ITS Security & Data Briefing

IT All Campus Workshop
January 23, 2024

Sorry, but your password must contain an uppercase letter, a number, a haiku, a gang sign, a hieroglyph and the blood of a virgin.

IT All Campus Workshop Info

- Website: https://www.hawaii.edu/its/itacw/
- Email: allcampus.workshop@hawaii.edu

Agenda

- Recap of 2023 security incidents/current threats
- Recap of issues identified at campus tours
- New security initiatives
  - Information Security Governance Council
  - AD assessments
  - penetration testing
  - additional training (examples: tabletop exercise, etc.)
  - endpoint detection and response (EDR)
  - Cyber Risk Management Program
- Compliance (and other) requirements
  - Google SPF/DKIM/DMARC email requirements; Google storage quota and impacts
  - PCI 4.0
  - CMMC (Cybersecurity Maturity Model Certification): Proposed Rules published on 12/16/23
  - GLBA/FTC
  - IPSC Personal Information Assessment
  - Device registration

Recap of 2023 security incidents & current threats

Breaches plus…..

- 2 **<u>major</u>** breaches - Resulted from a combination of things
  - Basic cyber hygiene (e.g. software updates, account management)
  - Active Directory environment configurations & practices
- Credential stuffing attacks
  - Over 170 compromised accounts
  - New dump of over 15M credentials – expect more attacks
- Successful phishing attack – resulted in payroll hijacking
  - Attacker used “Monkeypox” as subject of email
  - ***AND*** victims responded to MFA prompt
- ”Ghost” students

Campus Tours Summary

Common themes & issues

IT All Campus Workshop
January 23, 2024

Key Takeaways/Needs from Listening Tours

- Culture shift in how we view data – we keep too much data
- Training for technical and functional staff
- More centralized purchasing/systemwide contracts
- Centralized repositories
- Improve offboarding

New Security Initiatives

- Information Security Governance Council
- Penetration testing – pilot engagements
- Additional training based on risk & community needs
- Endpoint Detection & Response (EDR) tool rollout
  - Sentinel One (S1)
  - ITS already using Palo Alto Cortex – continue as is
- Active Directory “registration” and environment assessments
- ITS FortiAnalyzer
- In-process: Formalizing cyber risk management program
  - Patching, scanning, threat & vulnerability management, eliminating end-of-life hardware/software, self & external assessments, etc.
  - https://www.hawaii.edu/infosec/it-security-alerts/

S1 Stats

- 29 Departments/Campuses have registered for S1
- 22 have started deployment of the agent
- Total of 1197 agents registered in the new consoles
- 15 Departments/Campuses have protected their AD domain controllers
- Vulnerability Stats:
  - 176 Threats detected, 78% True positive threats were detected by full disk scan or agent policies
  - 3 Exploits were detected and mitigated
  - 736 Vulnerabilities detected, 46 Critical, 385 High with 1114 Vulnerable endpoints

Active Directory Assessments by Mandiant

- Conducted 6 training workshops – sessions were recorded
- Domain configuration review and recommendations
  - 24 submitted domains that were reviewed; 13 recommendations were provided to uplift privilege account protections, endpoint hardening, environment isolation and recovery preparations, and DC isolation and Active Directory Recovery protections

AD Assessments - continued

- **Critical Priority Recommendations**
  - AD-C-01: Review Domain Privileged Accounts in Built-in Groups
  - AD-C-02: Review and Mitigate Accounts with Non-Expiring Passwords
  - AD-C-03: Review and Mitigate Accounts with Password Not Required
- **High-Priority Recommendations**
  - AD-H-01: Upgrade the Forest and Domain Functional Level
  - AD-H-02: Review Non-Computer Accounts Configured with Service Principal Names (SPNs)
  - AD-H-03: Review Sensitive Accounts That Can Be Delegated
  - AD-H-04: Review Non-Computer Accounts Configured for Unconstrained Delegation
  - AD-H-06: Enhance Enforced Password Policies
  - AD-H-07: Implement CIS Hardening
  - AD-H-08: Enforce Logon Restrictions and Minimize the Exposure of Privileged Accounts
- **Medium Priority Recommendations**
  - AD-M-01: Review Accounts Assigned the “AdminSDHolder” Role – AKA: Legacy Admins
  - AD-M-02: Ensure KRBTGT rotate process
- **Low Priority Recommendations**
  - AD-L-01: Review Scope of Dormant Accounts

Compliance & Other Requirements

Google

- Email Requirements: DMARC/SPF enforcements (changes are coming)
  - https://www.proofpoint.com/us/blog/email-and-cloud-threats/google-and-yahoo-set-new-email-authentication-requirements
  - https://support.google.com/a/answer/81126?visit_id=638415676141377249-3898498670&rd=1#zippy=%2Crequirements-for-all-senders%2Crequirements-for-sending-or-more-messages-per-day
- Storage quota enforcement: January 29, 2024
  - https://www.hawaii.edu/askus/1882
  - Check your quota: https://drive.google.com/drive/quota

Payment Card Industry (PCI)

- UH Credit Card Program (AP 8.710)
- PCI DSS version 4.0 released Mar. 31, 2022 (64 new requirements but only 13 required now; remaining 51 are ”best practices” until Mar. 31, 2025)
- PCI DSS version 3.2.1 officially retired Mar. 31, 2024
- Self-Assessment Questionnaires (SAQ)
  - Every program with a UH Merchant ID is required to complete an SAQ annually for their “category” (e.g. SAQ A, SAQ B-IP, SAQ CVT, etc.)
  - Effective April 1, SAQ assessments will use PCI DSS 4.0

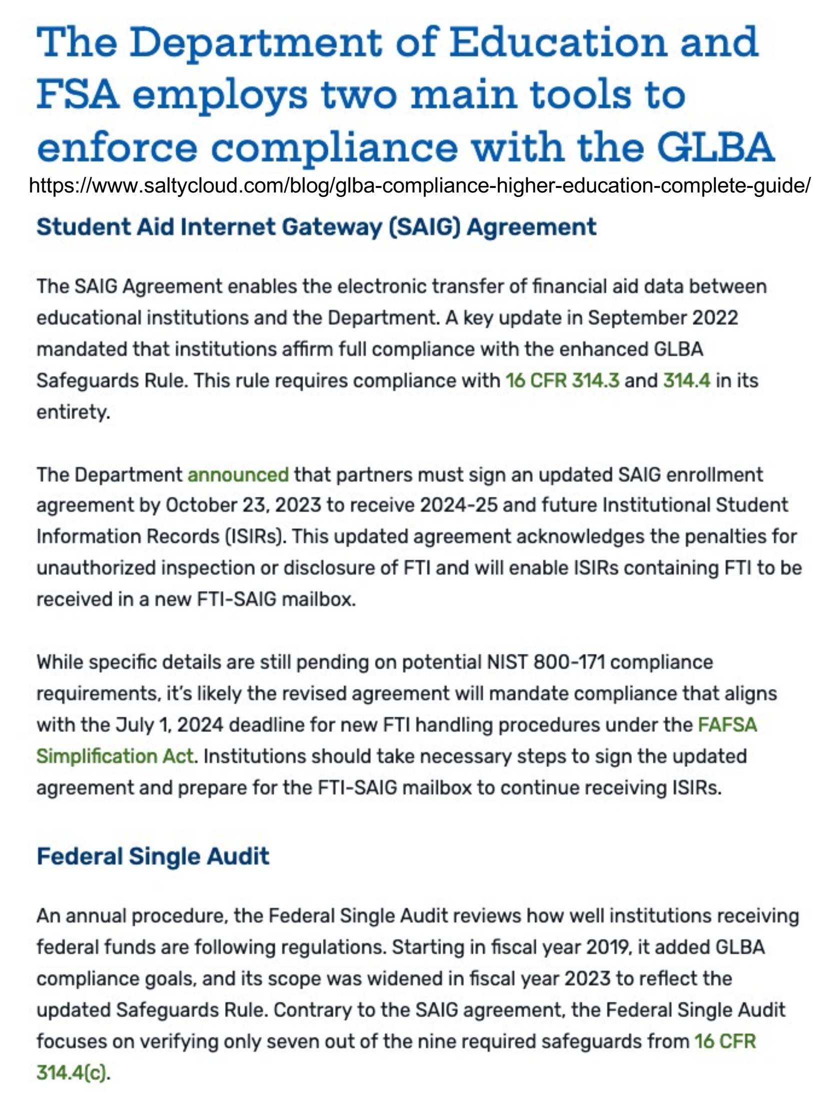
Cybersecurity Maturity Model Certification (CMMC)

- Dept. of Defense regulation
- Proposed Rule published 12/26/2023 – 60 day window for public comments
  - https://www.regulations.gov/docket/DOD-2023-OS-0063
- Expected that Final Rule will be published and in effect in early 2025
- 3 levels:
  - Level 1: 15 requirements very similar to Basic Safeguarding rule currently in effect: FAR 52.204-21; requires self-assessment
  - Level 2: 110 requirements aligned with NIST SP 800-171; some contracts will require 3rd party certification
  - Level 3: 110+ requirements – NIST SP 800-171, NIST SP 800-172; requires certification by government

FTC GLBA Safeguard Rule

- Federal Trade Commission Gramm-Leach-Bliley Act applies to UH because of the federal student financial aid program
- New security initiatives are required to comply with GLBA (e.g. MFA)
- Additional initiatives coming to formalize processes required by GLBA
  - Cyber risk management program
  - Vendor management program
- https://www.hawaii.edu/infosec/glba/

https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4



The Department of Education and FSA employs two main tools to enforce compliance with the GLBA

https://www.saltycloud.com/blog/glba-compliance-higher-education-complete-guide/

Student Aid Internet Gateway (SAIG) Agreement

The SAIG Agreement enables the electronic transfer of financial aid data between educational institutions and the Department. A key update in September 2022 mandated that institutions affirm full compliance with the enhanced GLBA Safeguards Rule. This rule requires compliance with 16 CFR 314.3 and 314.4 in its entirety.

The Department announced that partners must sign an updated SAIG enrollment agreement by October 23, 2023 to receive 2024-25 and future Institutional Student Information Records (ISIRs). This updated agreement acknowledges the penalties for unauthorized inspection or disclosure of FTI and will enable ISIRs containing FTI to be received in a new FTI-SAIG mailbox.

While specific details are still pending on potential NIST 800-171 compliance requirements, it's likely the revised agreement will mandate compliance that aligns with the July 1, 2024 deadline for new FTI handling procedures under the FAFSA Simplification Act. Institutions should take necessary steps to sign the updated agreement and prepare for the FTI-SAIG mailbox to continue receiving ISIRs.

Federal Single Audit

An annual procedure, the Federal Single Audit reviews how well institutions receiving federal funds are following regulations. Starting in fiscal year 2019, it added GLBA compliance goals, and its scope was widened in fiscal year 2023 to reflect the updated Safeguards Rule. Contrary to the SAIG agreement, the Federal Single Audit focuses on verifying only seven out of the nine required safeguards from 16 CFR 314.4(c).

National Security Presidential Memo (NSPM) 33

- Requires a certification from research organizations awarded in excess of $50 million per year in total Federal research funding that they have implemented a research security program
- Office of Research Compliance creating Research Security Program
- 4 elements
  - Cybersecurity*
  - Foreign travel security
  - Research security training
  - Export control training

*14 basic safeguarding protocols & procedures

Annual Personal Information Assessment

- State of HI Information Privacy & Security Council survey
- **[§487N-7] Personal information system; government agencies; annual report.** (a) Effective January 1, 2009, any government agency that maintains one or more personal information systems shall submit to the council an annual report on the existence and character of each personal information system added or eliminated since the agency's previous annual report. The annual report shall be submitted no later than September 30 of each year.
- https://www.hawaii.edu/its/information/survey/

Annual UH Device Registration

- As part of the University of Hawaiʻi's Information Security Program, all servers and endpoints (desktop/laptop) storing Regulated data operating on the UH network must be registered.
- https://www.hawaii.edu/its/device/registration/

Follow Basic Cyber Hygiene Principles!

https://www.hawaii.edu/infosec/minimum-standards/cyber-hygiene/

- Use anti-malware & host based firewalls
- Regularly update software
- Use multi-factor authentication
- Set strong passwords (and use different passwords)
- Use encryption
- Back up your data
- Lock your devices
- Limit the use of administrative accounts
- Recognize phishing
- Mobile device security
- IoT devices
- Scan your device for PII (personally identifiable information)

  https://www.hawaii.edu/askus/1297

Updates: ISAT, Records Retention, Privacy, and OVPIT Approval for IT Procurement

Sandra

What	ISAT Phase 2: Valid ISAT check upon login
Who	Personnel with access to selected enterprise wide information systems (i.e., those who work with Protected Data)
Where	Banner, STAR, KFS, PeopleSoft, myGRANT
When	Spring 2024 Announcements to UH community forthcoming
Why	Compliance with GLBA and AP2.215, increase awareness of cybersecurity risk

Records Retention Reduces Risk

- Changing culture takes time
  - Take the minimalist approach! Eliminate old files with Sensitive/Regulated data to reduce risk
  - Understand what files you don’t need to keep, what files you do need to keep and for how long
  - DGO/OGC can help analyze your records - contact Sandra (yano@hawaii.edu)
- Retention Schedules
  - State General Records Schedule (HR, fiscal)
  - EP 2.216, Institutional Records Management
    - Student records – Appendix I
    - Children’s Center records – Appendix II

Requests for Deletion of Data

- As concerns over privacy increases, we anticipate requests for deletion of personal data
- What is UH's obligation? Do we need to comply?
  - As of now, we are exempted from most privacy laws
  - GDPR data is a small subset
  - Starting to have system discussions
- Forward requests to Sandra (yano@hawaii.edu)

OVPIT Approval for IT Procurement

- EP8.200, Section III.B.f.(1)(b), Information Technology Purchases
- Nov 2023 update - causing confusion

  Purchases of electronic equipment, hardware, software, and related services:

  a) Proposed contracts (including purchase orders) relating to the purchase of electronic equipment, hardware, software, and/or related services that either exceeds $25,000 in the aggregate, whether it is over a single year or multiple years; or **NO CHANGE**

  b) Electronic equipment or hardware that will be connected to the UH network, regardless of the dollar value. This includes, but is not limited to, servers, desktop computers, laptops, printers, smart TVs, video cameras, or other Internet connected devices that has the potential to be remotely accessed. **IGNORE THIS**

- Planned spring 2024 revision - reverts back to 2020 version with clarification

  b) Electronic equipment or hardware or software that will be connected to, or is required to interact or integrate with the University's institutional data systems and requires technical assistance and/or support from Information Technology Services, or requires use or exchange of data from the University's institutional data systems, regardless of the dollar value.

Questions?

infosec@hawaii.edu

datagov@hawaii.edu