Impacts of Pandemic

• IT priorities shifted and highlighted the need for increased security
• IT focused on making remote working possible, easier and more secure
• Addressed and monitored vulnerabilities associated with 3rd party software
• Quickly responded to practical work needs such as sign a document or meet virtually as a public body
• Most central IT staff worked remote except for mandatory staffing needs
• Data management and software compliance needs escalated
Current National Threats

67% of reported breaches resulted from credential theft and social attacks (phishing, business email compromise, etc.)

Ransomware accounted for 80% of malware incidents, up from 48% in previous year

78% of attacks on web applications involved using stolen credentials

70% of incidents were caused by external actors, 30% by internal actors

92% of attacks were motivated by financial gain

819 incidents, 228 with data disclosure in 2019 within the education sector. Up from 382 incidents and 99 breaches in the previous year’s report
Risk & Threat Assessment at UNCW

Last 30 days:

193,700 2-factor authentications

Over 17 million email messages blocked as spam or phishing

Over 700,000 internet requests blocked for security (malware, phishing, crypto mining)

46,212 computer vulnerabilities remedied

1.1 billion internet requests protected

Last 12 months:

11,991 security events investigated

709,189 blocked web application attacks

1,288 campus users were assisted after their accounts were compromised

1.7 million computer vulnerabilities remedied

44.5 terabytes of events monitored

528 IT purchase compliance reviews
Policy Implementation

UNC System Office IT Policies

• **1400.1 – IT Governance**: requires each institution to have strategically aligned information technology governance within known and acceptable risk levels - responsible person reports to chancellor

• **1400.2 – Information Security**: requires each institution to establish an information security program and designate a senior officer, accountable to the chancellor, who is responsible for information security

• **1400.3 – User Access and Identity Control**: requires each institution to evaluate and conduct risk-based implementations of appropriate identity confirmation and access control techniques, such as multi-factor authentication, to control access to university data

UNCW is partially compliant with 1400.1

UNCW is compliant with 1400.2

UNCW is partially compliant with 1400.3
Policy Implementation (Cont’d)

UNCW Policies

Updated and Published in the Last 12 Months:
• 07.200.04 – Classroom Instructional Technology Baseline Standards
• 07.200.05 – Purchase Inventory Replacement and Disposal – Surplus of IT Resources
• 07.200.07 – Campus Electronic Resources Disaster Recovery Plan
• 07.200.11 – Audiovisual Media Services and Equipment

In Final Approval Review:
• 07.100.09 – Email Abuse
• 07.200.00 – Responsible Management of IT Resources
• 07.200.01 – University-Owned Computer Technology & User Support Services
• 07.200.02 – Server Management and Standards
• 07.200.03 – Network Management and Standards
• 07.200.12 – Campus Web Resources
Policy Implementation (Cont’d)

UNCW IT Security Programs, Policies & Standards

3rd Party Review In-Process:
• Vulnerability Management Standard
• Information Technology Security Incident Handling Procedure
• 07.300.01 Identity and Access Controls
• 07.300.03 Physical and Environmental Security
• 07.300.04 Cryptographic Security
• 07.300.05 Incident Investigation & Response

3rd Party Review Completed:
• Information Security Program
• IT Security Posture
• Cybersecurity Incident Response Plan (CSIRP)
• 07.300.02 Operational Security
UNCW Approaches and Mitigations to Risk

• **Supporting the Human Element of Risk**
  Security Training, Multi Factor Authentication, External Email Notification

• **Elements of Governance, Risk, and Compliance**
  IT Governance, Vendor Risk Management, Data Governance, and Enterprise Risk Management Committee

• **Tools to Manage the Complex Environment**
  Asset and Software Inventory and System Status Monitoring

• **Talent Pipeline and Employee Retention Risk**
  Partnership with the Center for Cyber Defense Education on the CCAP DoD grant to provide a pathway for apprenticeship

• **Reducing Infrastructure Risk**
  Off-Site Hosting of Critical Systems
  Next Gen Firewall and increased Network Segmentation
### Upcoming Audits & Assessments

IT audits are becoming increasingly demanding with higher expectations for security, compliance, and risk management.

<table>
<thead>
<tr>
<th>Audits</th>
<th>Assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNCW Internal Audit – ITS Resource Management</td>
<td>Payment Card Industry – Credit Card Handling</td>
</tr>
<tr>
<td>UN System Office – ISO 27002(1) Audit</td>
<td>Office of the State Auditor – Financial IT</td>
</tr>
<tr>
<td>Office of the State Auditor – IT Controls</td>
<td>UNC 1400's</td>
</tr>
<tr>
<td>TBD</td>
<td>ISO 27002</td>
</tr>
<tr>
<td></td>
<td>Security documents</td>
</tr>
</tbody>
</table>

(1) ISO 27002  “International Organization for Standardization 27002 – IT – Security Techniques”
Thank you