UNC GREENSBORO

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

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*

UNC GREENSBORO

Appendix

Detailed information about specific projects, activities, technologies, and

UNC GREENSBORO

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

Ransomware

- Anti-Virus / Anti-Malware (MS-SCEP) on endpoints prevents infection
- Network segmentation and IAM controls for administrative privileges limit the extent of infection
- Enterprise Security Gateway (Cisco Umbrella) prevents malware from activating by preventing calls to known Command & Control (C2) servers
- Data storage on Cloud services (Box, MS-OneDrive, Google Drive) leverages built-in ransomware defenses in SaaS apps.

Phishing

- Google G-Suite contains built-in defenses against phishing that leverages reports and data from all Google clients
- Enterprise Security Gateway (Cisco Umbrella) prevents users from reaching known malicious sites after they click a link in an email
- User awareness training highlights phishing as a key concern and delivers knowledge about how to detect and prevent attacks

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

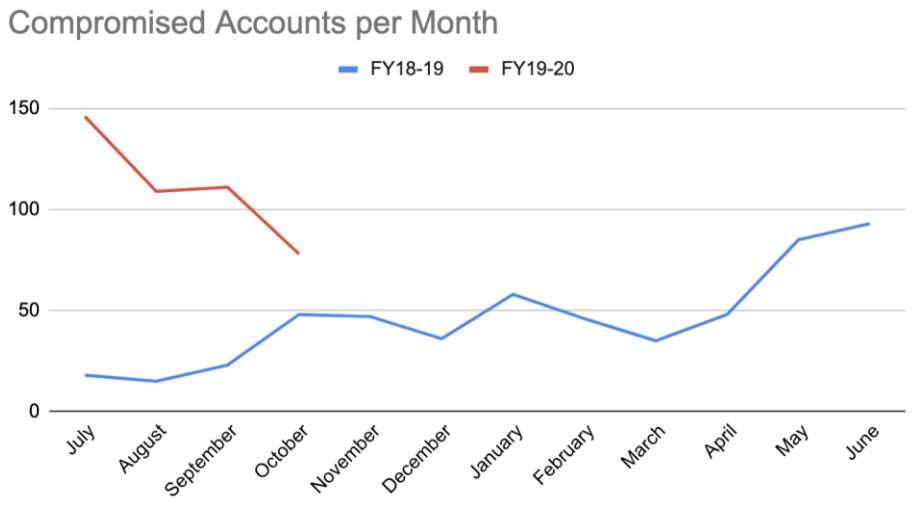
- SEIM system
- Network NGFW/IDS
- Network Behavioral Anomaly Detection
- Vulnerability Management
- Data audit & classification
- Phishing Assessment
- Penetration Testing

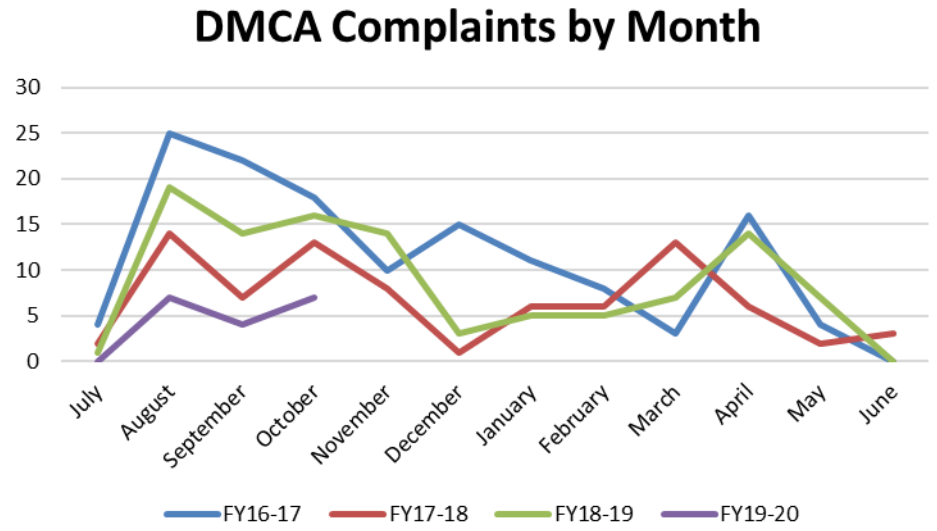
Respond

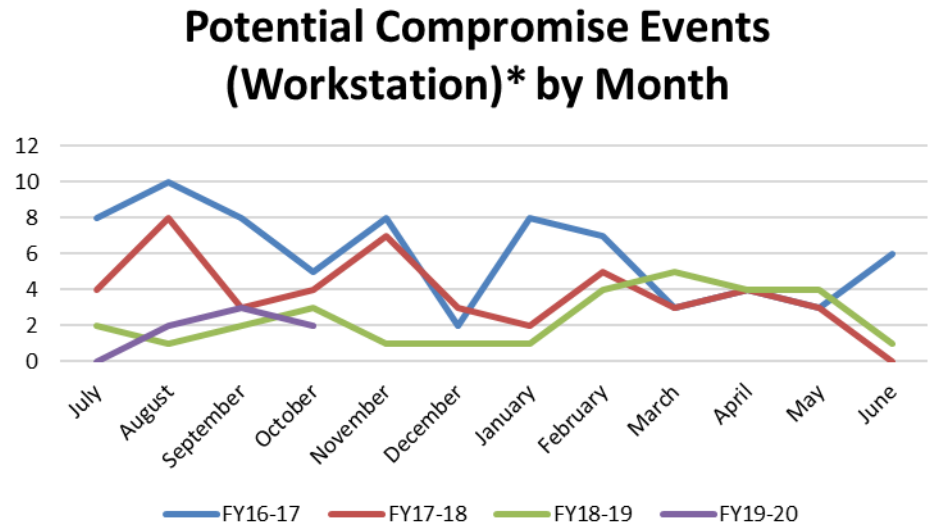
- Incident Response Plans
- Investigation Tools
- Digital Forensics
- Cyber Insurance
- Disaster Recovery Plan

UNC GREENSBORO

Security Volumes @ UNCG





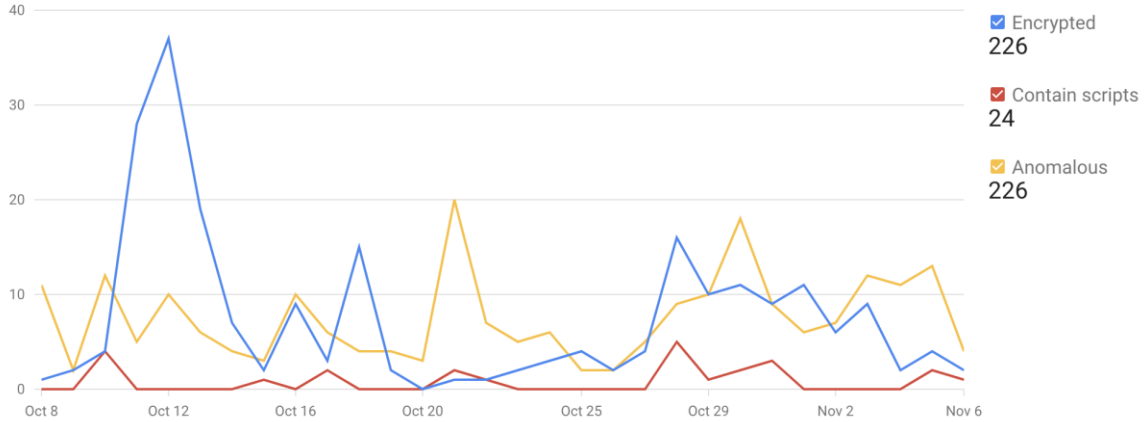


UNC GREENSBORO

Security Volumes @ UNCG

Confirmed Phishing Emails per day (uncg.edu)

Suspicious Attachments per day (uncg.edu)



Suspicious User Login Attempts per day (G-Suite)

UNC GREENSBORO

Tools & Solutions – Detective Controls

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

Tools & Solutions – Preventative & Administrative Controls

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

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