Information Security Update
Annual Report

Sharyne A. Miller
Chief Information Officer

William Wetherill
Director of Information Security

July 18, 2019

UNCW
University of North Carolina Wilmington
The Office of Information Security supports campus success through coordinating campus-wide security services and offering guidance to help safeguard the confidentiality, integrity, and availability of the University’s information and information systems.

Support university strategic priorities while simultaneously reducing risk.

<table>
<thead>
<tr>
<th>Devices</th>
<th>Emails</th>
<th>Logs Processed</th>
</tr>
</thead>
<tbody>
<tr>
<td>127,637</td>
<td>225,795,180</td>
<td>30 terabytes</td>
</tr>
</tbody>
</table>

Statistics over the last 12 months
Information Security Misconceptions

- Technology solutions are sufficient to address security risks and threats.
- Security is an add on task to the real work of IT staff.
- Security is expensive and time-consuming only when an institution is breached.

Educause 18-19 Top 10 IT Issues
Information Security Staff

- Director of Information Security - William Wetherill, CISSP
- IT Security Engineer - Brian Johnson, CISSP
- IT Security Operations – Search Underway

Certified Information Systems Security Professional (CISSP)
- The CISSP designation is a globally recognized, vendor-neutral standard attesting to an IT security professional's technical skills and hands-on experience implementing and managing a security program.
- As of December 31, 2018 there are 131,180 (ISC)² members holding the CISSP certification worldwide, in 171 countries
Top 5 Vulnerabilities

- Uninformed Users
- Default and Weak Credentials
- Unpatched Software
- Incomplete Monitoring
- Cloud, Mobile, and IoT Devices
Information Security Mission

The office of information security strives to implement a strategically aligned security program with a principled and measured approach to reducing information security risk while championing a sustainable and effective security culture in the campus community.
Higher Education Threat Profile

A cyber threat is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains.

Source: 2019 Verizon Breach Report
Information Security Risk Strategy

Biggest Direct Threats to UNCW:

• Phishing
• Denial of Service
• Ransomware
The Risk from Phishing

• Email continues to be the primary vector (96%) for attacks

• Nationally, 30% of U.S. users open phishing emails

• 12% of those who opened phishing emails later opened the infected links or attachments.

Source: 2018, Verizon Data Breach report
Phishing Risk Response

- Average of 51 emails with malware attachments blocked daily
- 65k possible phishing emails blocked daily
- Over 200k spam emails blocked per day
- 54% of email never makes it to an inbox
- Blocked over 10 million website requests to known malicious sites over the last 12 months
Phishing Risk Response

Other security controls -
• Malicious site filtering
• Reporting - phishing@uncw.edu

The opportunities -
• Incomplete Information Security Awareness Training Coverage
• Continue Multifactor Authentication rollout
The Denial of Service Risk

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.
Denial of Service Attacks

- 5 DDOS Cyber Attacks this year were stopped before they could negatively impact the University
Denial of Service Risk Response

- Cyber Insurance
- Disaster Recovery / Business Continuity Planning
- Critical Information System Resiliency
- Data Backup
- Incident Response / Triage
The Ransomware Risk

Ransomware is a type of malware threat actors use to infect computers and encrypt computer files until a ransom is paid.
National Ransomware Attacks

- **Greenville, NC** - ransomware attack April 10 – 23 on 750 computers did not pay ransom.
- **Baltimore, Md** - May 7 through June 12 (70% up). City has paid over $18 million, hackers demanded $76,000
- **Riviera City, FL** - paid $600,000 to hackers in June
- **Lake City, FL** - paid $500,000 in late June after being down for 2 weeks.
Ransomware Risk Response

- Cyber Insurance
- Disaster Recovery / Business Continuity Planning
- Critical Information System Resiliency
- Data Backup
- Incident Response / Triage
A Proactive Approach

- Security Incident and Event Monitoring
  - Security Operations Center investigates ~2000 security incidents a month
  - Leveraging Advanced Detection and Response Services to combat the threat before the impact

- Information Security Awareness Training
  - ITS completed mandatory training
  - Campaign being developed for university wide training
Initiatives

• Cyber Security Program and Roadmap
• Optional Multifactor Authentication for Students, Faculty and Staff – Fall 2019
• New Data Governance Committee in development
• IT Governance Redesign
• 3rd Party Identity and Access Management beginning implementation
Initiatives

- Table Top for Incident Response
- Third Party Risk Assessments
- Establishing Annual Audit Plan
- Internal Risk Assessments - ERM
- Campus and Local Community Engagement
Conclusion

In an increasingly interconnected environment, information is exposed to a growing number and wider variety of risks.

Threats, such as those outlined in this presentation, and many others, will continue to become more common, ambitious, and sophisticated.

Information Security is a critical initiative for the University that must continually rise to the demands of our changing threat landscape.