INFORMATION SECURITY LIAISON MEETING

January 30, 2019
AGENDA

• Welcome
• New CISO – Rob Ferrill
• FY2019 Initiatives
• SOC Updates
FY2019 MAJOR INITIATIVES

• Duo Two-Factor Authentication Expansion
• PII data reduction
• Desktop patching standard
• Security testing
• Secure Optidoc
• UAB ID
• Data Stewardship training
• HIPAA compliant high performance computing
• Authentication redesign
• BCP playbook / tabletops
• Block inappropriate sites
• Add research data to restricted class
• Endpoint protection evaluation
FY2019 INITIATIVES

• Duo Two-Factor Authentication Expansion
  • Automated on-boarding and off-boarding
  • Implementation phases begin March 4th
  • Mandatory for academic/administrative staff and faculty
  • Smartphone app with Push or Passcode, Call Me function, SMS text, hard tokens

** Health System is enabling MFA for Outlook Web Access for all Health System employees in March 2019 **
FY2019 INITIATIVES

• PII Reduction
  • Support Distributed IT’s Efforts
  • Types of Restricted Data
  • Current Use Cases
  • Current Plans for Reduction
FY2019 INITIATIVES

• Desktop patching standard
  • End of Life Operating Systems
    • macOS Sierra 10.12.x - September 2019
    • Windows 7 & Server 2008 – January 2020
  • Authenticated Vulnerability Scanning Findings
    • Several MS Patches require registry key to fully deploy
    • 3rd-Party application patches missing
    • Web Browser Updating (Chrome & Firefox)
    • Adobe Product Suite versions
FY2019 INITIATIVES

• Security testing
  • Welcome new Penetration Testers
  • Trustwave external pen test results
    • No critical findings
    • Planning new engagement mid-summer
• Transport Layer Encryption Standard
  • TLS1.2 is the minimum standard for all services
  • Improve configuration for Diffie-Hellman prime
  • Internet-facing web servers should disable SSLv3/TLS1.0 by June 1
FY2019 INITIATIVES

• Secure OptiDoc
  • Replacement solution Hyland OnBase forthcoming
  • Decisions need to be made around transferring all legacy documents
FY2019 INITIATIVES

• UAB ID
  • Goal here is to continue the reduction of SSN usage by transitioning to the UAB ID or the BlazerID
FY2019 INITIATIVES

• Data Stewardship training
  • Goal here is to get training rolled out for data stewards on their role and responsibilities
  • At UAB the role of the data steward is primarily defined around the responsibilities of security, privacy, and access.

• Data Steward Toolkit
  • Security & Privacy
  • Access
  • Reporting & Extracts
  • Definitions and Business Rules
  • Quality
  • Information Life Cycle
FY2019 INITIATIVES

• HIPAA compliant high performance computing
  • Goal here is to work with the Health System in architecting the HPCC or a segment within that has appropriate controls for storing ePHI
  • This is being turned into a formal project and will include efforts from several departments
FY2019 INITIATIVES

• Authentication redesign
  • Building inventory of Internet-facing webservers
  • Identify web applications which could utilize SSO capabilities
FY2019 INITIATIVES

• BCP playbook / table tops
  • Identify, mitigate, and measure risk
  • Document resiliency approach
  • Conduct tabletop exercises
  • Identify gaps
  • Update documentation
FY2019 INITIATIVES

• Block inappropriate sites
  • Plan here is to block “adult” related sites unless there is a need for a research related exception
  • These sites are typically loaded with malware and seen as high risk in addition to the harassment risk
FY2019 INITIATIVES

• Add research data to restricted classification
  • This effort is a result of criminals and nation states targeting university research data
  • A higher level of data classification for research data will allow for better protection of the data from compromise
FY2019 INITIATIVES

• Endpoint protection evaluation
  • Plan is to review several products in this space and decide which best fits our requirements
  • We will do a proof of concept with the preferred product and likely a pilot with a willing department before a full deployment
SOC UPDATES

• SSL Certificates
• DDoS Attack
SAVE THE DATE

April 10 - 11, 2019
Renaissance Ross Bridge Resort & Spa

TechBirmingham, the Central Alabama Chapter of the Information Systems Security Association (CAISSA), and the InfraGard Birmingham Members Alliance invite you to attend the 4th Alabama Cyber NOW Conference on April 10 for Full Day Training, *meals included, and April 11 for Full Day Conference at Renaissance Ross Bridge Resort & Spa.

MORE INFORMATION CAN BE FOUND AT ALABAMACYBERNOW.COM
Questions