Information Security

Larry Suto, CISSP
CISO CCC Technology Center

Takeaways

- General Concepts
- Know the Law
- Best Practices

Why Information Security?

•By the Numbers

- 36,000 – Number of compromised records from California Community colleges this year. Riverside City college and College of the Desert.
- 5.5 Million average cost of data breach according to Ponemon Institute Cost of a Data Breach study
- $194 cost on average per compromised record according to Ponemon Institute Cost of a Data Breach study
- $17.1 million cost so far of Maracopa Community College data breach in Arizona, not yet counting cost of resulting law suits

Data and Disclosure Laws Impacting Educational Institutions

- Family Educational Rights and Privacy Act (FERPA) for Educational Institutions
- Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
- Gramm-Leach-Bliley
- Payment Card Industry Data Security Standards (PCI-DSS)
- State Privacy Laws for Student, Medical and Consumer Records

FERPA – Access to Student Information

- Compliance required by schools receiving funds from any U.S. Department of Education program
- Requires written consent from student/parent to release any protected student information
  - Exception Applicable to Technology Vendors
    - Disclosure to other school officials with a legitimate educational interest
    - Vendor must have a legitimate reason for access and is accessing as a “school official”
    - Technology contract must reflect this and make vendor responsible for the data to the same extent as the institution

HIPAA –Access to Medical Information

- Privacy Regulations – govern use and disclosure of “protected health information” of covered entities and their business associates
- If medical information is involved, need to determine if the institution is a covered entity for HIPAA purposes
- If institution is a “covered entity,” then vendors must become business associates prior to institution allowing access to HIPAA protected data
- If medical information is involved, check with your legal counsel regarding HIPAA applicability

Gramm-Leach-Bliley Act and NIST 800-171

- Department of Education has starting sending out audit notification letters.
- The Department of Education updated their audit guidelines in July 2016 and greatly expanded the emphasis on Information Security
- Institutes of Higher Ed are considered Financial Institutions and must meet all of the requirements in GLBA

Section 501 of GLB Act

- Each agency or authority..., shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical ·safeguards –
  - (1) to ensure the security and confidentiality of customer records and information;
  - (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
  - (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

GLBA Conclusion

- The next time your Financial Aid Department is audited NIST 800-171 will be used.
- Act now to start implementing it
- If you have a security incident it must be reported the day it is discovered to the Department of Education

NIST 800-171

- Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  - 14 Families of Controls
  - 149 total Security Controls
  - Maps easily to CIS Critical Controls
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

Other State Laws

- Constitution, consumer protection statutes
- California is a leader in passing such laws
  - California privacy laws
  - Breach notification laws
    - Requires prompt notification if certain unencrypted personal information is compromised
    - If vendors control this type of data, they must comply with this law
  - Electronic signature laws

Department of Education Requirements

- Develop, Implement, and maintain a comprehensive information security program
- Designate employee(s) to coordinate the college's information security program
- Identify foreseeable internal and external risks to the security, confidentiality, and integrity of customer information
- Design and implement safeguards to control the risks the college has identified
- Oversee that third party service providers are also maintain appropriate security controls

Department of Education Requirements

- Colleges must report any suspected or actual data breaches to cpssaig@ed.gov
- Report must be submitted on the day the suspected breach is discovered
- The Department of Education has the authority to fine institutions that do not comply with the requirement to self-report data breaches. Such fines may be imposed up to $54,789 per violation per 34 C.F .R. § 36.2.

Department of Education Requirements

- In July 2016, the Department published another Dear Colleague Letter, GEN-16-12, the Department advised institutions that they should be using (NIST SP 800-171)
- NIST SP 800-171 focuses on protecting the confidentiality of private data in non-federal information systems and recommends security requirements to achieve that objective.

General Data Protection Regulation (GDPR)

- EU Privacy law goes into effect May 25th, 2018
- Much stricter than FERPA or California State Privacy laws
- Applies to entities with no physical presence in the EU
- EU could refuse student visa for non-compliant institutions
- Will need your campus general counsel to determine if GDPR is applicable.
- UC and Cal State Systems are currently contemplating what changes if any are needed to be in compliance and are making plans to become compliant.
- https://er.educause.edu/articles/2017/8/the-general-data-protection-regulation-explained

Data Security

- Where and How is the PII Maintained?
- What is “Reasonable”?
- Prevention, Detection, Correction
- Administrative, Technical, Physical

Three Basic Document Categories

Permanent Records (Class 1)

- Must be retained “indefinitely” (5 C.C.R. § 59023).
  - (e.g., employee records, student records, annual reports, etc.)

Optional Records (Class 2)

- Retained until reclassified as “Class 3 – Disposable” (5 C.C.R. § 59024).
- “Catch-all” designation for records that the district wishes to retain, but are neither permanent nor disposable.

Disposable Records (Class 3)

- Must be retained for three (3) years, or any other applicable retention period (5 C.C.R. § 59025).
- Includes records basic to audit (attendance, business and financial transactions, etc.) and periodic reports.

Document Retention Policy ***

Document or Record	Retention Period
Board Minutes	Permanent
Construction Pay Estimates, etc.	Completion of Projects Plus 10 Years
Litigation and Claims	Closure Plus 10 Years
Official Budget	Permanent
Payroll Records	7 Years
Personnel Records	Termination Plus 7 Years
Real Property Records	Permanent
Student Discipline Records, Other than Expulsion	Enrollment Plus 1 Year
Student Health Information	Enrollment Plus 5 Years
Student Transcripts	Permanent

***This is a mock example *Document Retention Policy*
and should not be relied upon for actual document retention purposes***

CCC Tech Center Services

- Data Inventory and Monitoring Tools
- SSL Certificates
- Logging/Monitoring-Splunk
- Security Awareness Training
- Phishing Services
- Vulnerability Assessments

Spirion DLP

- Data Inventory and Monitoring
  - Find your sensitive information a
  - Has clients for Windows, OS X, and Linux
  - Has central console server for reporting
  - Have 16 Districts signed up

InCommon

- Federated Identity
- Unlimited SSL Certificates
  - SSL/TLS Certificates
  - Extended Validation (EV) Certificates
  - Client (Personal) Certificates
  - Code Signing Certificates
  - IGTF Server Certificates

Splunk Core

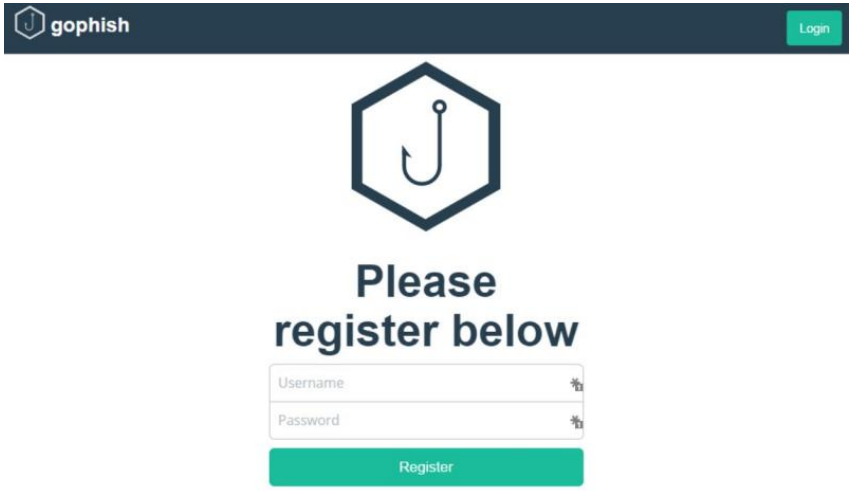
- Central logging system
  - Each College get 10 gigs per day
  - Centrally log all of your security information
  - Active Directory Security, firewall, IDS, Linux auditd, WAF, etc
  - Splunk apps for visualizing data

Security Awareness Training

- SANS Securing the Human
  - Can be customized for your users.
  - Meant for non-technical users.
  - Certification of completion when finished.

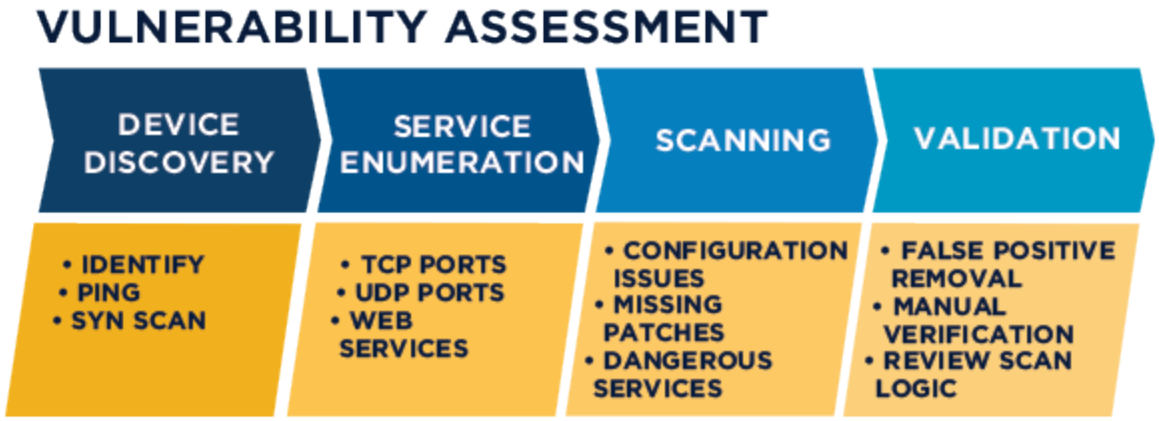
Phishing Assessments

- GoPhish Open Source Phishing Toolkit
- Campaigns, metrics, reports
- Clone websites, create templates
- Collect Passwords



Vulnerability Assessments

- Full inside Vulnerability scan
- Penetration Testing
- Report
- Remediation steps



CCC Information Security Standard

- Developed and approved by Systemwide Architecture Committee
- Reviewed by Gartner
- Reviewed by Information Security Advisory Committee
- Review by Chief Information's Systems Officers Association
- Review by the CC League of California, and now referenced in AP 3720

Existing Policies in Place

- Acceptable Use Policy – AP/BP 3720
- Student Records, Directory Information, and Privacy – AP/BP 5040
- CCLC board docs are minimum legally required.
- Need to raise the IT Information Security bar.

AR document templates

- Acceptable Use
- Change control
- Social Media
- Data Classification
- Physical Security
- Logging
- Others

Breach, Response Plan and Best Practices

Responding to a Breach

1. Investigate immediately
2. Notify and consult with counsel

   Consider contacting law enforcement
4. Consider consultants (IT, PR, Forensics, Security)

Breach, Response Plan and Best Practices

Responding to a Breach - continued

5. Is notification required and, if so, to whom?
6. Have clear communication strategies

   Determine insurance coverage and tender as appropriate

8. Learn from the incident

Questions

- lsuto@ccctechcenter.org
- cccsecuritycenter.org