2021 Annual Report to the Board of Trustees
Compliance, Audit, Risk and Legal Affairs Committee

Cybersecurity Briefing

September 28, 2021

Donna R. Heath
Vice Chancellor for Information Technology
& Chief Information Officer

Casey J. Forrest
Chief Information Security Officer
AGENDA

- Year In-Review - FY2020-2021
- Data & Trend Analysis
- Current Initiatives - FY2021-2022
- OSA IT General Controls Audit
- Future Plans - FY2022-2023
- Discussion
YEAR IN REVIEW - FY2020-2021

- Provided critical support and tactical response for key events
  - Finance Audit, Financial Aid Audit, IR Cyber Attestation, HR terminations, Litigation holds, etc.

- Improved Security Awareness training & education compliance
  - Next campaign to begin during October Cybersecurity Awareness Month

- Completed agreement with new Cyber Liability Insurance carrier
  - $5M coverage with comparable Crum & Forster; 43% cost savings in annual premium

- Refreshed or Created ITS policies and supporting documents
  - 3 Existing; 2 New -- Mobile Device Policy, and Digital Communications Policy

- Conducted Disaster Recovery Plan test activities
  - Ransomware Tabletop Exercise; and Structured Walk-through Test
  - Identified related updates and improvements

- Deployed mandatory University-wide MFA enrollment
  - Faculty, Staff, Students – Planned Completion by December 2021
DATA & TREND ANALYSIS

In 30 days UNCG’s information security systems blocked or prevented:

- **500** Malware infections
- **600** Brute force password-guessing attempts daily
- **28,000** Network intrusion attempts per day
- **32,000** Phishing attempts; 54 confirmed to date
- **125,000** blocked queries from known malware URL or IP addresses
- **500** Malware infections

Breach Patterns¹

- 86% of security breach patterns are related to Social Engineering, Miscellaneous Errors and System Intrusion

Bad Actor Motives¹

- Financial (96%), Espionage (3%), Fun (1%), Convenience (1%), Grudge (1%)

Industries Perspective¹

- Education 5th most amount of cybersecurity incidents out of 20 sectors, with 1,332 incidents.
- 62.6% increase from 2020 to 2021
- Surpassed Finance & Healthcare in 2021

¹ 2021 Verizon Data Breach Investigations Report (DBIR)
Our Top Cybersecurity Interests
- Managed Detection And Response
- Building A Secure Cloud Infrastructure
- Asset & Vulnerability Management
- Access Control Measures
- Security Awareness Education And Training
- Securing the Remote Workforce (ref.2)

Key Technologies & Practices²
- Cloud vendor management
- Multifactor authentication and single sign-on
- Endpoint detection and response
- Preservation of data authenticity and integrity
- Security of research
- Student data privacy and governance

External Support & Response
- Cyber Liability Insurance - Response Unit
- UNC-SO Security Council - Membership
- Federal Bureau of Investigation - Local Agent
- NC ISAAC Fusion Center - Cyber Unit Manager

2021 Cybersecurity Assessments
- North Carolina National Guard Cyber Assistance and Assurance Team (NCAAT)
- Financial Controls Audit - Security Access Controls
- Financial Aid - GLBA IT Risk Assessment
- MCNC ISO 27002 Maturity Assessment
- Office of State Auditor - IT General Controls Audit
CURRENT INITIATIVES - FY2021-2022

- Refill 3 Vacant ISO positions
  - Risk & Compliance Manager; Security Systems Engineer; Security Operations Analysts

- Improvements in 3rd Party Vendor Risk Management
  - Improvements in both purchasing/contracting & monitoring workflows

- Continue overhaul of IT Policy and supporting documents
  - 71 documents in-scope for refresh or creation

- Operational Security Improvements
  - Security Information & Event Management (SIEM) system, improved event data & threat intelligence feeds

- Identify UNCG Top 10 Cybersecurity Risks
  - Supports UNC-SO Policy 1400.1 and UNC IT Governance Charter requirements

- Manage & respond to external ISO 27002 Cyber Maturity Assessment
  - Engagement began August 11, 2021; Target Completion November 1, 2021

- Manage & respond to Office of the State Auditor – IT General Controls Audit
  - Engagement began July 2021; Target Completion December 2021
Objectives

**Protection of Data**
Ensure sensitive data is identified, retained and disposed of according to its classification.

**Vulnerability Management**
Processes implemented to scan, detect, classify, and remediate systems vulnerabilities on a timely basis.

**Service Provider Management**
Ensure sensitive data processed off-site with vendors or service providers are adequately protected.

Key Takeaways

- Engagement: July 2021 – December 2021
- Recent: ECU, NCAT, UNCP, WCU, ECSU
- Current: UNCG, UNCW
- First ever strong focus on Distributed Technology
- Initial 60 days: 116 Audit Requests; 192 File Uploads
- Expect to have Recommendations or Findings
- Remediations will significantly impact distributed technology functions, and could potentially require new staff in ITS
FUTURE PLANS - FY2022-2023

- Develop and Enforce Campus-wide IT Policies and Standards
  - e.g., Information Technology Risk & Compliance Manual/Standard; Integrate Asset Inventories

- Establish the IT Risk & Compliance Management programs
  - Supported by a Governance, Risk, & Compliance (GRC) module in Service Now (6-TECH)

- Improve security controls for Research enclaves
  - Anticipating increase in compliance requirements DHHS

- Continue improving Cloud-based security controls
  - Leverage tools & software for utility and practicality (Azure, Google, etc.)

- Mature Vulnerability Management Program
  - Also supports anticipated Post-Audit Response

- Expand Security Awareness Training & Outreach
  - Leverage External Partnerships
QUESTIONS?