Information Security
Annual Report to the Board of Trustees
Committee on Compliance, Audit, Risk and Litigation (CARL)
The Year in Review – FY2018-19

• Formulated a Strategic plan for Information Security improvements
  • Key components are Governance, Security Operations, Risk Management, and Regulatory Compliance

• Implemented Organizational Changes
  • Reorganized team into four sub-teams:
    • Architecture, Engineering, Operations, Risk & Compliance Management
  • Received funding approval and hired three new positions:
    • Security Operations Analyst, Security Engineer, Risk & Compliance Manager

• Provided critical support and tactical response for key events
  • Advancement issue, SHS ransomware, PD assistance, HR terminations, Litigation holds

• Improved Security Awareness training & education compliance
  • 2017: 63%, 2018: 87%, 2019: 93%

• Improved Visibility and Governance posture
  • Participating in 8 different councils, committees, and working groups

• Increased Cyber Liability Insurance
  • $5MM coverage from Beazley Breach Response
Current Initiatives – FY2019-20

• Overhaul of IT Policy and supporting documents
  • 71 documents in-scope for refresh or creation

• Improvements in Identity & Access Controls
  • Migration to modern identity management platform, implementation of new access controls

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

• Security Awareness Training & Education (SATE) improvements
  • New Security Awareness training provider for CY2020
  • Taking steps towards implementing Phishing susceptibility assessments

• Improvements in Cloud Security posture
  • Shifting to platform-focused security tools via key partnerships with Microsoft and Google

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

• Establish the IT Risk & Compliance Management programs
  • Supported by a Governance, Risk, & Compliance (GRC) tool implementation starting in CY2020

• Strategic, mandated increases in 2FA adoption for High Risk data users
  • ITS, Finance department, HIPAA Covered Entities

• ITS, Finance department, HIPAA Covered Entities
Future Plans – FY2020-21 and beyond

• Mature our compliance and risk management programs
• Continue maturing our Security Operations
• Continue migration to modern IAM controls & processes
  • Push for mandatory University-wide 2FA
• Continue improving Cloud-based security controls
• Improve security controls for Research enclaves
• Continue developing & empowering the team
• Monitor and react to changes in the regulatory environment
Find your way here
Appendix

Detailed information about specific projects, activities, technologies, and
Information Security Program Improvement Plan

• Objectives and Key Goals:
  ➢ Reorganize the team and staff key positions
    □ Pursue funding support for additional positions
    □ Reorganize team to support scalability and alignment with IT staff
  ➢ Overhaul IT policy and supporting documentation
    □ Rationalize, modernize, realign, and refresh all existing policies and supporting documents
    □ Create new documents to fill key gaps in policy
    □ Implement practices aimed at achieving sustainable support for administrative controls
  ➢ Create and implement an IT Risk Management program
    □ Implement a program of repeating risk assessments and self-identification
    □ Establish procedures for risk analysis, treatment, and reporting
  ➢ Create and implement an IT Compliance Management program
    □ Implement mechanisms to support periodic assessment and reporting for regulatory compliance
  ➢ Achieve 24x7 Operational Security capabilities
    □ Implement improvements to security operations tools and processes
  ➢ Implement Continuous Improvement methodologies
    □ Adopt Capability Maturity Model Integration (CMMI) for process improvement and appraisal
# Key Partnerships

## UNCG Committees, Councils, & Working Groups

- HIPAA Compliance Committee (co-chair)
- Data Governance Committee (member)
- IAM Governance Committee (chair)
- GDPR Working Group (chair)
- ITS Enterprise Architecture Group (member)
- ITS Change Advisory Board (member)
- Distributed Technology Services partnerships
- Future:
  - Risk Management Committee
  - Compliance Management Committee

## External Partnerships

- UNC Information Security Council (chair)
- REN-ISAC (officer)
- MS-ISAC (member)
- InfraGard (member)
- North Carolina Higher Education Information Security (NC-HEIS) coalition (member)
## Defense Against Common External Threats

<table>
<thead>
<tr>
<th>Ransomware</th>
<th>Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Anti-Virus / Anti-Malware (MS-SCEP) on endpoints prevents infection</td>
<td>• Google G-Suite contains built-in defenses against phishing that leverages reports and data from all Google clients</td>
</tr>
<tr>
<td>• Network segmentation and IAM controls for administrative privileges limit the extent of infection</td>
<td>• Enterprise Security Gateway (Cisco Umbrella) prevents users from reaching known malicious sites after they click a link in an email</td>
</tr>
<tr>
<td>• Enterprise Security Gateway (Cisco Umbrella) prevents malware from activating by preventing calls to known Command &amp; Control (C2) servers</td>
<td>• User awareness training highlights phishing as a key concern and delivers knowledge about how to detect and prevent attacks</td>
</tr>
<tr>
<td>• Data storage on Cloud services (Box, MS-OneDrive, Google Drive) leverages built-in ransomware defenses in SaaS apps.</td>
<td></td>
</tr>
</tbody>
</table>
Cloud Security Posture

• In alignment with UNCG’s continued trend towards cloud services and cloud-based computing infrastructure, the Information Security team will continue to pursue new and additional cloud security tools and methodologies in order to ensure the safety of cloud-based information resources.

• Targeted tool improvements:
  • Microsoft Azure Sentinel & Security Center
  • Security and investigation tools acquired via Google Enterprise for Education license
  • 3rd party vendor security ratings from BitSight

• Additional opportunities:
  • Industry standardization for cloud security posture monitoring, reporting, & assessment
## Prevent
- Policies & Standards
- Access controls
- Risk assessments
- Identity Management
- Multi-Factor Authentication
- Network firewalls
- Network Admission Control
- Enterprise Security Gateway
- User Awareness Training
- Threat Intelligence
- Anti-Virus software

## Detect
- SEIM system
- Network NGFW/IDS
- Network Behavioral Anomaly Detection
- Vulnerability Management
- Data audit & classification
- Phishing Assessment
- Penetration Testing

## Respond
- Incident Response Plans
- Investigation Tools
- Digital Forensics
- Cyber Insurance
- Disaster Recovery Plan
Security Volumes @ UNCG

Compromised Accounts per Month

DMCA Complaints by Month

Potential Compromise Events (Workstation)* by Month
Security Volumes @ UNCG

Confirmed Phishing Emails per day (uncg.edu)

Suspicious Attachments per day (uncg.edu)

Suspicious User Login Attempts per day (G-Suite)
## Tools & Solutions – Detective Controls

<table>
<thead>
<tr>
<th>Control Type</th>
<th>Control Area</th>
<th>Tool / Solution</th>
<th>Maturity Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detective</td>
<td>3rd party risk assessment</td>
<td>TBD</td>
<td>n/a</td>
</tr>
<tr>
<td>Detective</td>
<td>Cloud Security Monitoring</td>
<td>MS-Azure &amp; Google security tools</td>
<td>New</td>
</tr>
<tr>
<td>Detective</td>
<td>Data Classification, Audit, &amp; Protection</td>
<td>Varonis DatAdvantage</td>
<td>Improving</td>
</tr>
<tr>
<td>Detective</td>
<td>Digital Forensics</td>
<td>FTK</td>
<td>Mature</td>
</tr>
<tr>
<td>Detective</td>
<td>Email Security</td>
<td>Google G-Suite</td>
<td>Mature</td>
</tr>
<tr>
<td>Detective</td>
<td>Endpoint Detection &amp; Response</td>
<td>Microsoft Defender ATP</td>
<td>Maturing</td>
</tr>
<tr>
<td>Detective</td>
<td>Host Intrusion Detection &amp; File Integrity Management</td>
<td>Linux Advanced Intrusion Detection Engine (AIDE)</td>
<td>Mature</td>
</tr>
<tr>
<td>Detective</td>
<td>IT change risk assessment</td>
<td>ITS Change Management Process</td>
<td>Mature</td>
</tr>
<tr>
<td>Detective</td>
<td>IT controls self-audit &amp; risk assessment</td>
<td>ISO 27002 Gap Crosswalk</td>
<td>Maturing</td>
</tr>
<tr>
<td>Detective</td>
<td>Network Behavior Anomaly Detection</td>
<td>StealthWatch</td>
<td>Mature</td>
</tr>
<tr>
<td>Detective</td>
<td>Network device configuration compliance management</td>
<td>NetMRI</td>
<td>Mature</td>
</tr>
<tr>
<td>Detective</td>
<td>Network Threat Detection</td>
<td>FireEye</td>
<td>Improving</td>
</tr>
<tr>
<td>Detective</td>
<td>Packet Capture for Investigations</td>
<td>Arista, Endace PCAP</td>
<td>New</td>
</tr>
<tr>
<td>Detective</td>
<td>Penetration Testing</td>
<td>TBD</td>
<td>Planned</td>
</tr>
<tr>
<td>Detective</td>
<td>Periodic Firewall Rule Reviews</td>
<td>TBD</td>
<td>n/a</td>
</tr>
<tr>
<td>Detective</td>
<td>Periodic user access reviews</td>
<td>TBD</td>
<td>Planned</td>
</tr>
<tr>
<td>Detective</td>
<td>Security Event Information Management</td>
<td>Splunk</td>
<td>Maturing</td>
</tr>
<tr>
<td>Detective</td>
<td>Security posture assessment</td>
<td>Internal SPRA Process</td>
<td>Maturing</td>
</tr>
<tr>
<td>Detective</td>
<td>Server configuration compliance management</td>
<td>Ancible</td>
<td>New</td>
</tr>
<tr>
<td>Detective</td>
<td>Threat Intelligence</td>
<td>FireEye, Anomali</td>
<td>New</td>
</tr>
<tr>
<td>Detective</td>
<td>Vendor / 3rdparty security monitoring</td>
<td>BitSight Security Ratings</td>
<td>New</td>
</tr>
<tr>
<td>Detective</td>
<td>Vulnerability Management</td>
<td>Rapid7</td>
<td>Maturing</td>
</tr>
<tr>
<td>Detective</td>
<td>Web App Security testing</td>
<td>DorkBot, Burp Suite</td>
<td>Mature</td>
</tr>
</tbody>
</table>
## Tools & Solutions – Preventative & Administrative Controls

<table>
<thead>
<tr>
<th>Control Type</th>
<th>Control Area</th>
<th>Tool / Solution</th>
<th>Maturity Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventative</td>
<td>Access Management</td>
<td>Grouper</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Anti-Virus / Anti-Malware</td>
<td>Microsoft System Center Endpoint Detection (SCEP)</td>
<td>Maturing</td>
</tr>
<tr>
<td>Preventative</td>
<td>Data Loss Prevention (DLP)</td>
<td>SpiriionIdentityFinder</td>
<td>Improving</td>
</tr>
<tr>
<td>Preventative</td>
<td>DDOS Mitigation</td>
<td>MCNC</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Directory Services</td>
<td>LDAP</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Endpoint Encryption</td>
<td>MBAM / BitLocker</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Exploit PoC testing</td>
<td>MetaSploit</td>
<td>Improving</td>
</tr>
<tr>
<td>Preventative</td>
<td>Group Security Policy</td>
<td>MS-Active Directory</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Identity Management</td>
<td>Microsoft Identity Manager</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Information Security Awareness Training</td>
<td>KnowBe4</td>
<td>New</td>
</tr>
<tr>
<td>Preventative</td>
<td>Mobile Device Security</td>
<td>MS-InTune, JAMF</td>
<td>Mature, New</td>
</tr>
<tr>
<td>Preventative</td>
<td>Multi-factor Authentication</td>
<td>Duo</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Network Admission Control (NAC)</td>
<td>ArubaClearpass</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Network Firewalls</td>
<td>Cisco Firepower</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Next-Generation Firewall + Intrusion Detection/Prevention</td>
<td>Palo Alto</td>
<td>Mature</td>
</tr>
<tr>
<td>Preventative</td>
<td>Phishing Susceptibility Assessment &amp; Training</td>
<td>KnowBe4</td>
<td>New</td>
</tr>
<tr>
<td>Preventative</td>
<td>Privileged account management</td>
<td>TBD</td>
<td>Planned</td>
</tr>
<tr>
<td>Preventative</td>
<td>Secure Internet Gateway</td>
<td>Cisco Umbrella</td>
<td>Maturing</td>
</tr>
<tr>
<td>Preventative</td>
<td>Secure Password Storage for shared credentials</td>
<td>PassManPro, LastPass</td>
<td>Mature, New</td>
</tr>
<tr>
<td>Preventative</td>
<td>Security Orchestration and Automated Response (SOAR)</td>
<td>TBD</td>
<td>n/a</td>
</tr>
<tr>
<td>Administrative</td>
<td>eDiscovery</td>
<td>TBD</td>
<td>n/a</td>
</tr>
<tr>
<td>Administrative</td>
<td>Policies &amp; Standards maintenance</td>
<td>ServiceNow GRC &amp; KnowledgeBase</td>
<td>New</td>
</tr>
<tr>
<td>Administrative</td>
<td>Regulatory compliance reporting</td>
<td>ServiceNow GRC</td>
<td>New</td>
</tr>
</tbody>
</table>
Skill Gaps & Team Development

• Areas where skill development is needed:
  • Oracle/DB security
  • Banner security
  • Cloud security
  • Application security
  • Project management

• Future growth opportunities for team members
  • Technical and managerial (supervisory) leadership
  • System-level peer development and networking
  • Involvement in national programs and research opportunities

Team Composition (8 people)

• 1 x Chief Information Security Officer
• 1 x Security Architect
• 2 x Security Systems Engineers
• 2 x Security Operations Analysts
• 1 x Risk & Compliance Manager
• 1 x Compliance Analyst

Professional qualifications include: CISSP, CRISC, GPEN, PCIP, ITIL, CISA and several vendor technical certifications