IT All-Campus Workshop 2019

Regulations, Compliance & Security: Oh my!

Jodi Ito
UH Chief Information Security Officer
jodi@hawaii.edu

Increased Regulatory & Compliance Oversight

- Federal agencies are concerned about data protection
- Department of Defense & federal agencies more involved especially around projects with DFARS 7012/CUI specified (NIST 800-171)
  - e.g. FBI, NCIS, AFOSI, DCSA, DHS
- Federal Student Aid @ US ED
  - Outsourced management of some of its information systems to General Dynamics IT (GDIT.com)
  - Recently sent letters from FSATech@GDIT.com to institutions requesting the institution's IP range and IT contact for FSA protection
- UH external audit will be looking at controls related to NIST 800-171 (student financial aid)
- UH Internal Audit reviewed PCI-DSS controls as part of its review of UH Cash Receipts Process

IT All-Campus Workshop 2019

Payment Card Industry – Data Security Standards

- UH Internal Audit recently reviewed UH policies & procedures for credit card handling and payment (PCI-DSS)
  - Updated policies and procedures are being implemented by UH Treasury
  - Affects any department taking credit card payments/issued a merchant code from the Treasury office
  - Units will have to follow a very prescriptive process; including vulnerability scanning and network architecture & infrastructure reviews to ensure compliance with PCI-DSS
- Also in play, GLBA (Graham-Leach-Bliley Act)
  - Affects any program that “acts like a financial institution”: student financial aid, One Card program, etc.
  - https://library.educause.edu/topics/policy-and-law/gramm-leach-bliley-act-glb-act

IT All-Campus Workshop 2019

DFARS 7012/CUI/NIST 800-171

- Defense Federal Acquisition Regulation – contract language for safeguarding covered defense information
- Alphabet soup
  - CUI: Controlled Unclassified Information
  - CTI: Controlled Technical Information
  - CDI: Covered Defense Information
- Information must be protected in compliance with NIST 800-171
  - 14 control families; 110 controls
- May also require an SSP (System Security Plan) & POAM (Plan of Action and Milestones)
- Oversight agency: Defense Counterintelligence and Security Agency (DCSA) was DSS (Defense Security Services)
- NOT EASY!

NIST 800-171 Compliance Checklist

(sample controls)

NIST 800-171 Control Number	Control Type	Control Family	Control Text	Response	Responsible Party: IT Operations, Security Custodian, and/or Data Custodian
3.1.1	Basic	Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Maintain list of authorized users defining their identity and associated role and sync with system, application and data layers. Account requests must be authorized before access is granted.	IT Operations, Data Custodian
3.1.2	Derived	Access Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Utilize access control lists (derived from 3.1.1) to limit access to applications and data based on role and/or identity. Log access as appropriate.	IT Operations, Data Custodian
3.1.3	Derived	Access Control	Control the flow of CUI in accordance with approved authorizations.	Provide architectual solutions to control the flow of system data. The solutions may include firewalls, proxies, encryption, and other security technologies.	IT Operations
3.1.4	Derived	Access Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	If a system user accesses data as well as maintains the system in someway, create separate accounts with approriate access levels to separate functions.	IT Operations
3.1.5	Derived	Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Only grant enough privileges to a system user to allow them to sufficiently fulfill their job duties. 3.1.4 references account separation.	IT Operations

IT All-Campus Workshop 2019

Research & Data Governance

- Sandra Furuto & Emi Morita: Q&A session next
- Need increased oversight of research projects
- ORS is involved in modifying research project process to ensure that Principal Investigators (PIs) understand what is involved when DFARS 7012 is in their project contract/award language
- RCUH is ensuring that purchases are reviewed for appropriate Terms & Conditions related to data security and privacy
- Infosec is involved in the review processes
- Fall Data Governance & Infosec Roadshows will have more details
- Infosec will be doing a separate roadshow for IT support staff specifically about IT implications for regulatory compliance

IT All-Campus Workshop 2019

”Other” Category

- Preservation of information: investigation or termination
  - Involve UH Infosec early; provide guidance on what can be done
  - Ensure that the subject of the investigation does not have access to computers/accounts after notification
- Applications integrated with UH information systems accessing regulated data (data feeds, one-time push of data, etc.)
  - Will require data flow diagram and network architecture
- Contracts with 3rd party vendors
  - Example: Graduation Alliance for college planning & applications
- TWITCH! (live streaming, revenue generating activity)
  - On campus, violating UH policies & procedures

IT All-Campus Workshop 2019

“Human” Security Events

- Using SSN + full date of birth to authenticate
- Not changing the default password (and being surprised when the machine or device is compromised)
  - Includes sensors, IoT devices, raspberry Pi
- The account and password is the SAME (attacker got in – two tries)
- SSNs (and other sensitive information) being kept when not needed and is **NOT ENCRYPTED**
- SSNs displayed in envelope window

IT All-Campus Workshop 2019

Attacks on UH Network

- Attempts to Upload PhotoMiner Malware via FTP
- Possible APT activity to use UH webservers as Proxies
- Brute Force SSH Login Attempts
- Attempts to upload malicious script to UH webservers
- Large Outbound Transfers to China
- Successful RDP attacks
- Continued spear phishing attacks impersonating UH administrators

IT All-Campus Workshop 2019

Increased Security Measures

- Blocking inbound RDP at the UH network border
- Increased network & vulnerability scanning
- Increased network blocking
  - Adding threat feeds
- Additional endpoint monitoring where required
- Network re-architecting based on compliance requirements
- Look for additional training sessions: NIST 800-171, PCI, Research, Student Information (FSA)

IT All-Campus Workshop 2019

Best Ways to Secure Computers & Information

- Establish good “cyber hygiene” practices
- Know your assets; know where your sensitive data resides
- Apply operating system and application updates frequently and regularly
- Install and update anti-virus software
- Scan your computer for sensitive information
- Securely delete any sensitive information that is no longer needed
- Encrypt the sensitive information that is required to be maintained for business operations purposes
- www.hawaii.edu/infosec/techguidelines

IT All-Campus Workshop 2019

Best Practices - continued

- Practice good password management;
  - Use multi-factor authentication (Duo at UH)
  - Use STRONG passwords
  - All computers should have login credentials
- Disable remote logins (unless absolutely necessary)
- Back up your data regularly
- Use email & the Internet safely; be careful when clicking on attachments or links in email
- Monitor your accounts for suspicious activity

IT All-Campus Workshop 2019

“Bring It On”: Q&A Session

Sandra Furuto, Data Governance Director
Jodi Ito, Chief Information Security Officer
Emi Morita, Associate General Counsel