Santa Rosa Junior College

Initial Security Assessment

Kevin Snyder, Network Security Manager

Who am I?

- SRJC Alumni – AA 1983
- 28 years at State Compensation Insurance Fund
  - 19 Years in IT
  - CISSP since 2007
  - 15 Years in Security
    - Operations (Firewalls, VPN, Web Filtering, Proxy Servers, Secure File Transfer, network)
    - Policy (reviewing and updating security policies)
    - Threat Vulnerability Management (patch processes, risk assessments)

Since I started working here (July 16), the following companies have had data breaches…

- Port of San Diego
- **Facebook**
- **British Airways**
- Huazhu Group (500 Million records)
- **T-Mobile**
- Air Canada
- Sitter.com
- Cheddar's Scratch Kitchen
- **Eastern Maine Community College (42,000 records x $140/record = $5.9m)**
- U.S. State Department email system
- Adams County, Wisconsin
- Comcast Xfinity (26.5 Million records)
- Chegg.com (4 Million records, higher ed-related)
- SheIn (fashion retailer, 6.4 Million records)
- Apollo (Sales Engagement) – 200 Million contact records
- United Nations
- Newegg.com
- Government Payment Service Inc. (GovPayNow)
- FreshMenu.com
- Burgerville

Why are Colleges such attractive targets?

- Per https://www.ccdaily.com/2018/09/cyber-attacks-rise-colleges/, from Community College Daily (Amer. Assoc. Of Comm. Colleges)
- "A stolen credit card is worth about 25 cents, …, but a stolen student record from a college – containing a name, address, bank account, past work record and data on everything submitted to the registration office, can fetch $2,000."
- HIPAA-compliant student data is also very valuable on the dark web!
- **Criminals go where the money is…**

Summary/mandate

- Recommend/implement improvements
  - Awareness training (best bang for the buck)
  - Processes
  - Policies
  - Technologies (we need some, leverage what we already have even more)
- Impact/risks of hack
  - Students - Loss of Personal info (PII), payment card info (PCI), identity theft.
  - Faculty/Staff – Loss of Personal info, identity theft
  - College – possibly millions of dollars to fix/secure data, purchase of credit checks for all affected, triage (may need consultants), **loss of reputation and loss of enrollment.**

Where are we now?

- The SRJC IT department has made tremendous strides with technical security:
  - Modern Firewall (Palo Alto) at perimeter
  - Cloud-based email/spam filter (Barracuda)
  - Few older devices with outdated Operating Systems
  - Cloud-based apps (Canvas, etc.)
  - Frequent, rapid-response server patching (Critical patches)
  - Frequent workstation patching
  - PCI (successful attestation) compliance
  - IT (Help Desk in particular) is well thought-of

Where are we now? (cont.)

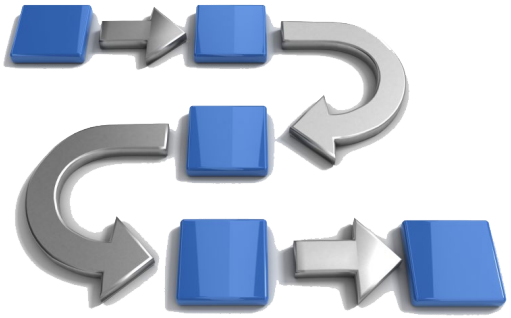
- Firewalls (Palo Alto) – 8 (out of 10)
  - Modern Firewalls, but not used to full potential
    - No east/west visibility, no IoT visibility
    - Can do some Data Loss Prevention (GDPR requirement)
    - Still refining Web Filtering
- Email Filtering (Barracuda) – 8/10
  - Cloud application, not used to full potential
    - Limited use/understanding of Quarantine function
    - Has Data Loss Prevention capability, not used currently (on roadmap)

Where are we now? (cont.)

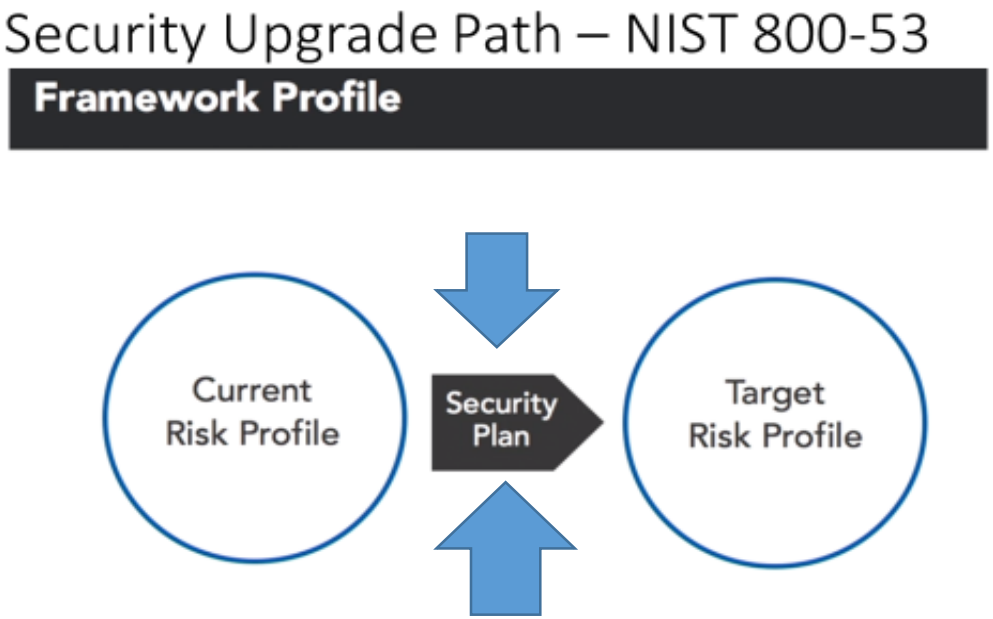
- Security awareness – 5/10
  - There is training at PDAs and Quarterly new hire orientation
  - I am sending a monthly Security Newsletter
  - No regular reminders of phishing and other threats to all employees
  - No phishing testing, no way to track progress/improvement
  - Awareness training is inexpensive, and has a lot of benefit
- Security Policies – 4/10
  - We have an Acceptable Use policy, but that's about it for security
  - Some processes for Disaster Recovery, Business Continuity, Incident Response Policies –
  - DR - Firewall in Petaluma failed, seamlessly failed traffic to Santa Rosa, but need to continue to improve, consider alignment with Emergency Response.
  - Approved policies create an environment for best practice processes

Where are we now? (cont.)

- Processes/Procedures 5/10
  - We have Wikis, some knowledge base in Sharepoint, some in Service Desk +
  - Inconsistent, partial documentation
  - Insufficient process and documentation for DR/BCP, Change Control, etc.



Where do we go from here?
What's the plan?

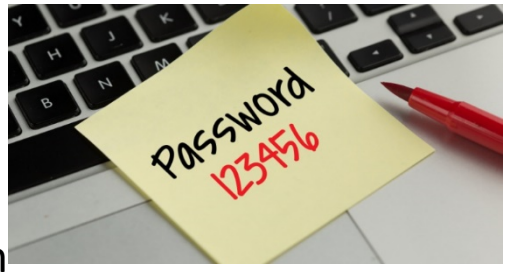


Awareness Training!

- Monthly Newsletter (already started)
- New Hire Orientation (some already in Quarterly O
  - Working with HR to expand to annual Faculty/Staff training
  - Getting Awareness training modules from CCCTech
    - Adding training modules to NeoGov (via HR collaboration)
  - PDA sessions (2 separate training sessions at next PDA!)
- **Phishing tests**
  - We already have software to simulate phishing emails
  - We can track results and progress
  - We can send back link click to a security video (for example)
- Awareness Training gets the best results for the money!

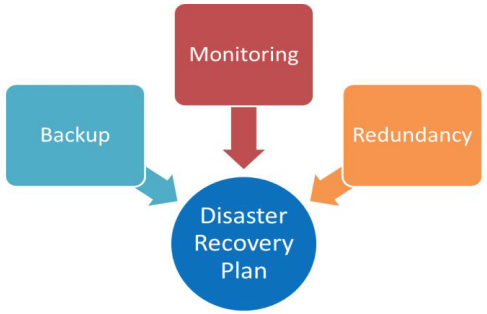
Some simpler things, some more complex…

- On the one hand –
  - Multifactor Authentication is coming, in certain scenarios
    - Gets us compliant with NIST (Federal funding), PCI, FERPA
    - Will be gradually rolled out
    - Still in discovery phase
    - Planned for next year



- On the other hand –
  - NIST has changed the password complexity paradigm
    - NO PASSWORD AUTO-EXPIRY!
    - Use of password strength meter, instead of a particular set of criteria
    - So yes, the passwords will likely be longer (passphrases, anyone?), but you will probably have the same password for a LONG TIME!

Disaster Recovery/Business Continuity, and Incident Response



- We need plans for each
  - Review our applications/systems for criticality
  - Review our infrastructure
  - Create processes to get downed systems up as soon a
  - TEST our failover regularly!
  - SLAs, written procedures needed
  - Protect systems, data, avoid **reputational damage, additional costs/fines.**
  - Just like Emergency Response, cyber response plans and testing are needed, including policies for quick hiring of consultants
- CIRT – work/notification flow, forensics, etc.

Compliance

- HIPAA
  - Medical data is very valuable on the dark web, co
- PCI
  - We were successful in our attestation last year, but as we expand our card sales, the bar for compliance also goes up.
    - Multifactor Auth will be critical
    - Protecting our PCI CDE with VLANs, Firewall rules, etc.
- FERPA/GDPR
  - Data Loss Prevention is a requirement for GDPR compliance.
  - We have some infrastructure we can leverage for this, need to implement
- NIST
  - In order to receive Federal funding, Colleges must be compliant
  - MultiFactor Auth, a complete DR/BCP plan, Cyber Incident Response needed

Technology

- PC Encryption
  - In testing phase now, workstations encrypted, on Windows 10
  - New, encrypted machines to gradually replace older workstations
  - BitLocker for Windows, FileVault for Macs
- VDI (Virtual Desktops)
  - Will start in Kiosks, select locations
  - Will scale up gradually, where most reasonable
  - Can be centrally secured and managed
  - Since the applications are on a central server, actual endpoint more secure
- Admin rights
  - We have a Help Desk to assist with application installation.
  - By funneling application installation through the Help Desk, we can monitor and secure our workstations better.

Internet of Things (IoT)

- Personal devices:
  - Cellphones, Amazon Echos, Bluetooth speake
- SRJC-owned devices:
  - HVAC controllers, Emergency phones, Electronic door openers (cardkey readers), Credit card readers, Security cameras (Mirai), **PRINTERS**!
- These devices often have little or no security built in – HVAC and other controllers are often installed and maintained by third parties, and the devices are usually not hardened at all.
- Consumer devices may or may not be secured/updated by owners
- Jamf may be of use for SRJC-owned Apple devices (iPhones)

Policies!

- Agreed-upon policies will make decisions faster and easier
  - Processes and procedures can map to policies (best practices)
  - Policy sources – CSU, CCCTech (Jeff Holden), Title V, NIST, and other sources.
  - Security policies will undergo several passes locally, so that we know how we can best implement them, given existing resources.
  - Policies for DR/BCP needed, for streamlining response in case of breach
    - Long Beach CC's recovery was more expensive, and took longer, because there were inadequate policies to cover response. President was our of town, no policies to give VP rock-solid authority to hire consultants.
  - **We need help and support from administration, to shepherd policy approval for DR/BCP and other facets of security.**

To sum up…

- We are doing a lot of things right!
- We lack organization and some documentation (policies and processes)
- We need to leverage what we already have, fully implement
- We need some new technology to be more secure and compliant
  - Multifactor Auth, Password Strength Meter, possibly a Password Manager
- Keep banging away at the awareness drum!
- Move towards a mature set of Security Policies
- Compliance with PCI/HIPAA/FERPA/GDPR/NIST will be a journey, but many steps/processes are common across most compliance bodies.