Discussion Item

CARL-5  Cybersecurity Update

Background Information

Donna Heath, Vice Chancellor for Information Technology Services, and Dr. Casey Forrest, Chief Information Security Officer, will provide a cybersecurity update.

Attachment

5.1  Cybersecurity Briefing
2022 Annual Report to the Board of Trustees
Compliance, Audit, Risk and Legal Affairs Committee

Cybersecurity Briefing

November 29, 2022

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

Casey J. Forrest
Chief Information Security Officer
AGENDA

- Year In-Review - FY2021-2022
- Data & Trend Analysis
- Current Initiatives - FY2022-2023
- Future Focus - FY2023-2024
- Discussion
YEAR IN REVIEW - FY2021-2022

- **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**
  - 2022 campaign to began during October Cybersecurity Awareness Month

- **Russia-Ukraine War -- Cyber Security Response**
  - Implemented over 16 critical defensive measures and safeguards recommended by DHS and UNC-SO
  - Established a Bi-Weekly Cyber Risk Task Force, sponsored by CFO & CIO

- **Refreshed or Created ITS policies and supporting documents**
  - Published university-wide GDPR Privacy Notice and Privacy Statement

- **Conducted Cybersecurity Tabletop Exercises**
  - Provided separate events with Executive Crisis Policy Group; ITS; HIPAA Committee
  - Identified related updates and improvements

- **Completed OSA IT Controls Audit**
  - 203 days of audit engagement; 184 auditor requests, 574 submitted artifacts
DATA & TREND ANALYSIS

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

- **874** Malware infections
- **511 million+** Network intrusion attempts
- **273,266** Brute force password-guessing attempts
- **18,066** Phishing attempts; 42 confirmed, as of Sept/22
- **7,750** blocked queries from known malware URL or IP addresses
- **100,000+** Spam emails

UNCG Perimeter Intrusion Activity

**February 2022**
- Malicious connection attempts from host in Russia
  
  *Daily average of 300k-400k, spiked to 1.3M*

**October 2022**
- Denial of Service (DoS) attack from host in France
  
  *Normal session count of 600k, spiked to 8M*

30 Day Intrusion Attempts Report

<table>
<thead>
<tr>
<th>Country</th>
<th>Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russia</td>
<td>47M</td>
</tr>
<tr>
<td>Taiwan</td>
<td>40k</td>
</tr>
<tr>
<td>China</td>
<td>2M</td>
</tr>
<tr>
<td>France (7 days)</td>
<td>5k</td>
</tr>
<tr>
<td>North Korea</td>
<td>0</td>
</tr>
<tr>
<td>North Carolina</td>
<td>0</td>
</tr>
</tbody>
</table>

Report Date Range: 10/7/22 – 11/6/22
DATA & TREND ANALYSIS

- Cybercrimes cost Americans $6.9B in 2021. 7% increase from last year.¹

- 80% of security breach patterns are related to System Intrusion, Basic Web Application Attacks, and Miscellaneous Errors.²

- Business email compromise attacks increased 39% in U.S., accounting for $2.3B in losses.³

- $2.73M average cost of ransomware attacks in Education. 48% higher than the global average, and highest among 13 industries.⁴

- The average business will invest between 6% and 14% of its annual IT budget in cybersecurity.⁵

- Bad Actor Motives²
  - Financial (95%)
  - Espionage (5%)

- 53% increase Number of overall attacks against higher education in 2021.⁵

UNCG Top Cybersecurity Interests

- Managed Detection And Response⁸
- Maintain a Secure Cloud Infrastructure
- Asset & Vulnerability Management
- Access Control Measures
- Security Awareness Education And Training
- Securing the Remote Workforce⁹

UNCG 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 Manager¹⁰
- Joint Cybersecurity Task Force (JCTF)¹¹
CURRENT INITIATIVES - FY2022-2023

- Implementation of a comprehensive IT governance program
  - 60% of distributed technology personnel workplans allocated to Information Technology Services
  - Centralize IT Procurement and IT Asset Inventory across the University
  - Centralize security controls and management of security functions (central and distributed IT)

- 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 Microsoft 365 Compliance and Cybersecurity requirements
  - Supports UNCG’s future state, single destination for file storage and collaboration tools

- Integrated response to Office of the State Auditor – IT General Controls Audit
  - Engagement completed May 2022
FUTURE FOCUS - FY2023-2024

- Develop and Enforce Campus-wide IT Policies and Standards
  - e.g., Minimum Information Security Controls; Information Security Audit and Compliance Reviews

- Establish the IT Risk & Compliance Management programs
  - Supported by a dedicated Governance, Risk, & Compliance (GRC) platform

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

- Continue improving Cloud-based security controls
  - Leverage licensed tools & software for highest utility (e.g., Azure)

- Overhaul ITS Disaster Recovery Plan
  - Enhancements will enhance cyber incident response and support cloud-first modernization

- Institute Cyber Threat Hunting as proactive cyber defense activity
  - Detect and isolate advanced threats that evade our existing security solutions

- Expand Security Awareness Training & Outreach
  - Leverage External Partnerships
QUESTIONS?
Find your way here