Cybersecurity and the Remote Workforce

Safeguarding IT at UNC Charlotte

UNC CHARLOTTE
Office of OneIT
Our University
Largest regional University in Charlotte, NC

**QUICK STATS**

- Eight colleges
- 29,615 students
- 4,500 faculty/staff
By the Numbers
Doctoral & research intensive institution

19,500+ computing devices
3 Campus locations
3,700 TB of storage
7 Cybersecurity Professionals
AWS, Azure, Google Cloud, On-Premise
4,801 remote workforce
Security Protection

1,000 system compromises blocked by Advanced Malware Protection (AMP) per month

22 million malware, phishing & spam emails blocked by Cisco Email Security (CES) per month
Security Protection

- 400 million malicious perimeter connection attempts per day on average
- 200 account compromise detections and resets per month on average
Security Protection

- 200 Command & Control (C&C) & 100 data exfiltration attempts detected by Stealthwatch monthly
- 130,000 malicious URL attempts blocked by Umbrella monthly
Breach Stats

Average cost of a U.S. Education sector breach: $4.2 million

Average breach size: 27,000 records
Our Top 3 Threat Vectors

1. **Phishing**
   Emails purporting to be from reputable sources to induce individuals to reveal personal information, such as passwords & credit card numbers.

2. **Malware**
   Short for “malicious software,” this intent to damage devices includes viruses, trojans, ransomware & spyware.

3. **Vulnerability Exploitation**
   Taking advantage of a vulnerability to compromise the confidentiality, availability, or integrity of a resource.

Additional Threats We Face

- **Brute Force Attacks**
  Relentless trial & error attacks where the hacker attempts to determine passwords or access encrypted data.

- **Nation-State Attacks**
  When hackers target government entities or any other industry with sensitive data or property. Examples include Crypto Mining resource theft & Intellectual property theft.

- **Human Error**
  Humans play a major role in the vulnerability of businesses worldwide.

- **Data Exfiltration**
  A technique used by malicious actors to target, copy & transfer sensitive data.

- **Social Engineering**
  Manipulation to get confidential information, credentials or access.

- **Denial of Service (DoS)**
  When legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

- **Credential Theft**
  The unlawful attainment of an organization's or individual's password(s) with intent to access & abuse/exfiltrate critical data & information.
On-Campus vs Remote Security

● On-Campus
  ○ IPS/IDS
  ○ Network Firewall and Segmentation
  ○ DNS Security (Umbrella)
  ○ Next-Gen Antimalware (Amp)
  ○ Hardened Configuration (Center for Internet Security)
  ○ Enhanced Monitoring and Detection with Automated Response (Splunk)
  ○ Email Security (CES)

● Remote (Managed University Devices)
  ○ DNS Security (Umbrella)
  ○ Next-Gen Antimalware (Amp)
  ○ Hardened Configuration (Center for Internet Security)
  ○ Email Security (CES)
Endpoint Security

- Next generation anti-malware (AMP)
- Domain Name System protection service (Umbrella)
  
  \[\text{DNS} = \text{"Phonebook of the internet" e.g. uncc.edu}\]

- Endpoint hardening
  
  \textit{Center for Internet Security Level 1 Security Standard}

- Regular, phased-in patching
- Rapid7 Agents continuously monitor endpoint vulnerabilities

13,000
Computers & Tablets

700
Servers
Advanced Malware Protection (AMP)

- Like virus protection but better because it pulls in threat information from multiple agencies in real-time
- Deployed on University managed endpoints & servers
Umbrella
Domain Name System (DNS) protection service

*DNS = “Phonebook of the internet” e.g. uncc.edu*

- Protects users on- & off-campus from malicious websites by utilizing software installed on each University computer that analyzes web traffic
- Uses a global database of recognized offenders
- Stops attacks earlier with real-time analysis of unknown websites

Image: Cisco
Cisco Email Security

- Real-time analysis
- Emails identified as “threats” are NOT delivered
- Readers immediately see emails from external senders (outside @uncc) as flagged [EXTERNAL]

From: NC Employee Forms Direct
Subject: [EXTERNAL] Urgent University Request

[Caution: Email from External Sender. Do not click or open links or attachments unless you know this sender.]
Cisco Email Security
Stealthwatch

- Detects malicious behavior patterns by sampling traffic from University network devices
- Gathers real-time data from networked devices
- Uses data to detect behavior changes & predict threats

Detects threats from non-managed network devices & any device connected to our network
Remote Workforce Risks

- Some security protection measures are only available on campus
- Expanded attack vectors
  - System theft/damage
  - Insecure home networks
  - Poor user practices
- Little to no remediation or detection capability
- Employees using personal devices to accomplish sensitive University tasks
- Social Engineering
- Data theft/loss
- Ransomware
- Denial of Service
Insecure Home/Public Networks

- Average home in the US contains 11 or more connected devices
  - Smart devices are inherently insecure, may already be compromised
    - Example Mirai Botnet (October 2016)
- Most people lack technical expertise to secure home networks against attack
- Little to no remediation or detection capability
- Eavesdropping
- No network segmentation

- Mitigation Methods
  - Use the University VPN
  - Change smart device default passwords
  - Utilize modem/router built-in firewall
BYOD vs University-Managed Devices

- Employees often utilize personal devices to accomplish sensitive tasks
- University devices used for personal business

Mitigation methods (for home)
- Keep your digital life separate
- Ensure you utilize up to date Anti-virus
- Enable host-based firewall
- Utilize DNS Security service such as OpenDNS
- Utilize a password manager (average person has 50+ online accounts)
- Use MFA anywhere possible
- Keep system and applications patched to current levels
- Utilize full disk Encryption (Bitlocker/FileVault)
- Enterprise Application Access (EAA)
- VPN
Account Compromise

- Multi-Factor is the best defense (Duo)
- OneIT detects and resets constant account compromise attempts
Social Engineering

- 80% of hacking attempts have a social aspect
- Social engineering is non technical attack type, but is often combined with technical attacks
- Remote workers have additional distractions = more susceptible
- Social attacks work best when there is a lack of established documented procedures

- Mitigation Methods
  - Security Awareness Training (SAT)
  - Establish written procedures for sensitive business tasks
  - Ensure employees are trained and held to policies and standards
Phishing

● Phishing email is the No. 1 threat vector
● Over 50% of incoming emails are threats
● Remote work = distractions = more susceptible

● Mitigation Methods
  ○ Security Awareness Training (SAT)
  ○ Cisco Email Security (CES)
  ○ Umbrella DNS Protection
  ○ Phishing Training
  ○ Next Generation Anti-malware (AMP)
Vulnerability Management

Last Month
- Total Vulnerabilities: 2,419,240
- Remediated: 2,075,805 (-33.7%)
- New: 848,915 (-63.8%)

Remediation
- Current Vulnerability Count: 1,921,806 (-20.6%)

Top 10 Riskiest Assets

<table>
<thead>
<tr>
<th>Area</th>
<th>Asset</th>
<th>OS</th>
<th>Owner</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHC</td>
<td>SASDC08TSK9IWW</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>826335</td>
</tr>
<tr>
<td>Urban</td>
<td>UBNBC04M7J7WLT</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>810563</td>
</tr>
<tr>
<td>CLAS</td>
<td>PSYCC443N02WGS</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>780726</td>
</tr>
<tr>
<td>COAA</td>
<td>AART062DHTJAWS</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>703575</td>
</tr>
<tr>
<td>CDE</td>
<td>CDE-4C3JK02</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>707794</td>
</tr>
<tr>
<td>CLAS</td>
<td>XANTHS15SQ7ZW</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>699268</td>
</tr>
<tr>
<td>Business Affairs</td>
<td>BAFM78LJ32WLT</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>697405</td>
</tr>
<tr>
<td>FM</td>
<td>FM38GB3WWS</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>667432</td>
</tr>
<tr>
<td>CLAS</td>
<td>MAS4DMFM02WWS</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>661593</td>
</tr>
<tr>
<td>DCS</td>
<td>OC3SH0043M3WL</td>
<td>Windows 10</td>
<td>Brandon DeLee...</td>
<td>500906</td>
</tr>
</tbody>
</table>

Highest Risk Assets by Area

<table>
<thead>
<tr>
<th>Name</th>
<th>Assets</th>
<th>Vulnerabilities</th>
<th>Avg # Asset</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNCC - CXE</td>
<td>1733</td>
<td>267,717</td>
<td>154</td>
<td>88928504</td>
</tr>
<tr>
<td>UNCC - CDE</td>
<td>231</td>
<td>299,236</td>
<td>130</td>
<td>7624826</td>
</tr>
<tr>
<td>UNCC - CLAS</td>
<td>1481</td>
<td>171,261</td>
<td>116</td>
<td>49970976</td>
</tr>
<tr>
<td>UNCC - BCD</td>
<td>511</td>
<td>585,681</td>
<td>109</td>
<td>12917654</td>
</tr>
<tr>
<td>UNCC - FM - Facilities</td>
<td>257</td>
<td>273,177</td>
<td>106</td>
<td>10199035</td>
</tr>
<tr>
<td>UNCC - CCI</td>
<td>972</td>
<td>818,009</td>
<td>84</td>
<td>2157288</td>
</tr>
<tr>
<td>UNCC - Library</td>
<td>523</td>
<td>437,544</td>
<td>84</td>
<td>10879009</td>
</tr>
<tr>
<td>UNCC - CHHS</td>
<td>387</td>
<td>317,500</td>
<td>82</td>
<td>9972774</td>
</tr>
</tbody>
</table>

[Graph showing asset counts and vulnerability counts]
Expanded Risk Vectors

- Unauthorized remote access tools
- Lack of Data Loss Protection (DLP)
- Non-University Cloud Services
- Freeware
- Local Admin
- Security Awareness Training not required for all UNCC Staff/Faculty
Cyber Resilience

- Defense in Depth
- User training
- Zero-Trust architecture
- Continuous monitoring
- Incident Response tabletop exercises
- Identity based access control
- Cyclical Vulnerability Management
- Cybersecurity Insurance

“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him”

Sun Tzu, The Art of War
What makes us Cyber Resilient?

OneIT prepares for, responds to & recovers from cyber attacks when they occur at UNC Charlotte.

- We defend against cyber attacks with a Defense in Depth methodology
- We limit the effects of a security incident
- We guarantee the continuity of University operations during & after the attacks