INFORMATION SECURITY OFFICE BRIEF FINANCIAL SERVICES WORKSHOP 2025

AGENDA

- THREAT LANDSCAPE // ATTACK SURFACE

- ANATOMY OF A CYBER ATTACK

- WHY DOES THIS MATTER TO YOU

- ECU INFORMATION SECURITY OFFICE SERVICES

- QUESTIONS

THREAT LANDSCAPE

\\

ATTACK SURFACE

LIVE THREAT MAP

ANATOMY OF A CYBER ATTACK

WHY DOES THIS MATTER TO YOU
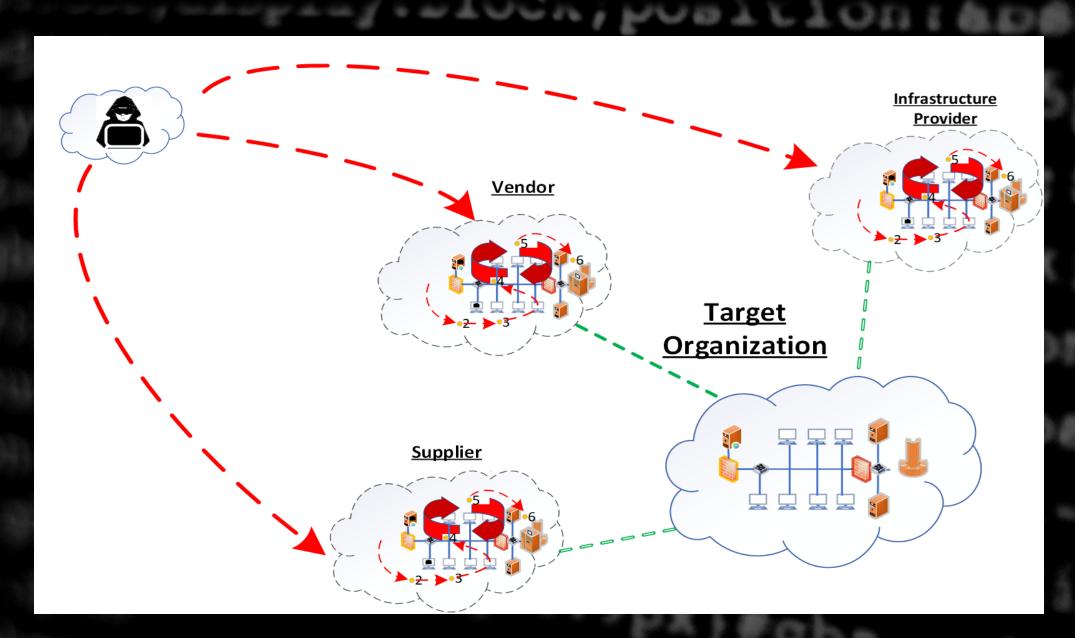
HERE'S WHY IT MATTERS:

Protection of Sensitive Financial Data

- Financial departments like the Cashier's Office, Accounts Payable, and Payroll ==manage tuition payments==, ==vendor transactions==, and ==employee salaries==.

- Cyberattacks can lead to ==financial fraud==, ==unauthorized fund transfers==, or ==exposure of Social Security numbers==, ==bank details==, and ==tax information==.

Defense Against Cyber Threats

- Phishing & Social Engineering: Cybercriminals target financial employees with ==fraudulent emails==, ==impersonating university officials== or ==vendors== to ==steal login credentials==.

- Ransomware Attacks: Universities are frequent targets of ransomware, which can ==lock financial systems== and ==demand payment== for ==data restoration==.

- Insider Threats: Employees or compromised accounts could be ==exploited== to ==alter payroll records==, ==manipulate transactions==, or ==steal funds==.

Compliance and Legal Responsibilities

- Higher education institutions must comply with ==FERPA==, ==PCI DSS==, and other ==financial regulations==.

- A data breach can lead to ==hefty fines==, ==legal action==, and ==reputational damage== if financial records or student information are exposed.

Vendor and Third-Party Risks

- Financial services often integrate with external vendors for ==payment processing==, ==payroll==, and ==student aid disbursement==.

- A cyberattack on a vendor could compromise the institution's ==financial ecosystem==, leading to ==fraud== or ==system disruptions==.

ECU INFORMATION SECURITY OFFICE SERVICES

SERVICES

➢ Information Security \\ Cybersecurity Training & Awareness

➢ Information Security \\ Cybersecurity Consultations

➢ Technology Security Assessments

➢ Risk Acceptances

SUPPORTS

➢ Information Security \\ Cybersecurity Incident Response

➢ Information Security \\ Cybersecurity Compliance & Policies

➢ Information Security \\ Cybersecurity Posture at the University

➢ External Security Testing

➢ Security Process Improvement Initiatives

THANK YOU

Mike Barry

Information Security Specialist

252-328-9554

barrymi16@ecu.edu

Information Technology and Computing Services