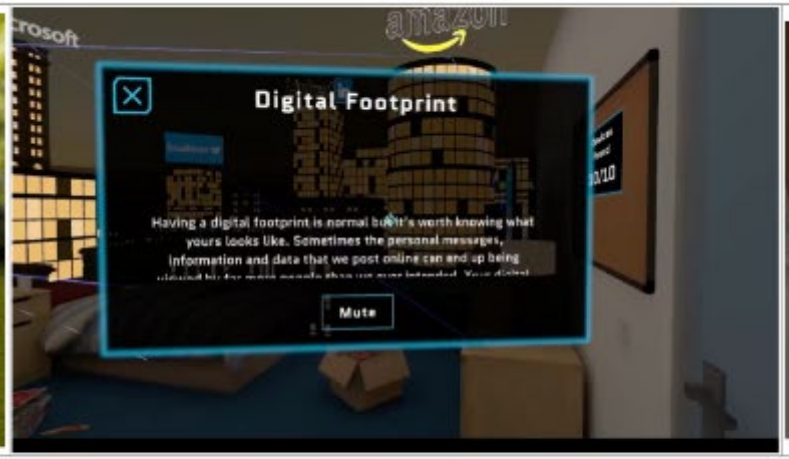
Phase 3 focused on further development of the cyber security immersive experiences to **increase accessibility** and hence completion of the training and to make the application suitable for **deployment in other settings** (principally other ACE-CSE universities).

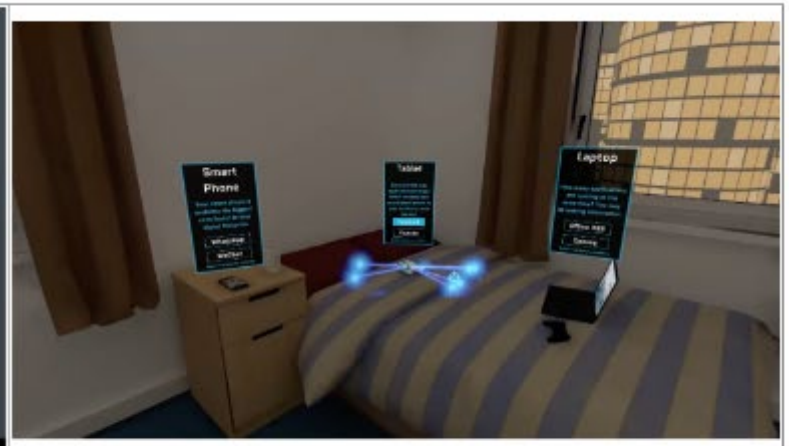
- A web-browser version of EXCITE.
- A generic (non-branded) version of the application (web-browser).
- A demo VR version with two experiences.

QUEEN'S UNIVERSITY BELFAST

ACE-CSE Student Cyber Security Awareness Training

We invite you to complete the immersive cyber security training. Here is an idea of what to expect in the immersive training:





Click here to launch the immersive training in your web browser.

1. Log in as a new user (take a note of your user ID for later use).
2. Select your School from the drop-down menu.
3. Follow the instructions to complete the training.

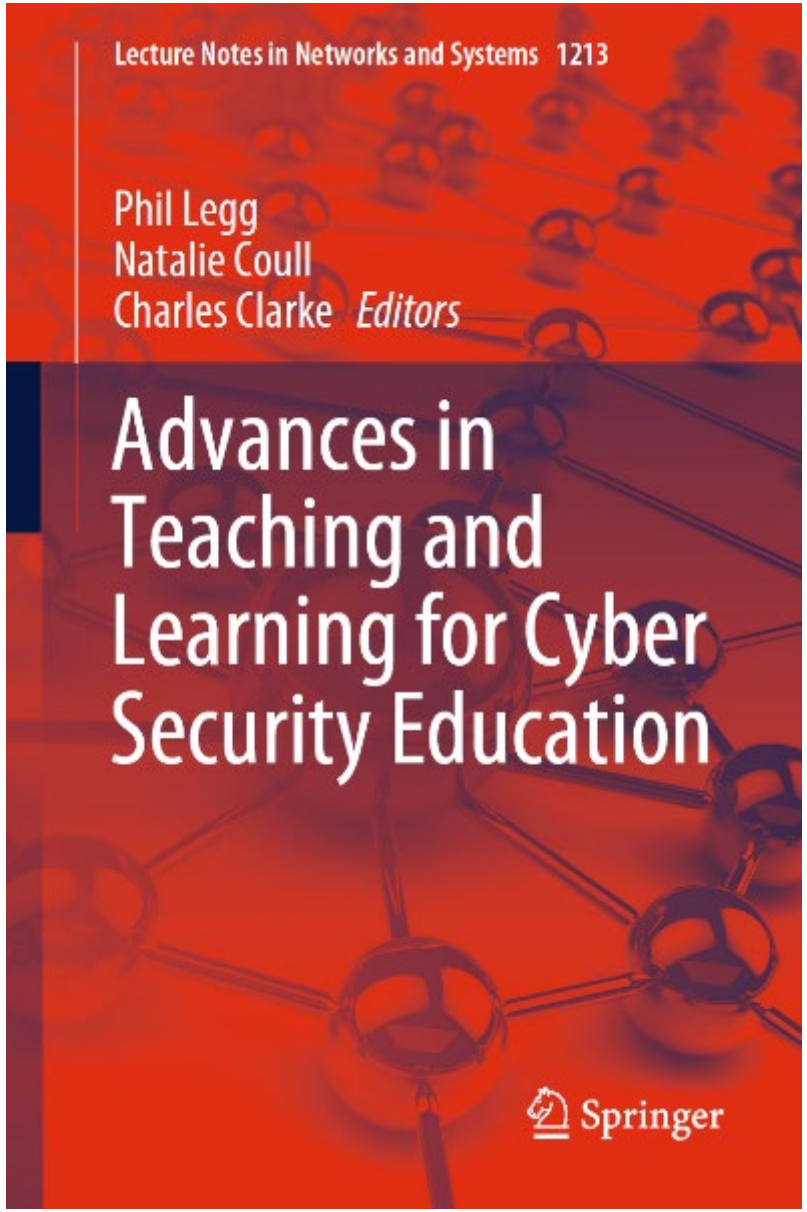
Gold Award

in association with National Cyber Security Centre

Department for Science, Innovation & Technology

Academic Centre of Excellence in **Cyber Security Education**

QUEEN'S UNIVERSITY BELFAST



EXCITE: EXploring the enhancement of Cyber security training through Immersive TEchnology

Sandra Scott-Hayward(✉), Michelle Butler, and Carole Parsons

Queen's University Belfast, Belfast, UK
s.scott-hayward@qub.ac.uk, michelle.butler@qub.ac.uk, c.parsons@qub.ac.uk

Abstract. The goal of the EXCITE (EXploring the enhancement of Cyber security training through Immersive TEchnology) project was to explore the potential to increase the efficacy of cyber security training for third-level students through the use of immersive experiences supported by virtual reality design. In the first phase of the EXCITE project, we explored the cyber security experience of a diverse, multi-disciplinary group of third-level students, their views on the suitability and effectiveness of cyber security training materials, and their perspectives on the potential use of immersive technologies in cyber security training. Based on our findings in Phase 1, Phase 2 focused on the design and development of a suite of cyber security immersive experiences presented in virtual three-dimensional student-oriented scenarios e.g., student residence, university computer lab, café. The experiences cover the topics of *Password Guidance*, *Phishing Awareness*, *Social Engineering*, *Your Digital Footprint*, *Social Media Use*, *Secure Remote Working*, *Protecting Your Data and Devices*, and *Incident Reporting*. In this chapter, the design of each phase of EXCITE is presented, along with its findings, feedback from students, and recommendations based on the experience of rolling out the cyber security awareness experiences in a university.

1 Introduction

Universities are key contributors to the economy, skills development, and innovation in the UK. In making this contribution, they handle personal and research data, intellectual property, and other assets, each of which has significant value to others. Further, those individuals that come to university learn the foundational skills, across all disciplines, upon which they build their careers; this represents a significant opportunity to bring cyber security knowledge to a broad spectrum of industries and roles to strengthen digital security for years to come. In the EXCITE project, the potential to increase the efficacy of cyber security training for students through the use of immersive experiences supported by augmented and virtual reality (AR/VR) design were explored.

There were two main motivations driving EXCITE. Firstly, a gap in the provision of cyber security awareness training that is broadly accessible to all

P. Legg et al. (Eds.): CSE 2024, LNNS 1213, pp. 96–115, 2024.
https://doi.org/10.1007/978-3-031-77524-6_6

QUEEN'S UNIVERSITY BELFAST

Thank you

s.scott-hayward@qub.ac.uk

www.csit.qub.ac.uk

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Q&A

Are There Any Questions?

Supercharging the Cybersecurity Industry Through Disability Inclusion

Dr. Kirk Adams
Managing Director
Innovative Impact, LLC

Supercharging the Cybersecurity Industry Through Disability Inclusion

Dr. Kirk Adams, Managing Director, Innovative Impact LLC

About the Speaker

- Dr. Kirk Adams
- Former CEO, American Foundation for the Blind
- Managing Director, Innovative Impact LLC
- Advocate for disability inclusion and employment
- Expert in cross-sector collaboration

The Challenge

- Critical shortage in cybersecurity professionals
- 700,000+ unfilled positions in US
- 70% unemployment rate among blind adults
- Untapped talent pool with unique capabilities

The APEX Program Solution

- Partnership between Innovative Impact and Novacoast
- Virtual training program for blind individuals
- CompTIA Network+ and Security+ certifications
- Job placement through Novacoast's staffing division
- www.theapexprogram.com

Multi-Sector Alignment

- Government: Vocational Rehabilitation funding
- Corporate: Novacoast and industry partners
- Nonprofit: Vision-specific organizations
- Community: Blind individuals and families
- Reference: 'Forces for Good' framework

Disability as Strength

- Resilience and adaptability
- Creative problem-solving
- Attention to detail
- Advanced communication skills
- Reference: 'The Talent Code' principles

Success Through Partnership

- VisionServe Alliance network
- National Federation of the Blind
- American Council of the Blind
- Local chapters and leaders nationwide

Corporate Leadership Examples

- Microsoft's inclusive hiring initiatives
- Walgreens' distribution center model
- ROI of disability inclusion

The Vocational Rehabilitation Model

- Federal/state funding structure
- Training and certification coverage
- Support services
- Employment outcomes

Nonprofit Network

- VisionServe Alliance
- 150+ member organizations
- Employment services
- Local expertise and support

Call to Action

- Visit www.theapexprogram.com
- Training programs: Partner with APEX
- Employers: Access trained talent
- VR professionals: Fund participants
- Blind individuals: Start your cybersecurity career

Contact Information

- Dr. Kirk Adams
- Innovative Impact LLC
- Website: www.theapexprogram.com
- Email: kadams@novacoast.com
- kirkadams@drkirkadams.com

Q&A

Are There Any Questions?

Privacy Evolved: How to Teach, Train, and Thrive Amid Regulation Change

Sanford Weinberg

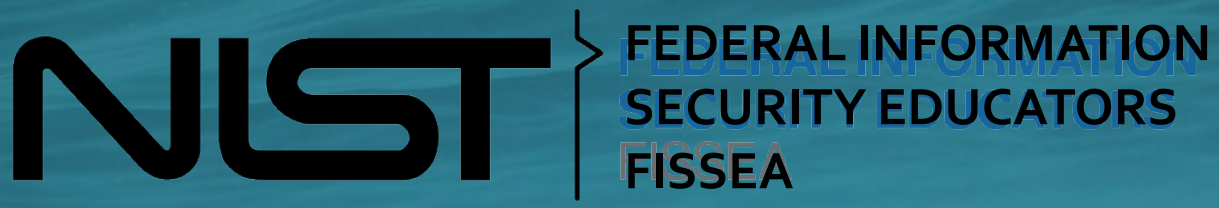
CyberSecurity Speaker, Professor, and Consultant

SpeakcyberSecurity.com

Privacy and Cybersecurity Evolved:

How to teach, simplify, and thrive amid constant regulation changes

FISSEA Winter Forum: February 11, 2025



Sanford Weinberg - SpeakCyberSecurity.com
sanford@speakcybersecurity.com
linkedin.com/in/sweinberg

691

Legislation Numbers 2020 - 2024

Federal Privacy / Cybersecurity Proposed	215
State Privacy / Cybersecurity Proposed	290
Federal AI Bills Proposed	112
State AI Bills Proposed	74

How do we effectively teach this?

First – Get to know the end-user's pain

Second -- Give them strategies along with knowledge and tools to lessen their pain.

Seek first to understand, then to be understood – Steven Covey

How do you eat an elephant?

How do we make it less overwhelming and less stressful? What do they need?

1. Make it easier to analyze of the laws
2. Simplify what needs to be implemented
3. Reduce the amount of work to implement

Questions:

What might it take to implement those requirements?

Who would be involved with implementing those changes (job titles or departments

What might the timeframe needed to implement some of those new requirements?

If you are involved with implementing those requirements, How might you feel about trying to keep up with those numbers of new laws and what is needed?

Data Regulatory - Dirty Dozen

Consumer Data Rights, Tracking & Protections	Biometric Data & Facial Recognition Regulations	Data Breach Notification Requirements	Children's Online Privacy & Safety
Cross-Border Data Transfers	Health Information Privacy (PHI Protection)	Sensitive Personal Data Protection	Algorithmic Transparency & Data Usage Disclosure
Right to Be Forgotten & Data Deletion Rights	Privacy Rights for Employees & Workplace Monitoring	Smart Device & IoT Data Privacy	Data Retention & Expiration Policies

Further Simplification: Breakdown of types

1. Identity and Permissions
2. Sensitive Personal Information (PII, PHI, Financial)
3. Data leakage (Reporting, Containment, Restoration, Repair)
4. Individual data rights (access to their data, correction of their data, removal of data (and non-removal rights)
5. Tracking and selling of user activity and information

Most Restrictive Legislation by Category

Topic	Most Restrictive State Law (USA)	Most Restrictive Federal Law (USA)	Most Restrictive International Law
Consumer Data Rights & Protections	California Privacy Rights Act (CPRA) (2023)	American Privacy Rights Act (Proposed 2024)	General Data Protection Regulation (GDPR) - EU
Biometric Data & Facial Recognition Regulations	Illinois Biometric Information Privacy Act (BIPA) (2008, Amended 2023)	No comprehensive federal law	GDPR (EU) & Canada's PIPEDA
Data Breach Notification Requirements	California's Data Breach Notification Law (SB-24, 2022)	No unified federal law, FTC guidelines & CIRCIA (2022) apply	GDPR (EU) – 72-hour breach notification rule
Children's Online Privacy & Safety	California Age-Appropriate Design Code Act (2022)	Children's Online Privacy Protection Act (COPPA) - 1998	UK's Age-Appropriate Design Code (2020), EU's GDPR (Children's Rights)
Cross-Border Data Transfers	California CPRA (2023) with restrictions	No comprehensive law, FTC enforcement applies	GDPR's Data Transfer Mechanisms (EU), China's PIPL
Health Information Privacy (PHI Protection)	California Confidentiality of Medical Information Act (CMIA) (Expanded 2021)	Health Insurance Portability and Accountability Act (HIPAA) - 1996	GDPR (EU) & Australia's Privacy Act (1988, updated 2022)
Sensitive Personal Data Protection	New York SHIELD Act (2019)	No specific federal law	GDPR (EU), Brazil's LGPD
Algorithmic Transparency & Data Usage Disclosure	Colorado Privacy Act (CPA) - 2023	Proposed under the American Data Privacy and Protection Act (ADPPA) - 2022	EU AI Act (Finalizing 2024)
Right to Be Forgotten & Data Deletion Rights	California CPRA (2023)	No comprehensive federal law	GDPR (EU), Brazil's LGPD
Privacy Rights for Employees & Workplace Monitoring	New York AI Employment Law (2023)	No federal law	GDPR (EU) Employment Provisions

Use AI to help you slay the dragon

(Just make sure to verify)

1. Regulatory Summaries
2. Pending Legislation Tracking
3. Compliance Comparisons
4. Automated Compliance Gap Identification
5. Checking for specifics like Breach Notification Requirements
6. Privacy Impact Assessments
7. Automated Contract Review
8. Data Localization Requirements
9. Regulatory changes or updates (like CCPA and others)
10. State Level vs. Federal-Level Differences
11. Overlap between Industry Frameworks and Legal Mandates
12. Privacy-by-Design and Security-By Design Guidance

(As always, consult real legal counsel)

Questions or Comments

Privacy and Cybersecurity Evolved:

How to teach, simplify, and thrive amid constant regulation changes

Sanford Weinberg - SpeakCyberSecurity.com
sanford@speakcybersecurity.com
linkedin.com/in/sweinberg

Q&A

Are There Any Questions?

Federal Information Security Educators (FISSEA) Winter Forum

BREAK

The Forum will resume at 2:55pm ET

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Welcome Back!

Frauke Steinmeier
FISSEA Co-Chair

Board-Level Reporting

Ryan Leirvik
CEO
NEUVIK

Board-Level Reporting

Ryan Leirvik, CEO

NEUVIK

February 11, 2025

Discussion Document for

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

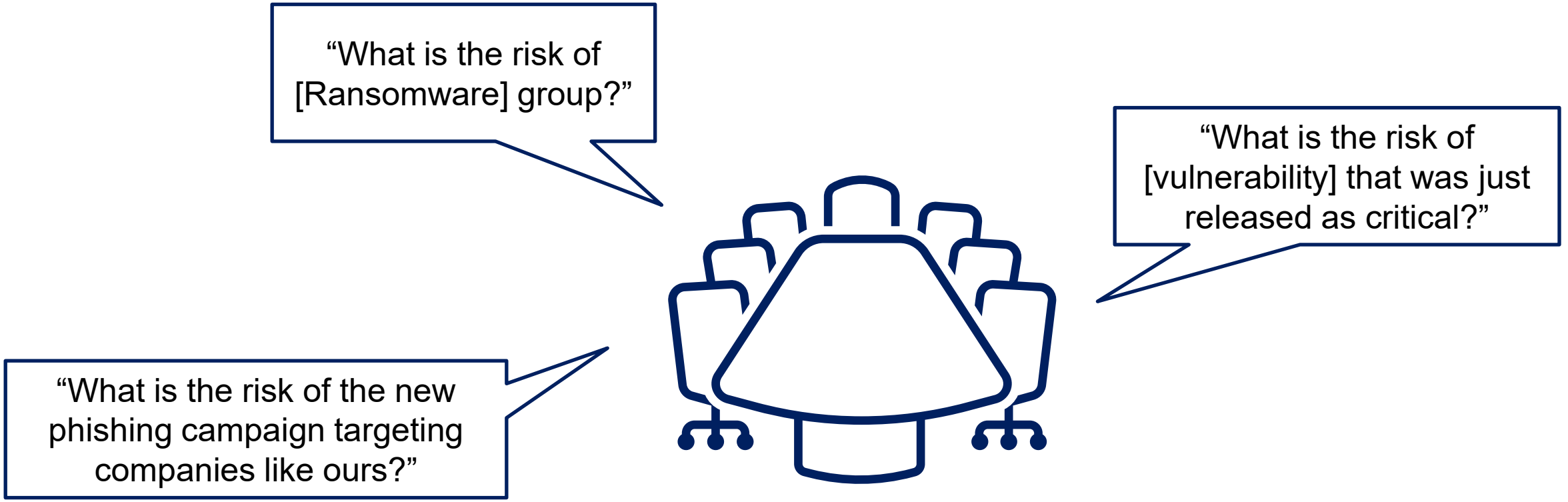
Why is gaining buy-in for cyber awareness and training difficult?

1. **Executives do not always have the context** to know what questions to ask regarding cyber program / training effectiveness

2. **Communicating** the strength / weakness of cyber risk awareness programs **becomes challenging due to various degrees of understanding**

3. One approach that has worked is a **simplified message, leveraging core components of current NIST guidance** in an executive-consumable narrative

1 Risk is not always well defined, leading to confusion

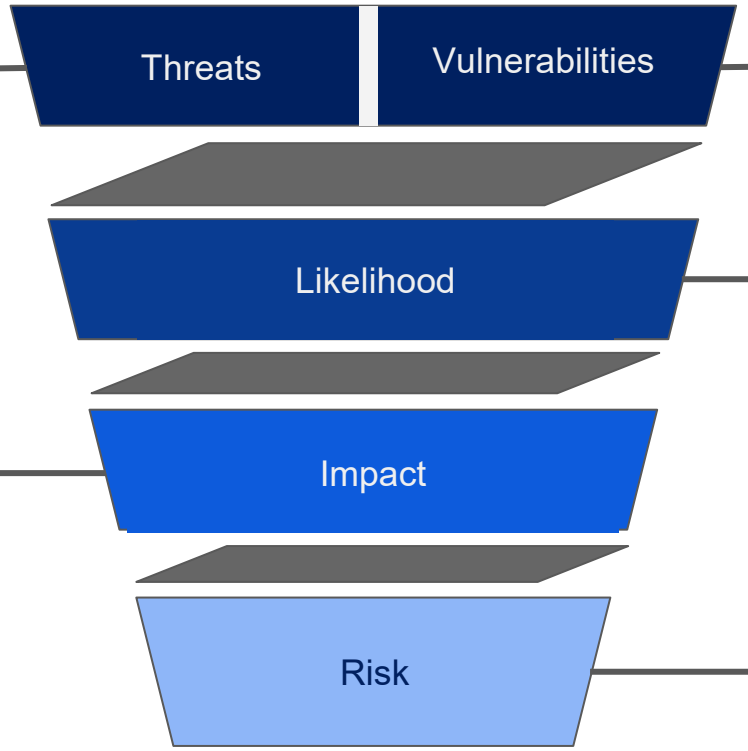


Threats, vulnerabilities, and/or likelihood ≠ Risk

1 Approach: Use NISTIR 7621r1 to categorically separate "risk" components and use language executives already know

"Risk is a function of threats, vulnerabilities, the likelihood of an event, and the potential impact such an event would have to the organization"*

Malicious **actors** (e.g., hackers, hacktivists, criminals, nation-state actors)



A **flaw/weaknesses** that may be used to harm the enterprise (e.g., unsecured WiFi network, unprotected physical access, unpatched software)

The **chance** that a threat will affect the enterprise and helps determine what types of protections to put in place"

An event that could create **potential harm** to the enterprise depending on the information affected (e.g., PHI data, PII data, FTI, intellectual property) and the cost to the organization (e.g., fines, fees)

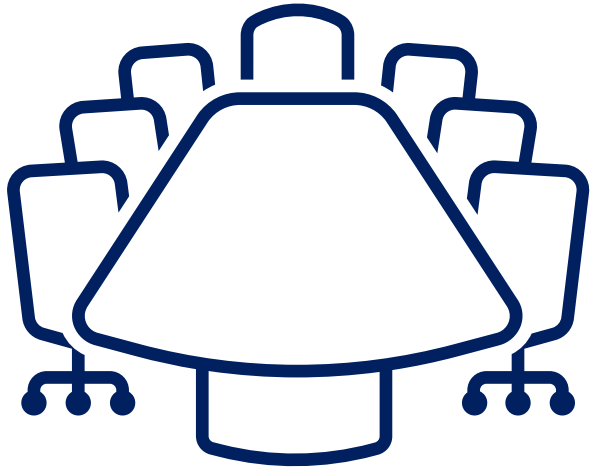
"A **function** of threats, vulnerabilities, the likelihood of an event, and the potential impact such an event would have to the [enterprise]"*

*From NISTIR 7621 Revision 1 Small Business Information Security: The Fundamentals

2 Impact is not always well defined, leading to disconnect between impact categories and cost

"What is the impact to the organization?"

"How does this relate to us?"



"Could you explain impact categories again?"

"How much will this cost?"

Impact (e.g., damage to information systems, regulatory fines) ≠ actual cost

2 Approach: Use language executives understand – dollars and cents

Impacts* may include:


Damage to information or information systems


Regulatory fines and penalties / legal fees


Decreased productivity


Loss of information critical in running your business


An adverse reputation or loss of trust from customers


Damage to your credit and inability to get loans from banks


Loss of business income

*Categories published in the NISTIR 7621 Revision 1 Small Business Information Security: The Fundamentals

3 One way of increasing success in executive-level cyber communications

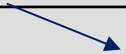
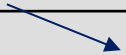
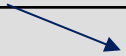
With an understanding of impact components, **qualitative risk metrics become simpler to craft, more compelling, and Board-ready** for a risk narrative

3 Align to CSF: Offer specific measures that meet the intent of each Function

FUNCTION*	DESCRIPTION	PROPOSED ACTIVITIES	Sample MEASURES
GOVERN	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	• Implement **on-time strategic program management** • Increase efficiency of cybersecurity team • Increase hiring to fill gaps in headcount resourcing	• % of strategic cybersecurity initiatives on time • # of cybersecurity employees • Cybersecurity FTE count as % of IT FTEs • % budget utilization against key milestones, e.g., projected Q1 spend
IDENTIFY	The organization's current cybersecurity risks are understood.	• Update Asset Management program • Conduct in-depth Risk Assessments • **Remove and replace legacy assets**	• % of assets reviewed for criticality • % of employees passing annual Cybersecurity Awareness training • # of out-of-date systems operating • % of supply chain / 3rd parties with up-to-date compliance / attestation
PROTECT	Safeguards to manage the organization's cybersecurity risks are used.	• Access Control • **Awareness and Training** • Data Security • Maintenance of critical assets	• % of privileged accounts under privileged access control • % of applications monitored for appropriate data quality use • Mean Time to Patch (MTTP) – defined as date from when vulnerability comes out vs. patching occurs
DETECT	Possible cybersecurity attacks and compromises are found and analyzed.	• Continuous Monitoring • Detection Processes • **Faster response to anomalies and events**	• Mean Time to Detect (MTTD)
RESPOND	Actions regarding a detected cybersecurity incident are taken.	• Improve response planning • **Quicken mitigation strategies**	• Mean Time to Respond • # of unremediated critical vulnerabilities after 30 days
RECOVER	Assets and operations affected by a cybersecurity incident are restored.	• **Perform active recovery planning (internal, 3rd parties)** • Improve communications during recovery	• # response plans tested in [X time horizon, e.g., annual] • # SLAs out of compliance due to incidents

Methodology informed by Understand, Manage, and Measure Cyber Risk®

3 Set up for trending and long-term reporting

FUNCTION*	DESCRIPTION	SAMPLE MEASURES	CURRENT	GOAL	TREND
GOVERN	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	• % of strategic cybersecurity initiatives on time • # of cybersecurity employees • Cybersecurity FTE count as % of IT FTEs • % budget utilization against key milestones, e.g., projected Q1 spend	• …% • …#	• …% • …#	
IDENTIFY	The organization's current cybersecurity risks are understood.	• % of assets reviewed for criticality • % of employees passing annual Cybersecurity Awareness training • # of out-of-date systems operating • % of supply chain / 3rd parties with up-to-date compliance / attestation	• …% • …%	• …% • …%	
PROTECT	Safeguards to manage the organization's cybersecurity risks are used.	• % of privileged accounts under privileged access control • % of applications monitored for appropriate data quality use • Mean Time to Patch (MTTP) – defined as date from when vulnerability comes out vs. patching occurs	• …% • …%	• …% • …%	
DETECT	Possible cybersecurity attacks and compromises are found and analyzed.	• Mean Time to Detect (MTTD)	• XYZ	• XYZ	
RESPOND	Actions regarding a detected cybersecurity incident are taken.	• Mean Time to Respond • # of unremediated critical vulnerabilities after 30 days	• XYZ • …#	• XYZ • …#	
RECOVER	Assets and operations affected by a cybersecurity incident are restored.	• # response plans tested in [X time horizon, e.g., annual] • # SLAs out of compliance due to incidents	• …# • …#	• …# • …#	

Methodology informed by Understand, Manage, and M

Q&A

Are There Any Questions?

Next-Gen Cybersecurity Education: Using Generative AI to Rapidly Produce Cybersecurity Learning

Jim Wiggins

Chief Executive Officer

FITSI - Federal IT Security Institute

Next-Gen Cybersecurity Education Using Generative AI to Rapidly Produce Cybersecurity Learning

Jim Wiggins
Chief Executive Officer
Federal IT Security Institute

FISSEA Winter Forum
Date: 02/10/25

Version: Arial, 10

FITSI
FEDERAL IT SECURITY INSTITUTE
HELPING SECURE THE NATION'S FEDERAL INFORMATION SYSTEMS

Agenda

- Introduction
- Challenges with Content Creation
- Overview of Generative AI
- Role of Prompting
- Use Cases in Cyber Content Creation
- Use Case #1 – Creating Learning Objectives
- Use Case #2 – Creating Slides
- Use Case #3 – Creating Lab Activities
- Use Case #4 – Creating Case Studies
- Use Case #5 – Creating Quizzes and Assessments
- Leading Practice #1 – Incorporate Educational Frameworks
- Leading Practice #2 – Uploading Sources Materials
- Leading Practice #3 – Use Web Search for Current Information
- Leading Practice #4 – Use “Chain of Thought” in Prompting
- Leading Practice #5 – Separate Modules into different Chats
- Leading Practice #6 – Use SMEs to Review all Content
- Leading Practice #7 - Use the Appropriate AI Subscription Model to Protect Your Content
- Samples
- Q&A
- Resources
- Contact Information

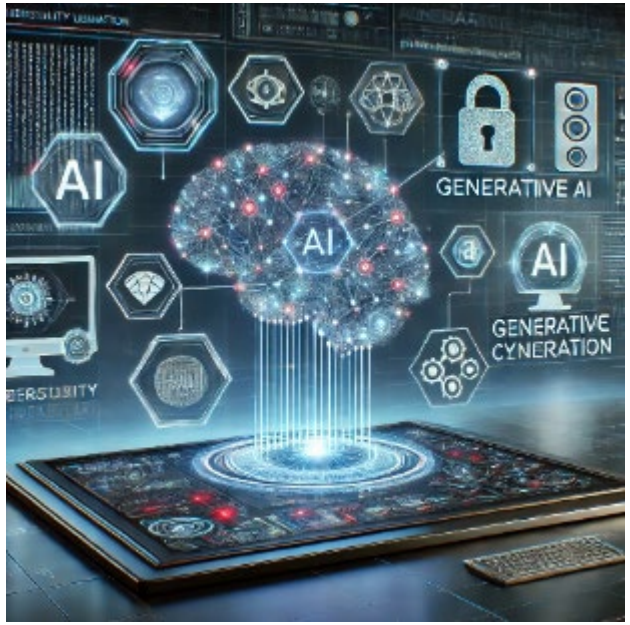
Introduction

- Jim Wiggins
  - Chief Executive Officer of the Federal IT Security Institute
  - Cybersecurity Trainer and Information Security Practitioner
  - 28 of experience in IT
  - 23 of experience in IT security
  - 1.75 years of experience in Generative AI
    - Trained Over 1000 Students in Generative AI
      - 500+ National Risk Management Center
      - 400+ Defense Information Systems Agency
      - 90+ Department of Interior
      - 90+ ISACA-GWDC Chapter
  - Working on a Master's in Assessment Testing and Measurement at GWU

Challenges with Content Creation

- Manual methods remain time-consuming
- Rapid threats challenge content
- Expert input burdens production

Overview of Generative AI



- AI automates content production
- Advanced models drive generation
- Tailored outputs meet demands

Role of Prompting

- Precise prompts guide output
- Structured input refines content
- Prompts ensure relevance

Use Cases in Cyber Content Creation

- Diverse materials via AI
- Automates objectives, slides, labs
- Supports updated engaging content

Use Case #1 – Creating Learning Objectives

- Clear, measurable objectives generated
- Aligned objectives boost clarity
- Accelerates framework development

Use Case #1 – Creating Learning Objectives

- Demo

Use Case #2 – Creating Slides

- Automated slide deck generation
- Consistent visual presentation formats
- Dynamic updates mirror trends

Use Case #2 – Creating Slides

- Demo

Use Case #3 – Creating Lab Activities

- Realistic lab scenarios simulated
- Interactive exercises enhance practice
- Hands-on labs reinforce theory

Use Case #3 – Creating Lab Activities

- Demo

Use Case #4 – Creating Case Studies

- Detailed incident narratives generated
- Structured analysis of incidents
- Bridges theory with practice

Use Case #4 – Creating Case Studies

- Demo

Use Case #5 – Creating Quizzes and Assessments

- Dynamic quiz generation automated
- Assessment items updated continuously
- Standardized evaluation of learning

Use Case #5 – Creating Quizzes and Assessments

- Demo

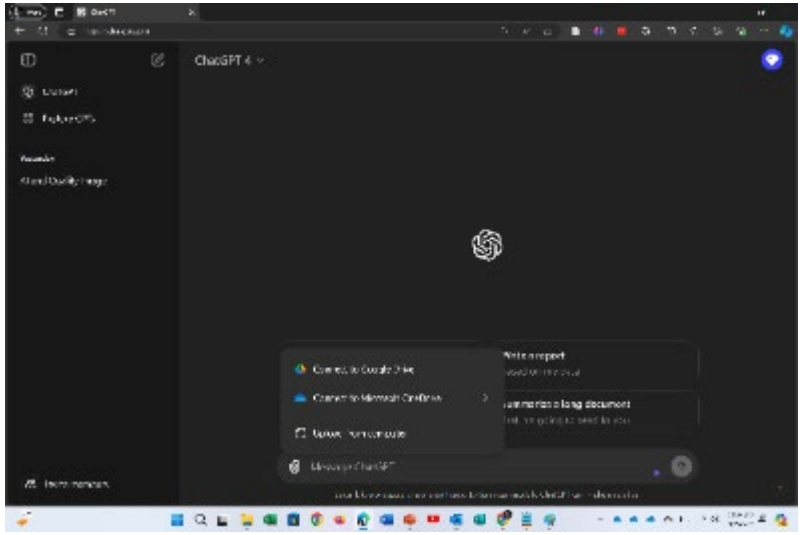
Leading Practice #1 – Incorporate Educational Frameworks

- Gen AI knows about educational frameworks
  - Bloom’s Taxonomy
  - ADDIE
  - Webb's Depth of Knowledge
  - Mager’s Performance Objectives

Leading Practice #2 – Uploading Source Materials

- Upload verified source materials
- Establishes robust data foundation
- Ensures content accuracy traceability

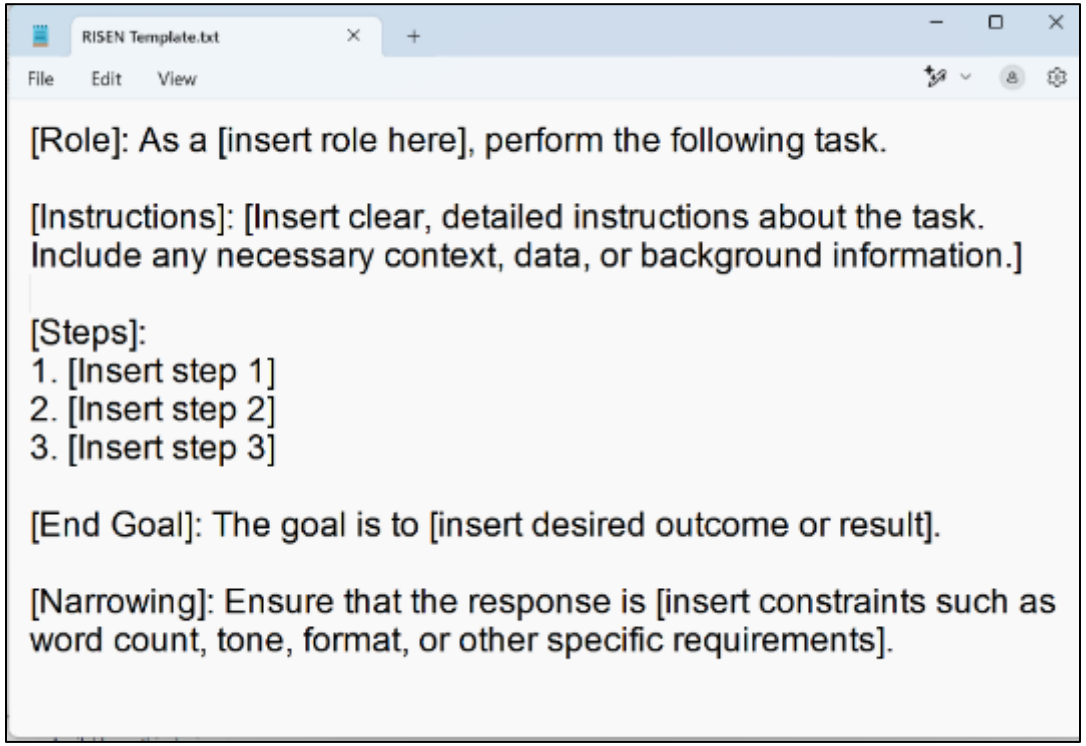
Leading Practice #3 - Use Web Search for Current Information



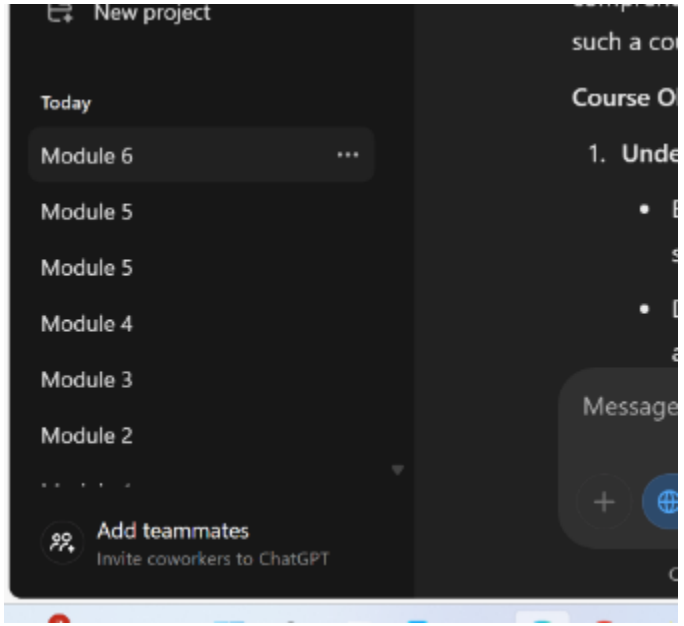
- Use web search for updates
- Verify sources for accuracy
- Integrate real-time threat data

Leading Practice #4 – Use "Chain of Thought" in Prompting

- RISEN Example



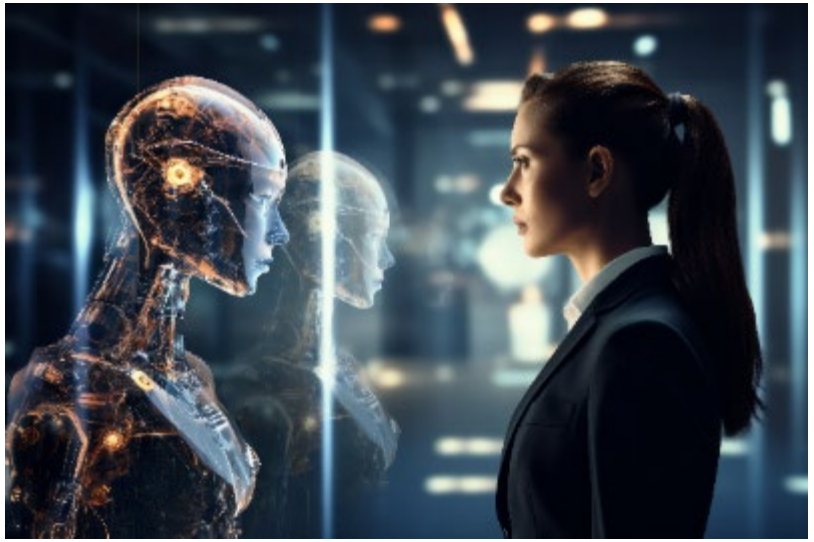
Leading Practice #5 – Separate Modules into Different Chats



- Segment content into modules
- Distinct topics for clarity
- Optimizes focused AI interactions

Leading Practice #6 – Use SMEs to Review All Content

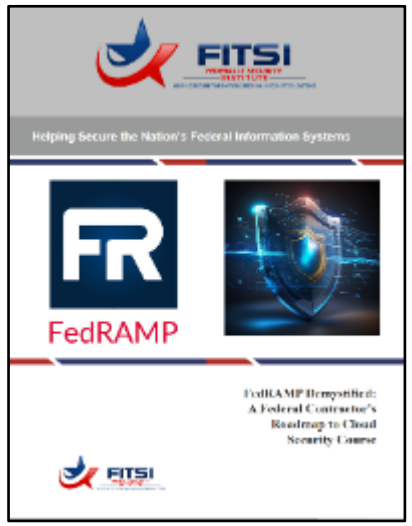
- SMEs review generated content
- Ensures technical accuracy rigor
- Integrates expert feedback continuously



Leading Practice #7 – Use Appropriate AI Subscription Model

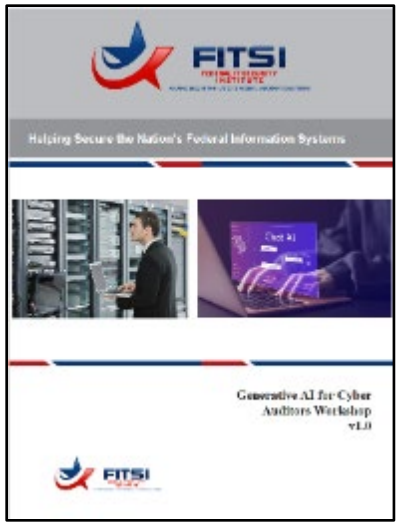
- Select secure AI subscription
- Protect proprietary content integrity
- Implement controlled access measures

Samples



- FedRAMP

- NIST CSF 2.0



- Gen AI for Cyber Auditors

Q&A

Resources

- Use the QR Code

Contact Information

- Jim Wiggins
  - Email: jim.wiggins@fitsi.org
  - Phone: 703-828-1196 x701
  - Cell: 571-277-4661

Q&A

Are There Any Questions?

Closing Remarks

Marian Merritt
Deputy Director NICE
National Institute of Standards and Technology

Frauke Steinmeier
FISSEA Co-Chair

Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates+subscribe@list.nist.gov

Volunteer for the Planning Committee
https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee

Serve on the Contest or Award Committees
Email fissea@nist.gov

Submit a presentation proposal for a future FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations

SAVE THE DATE

Federal Information Security Educators (FISSEA) Spring Forum

May 13, 2025

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

THANK YOU

We look forward to receiving your feedback via the post-event survey!

https://www.surveymonkey.com/r/fisseawinterforum2025

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA