BUILDING A CULTURE OF SOCIAL ENGINEERING AWARENESS IN HIGHER EDUCATION

HALF-DAY WORKING SESSION

FOR CISO/IT/RISK LEADERSHIP

WHY THIS MATTERS NOW - THE CURRENT LANDSCAPE

Recent **phishing attacks** on top universities have **exposed millions of records**.

High-Profile University Breaches

Harvard, Princeton, and UPenn suffered major phishing attacks in late 2025, compromising donor, alumni, and student information including contact details and donation history.

Sophisticated Phishing Methods

Attackers used **phone-based phishing, employee impersonation, and targeted email campaigns** to gain unauthorized access to advancement and CRM systems.

Sector-Wide Risks and Impact

Education institutions hold high-value data but do not have corporate-grade security, leading to **increased risk of identity theft, financial losses, lawsuits, and reputational damage**.

Education and research are among the most-targeted industries globally; phishing and ransomware are frequently intertwined as initial access vectors.

UNIVERSITIES ARE OPEN ECOSYSTEMS WITH DISTRIBUTED ACCESS TO PROMOTE LEARNING AND KNOWLEDGE-SHARING.

The Reality

Regulatory Complexity — FERPA, GLBA, state privacy laws
Limited Security Capacity — Teams stretched across research, teaching, operations
Distributed Access Model — Scale makes managing access complex

What Attackers Exploit

People
Missing role-based training for high-risk staff
Process
Unclear or outdated incident reporting paths or playbooks
Technology
Email controls misconfigured; logging gaps; inconsistent MFA

WHAT ATTACKERS ARE REALLY AFTER

	Advancement CRM Platforms	Donor Databases	Alumni Records	Student Information Systems
The Prize	Complete donor relationship history, giving capacity, contact details, preferred giving methods.	Name, address, phone, email, financial patterns, giving preferences across decades.	Career info, employer details, employment history, contact methods for social engineering follow-up.	SSNs, financial aid data, family contact info, banking details for federal loan disbursement.
Why It Matters	**Direct path to high-net-worth individuals**; one breach = entire donor pipeline exposed.	**Donors are repeat victims**; stolen info fuels identity theft and donation fraud.	**Alumni can be used to re-target staff and faculty** because they are a trusted network.	**Students = are prime targets for identity theft**; younger victims with longer credit histories.
The Real Impact	Princeton's compromised advancement database put **100,000+ donors** at risk of targeted fraud.	Harvard's November 2025 breach exposed **decades of alumni giving records**; **lawsuits** followed.	One compromised alumnus becomes a vector for **spear-phishing campaigns** at the university.	UPenn's **1.2M student records** led to years of **identity theft complaints** and **regulatory exposure**.

INTRODUCING RESILIENTTECH ADVISORS

ResilientTech Advisors
Empowering Resilient Technology

Julie C. Chatman

Founder & CEO

Former FBI insider-threat program manager, leading a 22-member team handling 150+ investigations per year.

Dr. Sybil L. Ingram

Principal, Compliance & Risk

PhD Health Science. Expert in HIPAA, GDPR, ISO 27001, SOC 2. Led multi-year audits across large federal public sector organizations.

Raj Sahas

Principal, Security Engineering & Operations

20+ years leading enterprise security for Fortune 500. Cloud, AI/ML governance, secure research collaboration, incident response at scale.

HOW WE WORK

Clarity over jargon.

Substance over spin.

Integrity, always.

OUR COMMITMENT TO ACADEMIC CULTURE

Transparency

We work openly with governance teams, faculty, staff, and students without hidden surveillance or secret escalations. Communication about our actions, reasons, and findings is clear and continuous.

Proportionality

Not every security issue demands heavy-handed controls. We differentiate accidental mistakes needing education from malicious intent requiring escalation, calibrating controls to real risk levels.

Privacy by Design

FERPA compliance is embedded from day one. We explicitly protect faculty academic freedom and student privacy, ensuring your institution’s policies guide our approach to security.

Cultural Impact Measurement

Success is measured beyond technical metrics, including training reach, reporting volume, trust in security teams, and reductions in phishing-vulnerable behaviors.

ResilientTech Advisors
Empowering Resilient Technology

THE WORKSHOP: A HALF-DAY SESSION

- **Format**: Virtual or In-Person
- **Duration**: 4 hours
- **Investment**: Virtual $6,800 (All-inclusive. Travel is billed separately for in-person sessions)
- **Participants**: CISO, IT leadership, Risk Management Leadership
- **Pre-workshop**: Share with us – your org chart; current phishing training, metrics, & results; tech stack; internal IT security challenges; recent incidents. Confidentiality is assured via NDA.
- **Outcome**: Written gap analysis, resilience roadmap with next steps, and materials for executive briefings within 7 business days after the workshop.

SAMPLE WORKSHOP AGENDA

Phishing Threats Overview

Review recent university phishing incidents and attacker methods. Understand why universities are targeted and what your institution faces.

Mapping People, Process & Tech

Discuss current training, reporting, governance, and security tools. Discuss strengths and gaps interactively.

Identify Gaps & Quick Wins

Pinpoint top risks and brainstorm quick wins (e.g., social engineering simulations, improved workflows.) Plan a 6–12-month roadmap.

Readout & Next Steps

Summarize findings, hold Q&A, and define action items with a timeline for leadership briefing and any follow-up work you choose to pursue.

ResilientTech Advisors

Empowering Resilient Technology

Let’s start a conversation about building resilience on your campus.

Get in touch:

jchatman@resilienttechadvisors.com

+1 (804) 621-1136

https://resilienttechadvisors.com/