A General Review of Key Security Strategies

Disclaimers

- All content and comments are my own and may not reflect the views of the:
  - United States Government
  - United States Department of Justice (DOJ)
  - Federal Bureau of Investigation (FBI)
  - Any local or state agency
- No guarantees or warranties for completeness, omissions, misstatements or errors

Cyber Attacks

Biggest Cyber Hacks in 2017

- **Do you remember these…?**

What did we learn?

- Do the simple stuff
  - Asset Management
  - Secure Configuration & Patch Management
  - Vulnerability Assessment & Remediation
  - Admin Permissions/Least Privilege/Need to Know
  - Whitelist Applications & Malware Defenses
- Encryption can safeguard your data post exfiltration
- Most breaches are not technical issues…
  - **PEOPLE & PROCESS…**

Cost of Data Breach Calculator

The cost of a data breach differs for every organization. Use the calculator to explore how much would it could cost yours, then download the report to learn how average time to identify or average time to contain can save your bottom line.

Select location

- Global
- ASEAN
- Australia
- Brazil
- Canada
- France
- Germany
- India
- Italy
- Japan
- Middle East
- South Africa
- United Kingdom
- United States

Select an industry

- All
- Communications
- Consumer
- Education
- Energy
- Entertainment
- Financial
- Health
- Hospitality
- Industrial
- Life Science
- Media
- Public Sector
- Research
- Retail
- Services
- Technology
- Transportation

Select your cost factors

- [x] Incident response team
- [x] Extensive use of encryption
- [ ] Employee training
- [ ] BCM involvement
- [ ] Participation in threat sharing
- [x] Use of security analytics
- [ ] Extensive use of DLP
- [x] Data classification schema
- [ ] Insurance protection
- [ ] CISO appointed
- [ ] Board-level involvement
- [ ] CPO appointed
- [ ] Provision of ID protection
- [x] Consultants engaged
- [x] Rush to notify
- [x] Lost or stolen devices
- [ ] Extensive use of mobile platforms
- [ ] Compliance failures
- [ ] Extensive cloud migration
- [ ] Third party involvement

On average, public sector organizations in United States with the selected cost factors will incur the cost below for a data breach.

2018 - 2019 Predictions

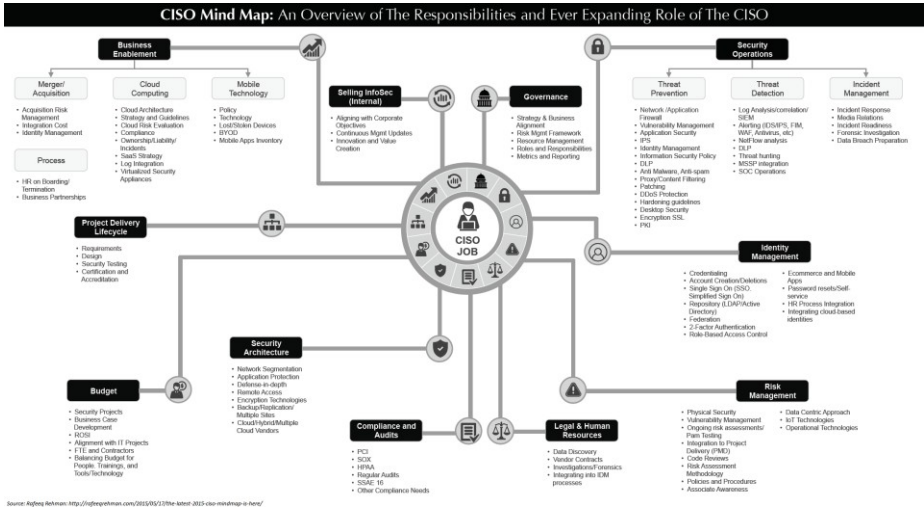
- Hacks will fall into one of three categories:
  - Profit = Extortion & Ransomware
  - Destruction = Data sabotage
  - Political Gain = Hacktivism & Terrorism
- Hackers will always go after the weakest link
  - Suppliers
  - Account Hijacking & Purchasing Credentials
- Attacks
  - Velocity is increasing
  - Sophistication is increasing
- Your users and suppliers will be breached…
  - What are their cyber postures?
- **You will be breached… eventually if you haven't already!**

Please, please, please… not on my watch!!!

- Every CIO and CISO in the world goes to bed at night like this…
- CIOs are not infallible
- CIOs cannot read your minds
- CIOs don't normally have close relationships with CEOs and Boards leading to a lack of communication and awareness
- **Are you concerned…?**
- **CIOs & CISOs need to be in the Board Room, understand the business, align and communicate the IT Strategy and establish relationships**

What is a Holistic Cyber Program?

- Stop buying expensive point solutions that don't integrate
- Know what's important
- Focus on People, Process & Technology
- Ensure your policies are up to date
- Leverage industry best practices
- Map and monitor process efficiencies
- **Prioritize your resources & investments**



CYBER
ESSENTIALS

For Personal

Personal Physical Security

- Lights at night and/or motion sensitive flood lights
- Cut your bushes so people can't hide behind them
- Lock your doors and windows (do a nightly check before bed)
- Have an alarm and monitoring service… and use it…
- Motion sensitive cameras sent to the cloud
- Get a dog
- How will you respond to an intruder?
- Practice drills – fire, intruder, etc…

Personal Identity Protection

- Identity protection service… (don’t forget your kids!)
- Wipe unused electronics (or better yet destroy them)
- Don’t give out info you don’t need to… ask why!
  - Limit information on checks… (e.g. R. Balzer, no address, etc…)
- Check privacy settings on social media (check often as they change)
- No paper statements (nothing to steal in the mail)
- Shred everything else…

Personal Financial Protection

- Get credit reports yearly and check them
- Consider blocking your credit with Experian, Equifax and TransUnion
- Pay bills at the Post Office or better yet online
- Cover when you ATM/pin
- Don’t sign Credit Cards – “Ask for ID or Photo ID”
- Shield your smartcard chips
- Have 1 credit card for recurring bills and 1 credit card that you take out of the house

Personal Technology Protection

- Keep your devices up to date and use security software
- Don’t click on links in email
- Use a password manager tool; never save passwords in your browser
- Use 2 factor authentication for everything that offers it
- Don’t let your devices out of your sight on travel
- Home Wifi – change the admin password, hide SSID, WPA2 encryption, Mac address filtering, offer Guest Wifi for friends
- Don’t use USB devices from others
- Only use your personal devices when a password is required to log into a website
  - Never use public computers (hotels, libraries, etc… for personal stuff)

For Work

- **The number of data breaches in the U.S. jumped 29 percent in the first half of this year**
- **63% of Data Breaches Result From Weak or Stolen Passwords**
- **The most glaring blind spot for organizations is how stolen credentials are the primary means by which hackers exploit their vital systems**
- **More than half of organizations attribute a security incident or data breach to a malicious or negligent employee**

Security Background Checks

- Do them! (Seriously)
  - Academic and Employment Verifications
  - Character Reference Check
  - Criminal, arrest, incarceration and sex offender background checks
  - Identity and Address Verification (typical I9 stuff)
  - Whether an applicant holds a directorship (conflicts of interest)
  - Credit History (remember the Fair Credit Reporting Act)
  - Litigation records (do they sue a lot)
  - Drug testing

Critical Security Controls (CSCs)

CSCs are my favorite industry standards but there are a number of global standards to choose from… of course, they are all pretty much the same

CSCs 1-5

- (1) Inventory of Authorized and Unauthorized Devices
  - Know every piece of gear on your network
- (2) Inventory of Authorized and Unauthorized Software
  - Whitelist all known good apps and disallow everything else
- (3) Secure Configurations for Hardware and Software
  - Use gold OS images, patch your OS's and applications and use a formal change management processes
- (4) Continuous Vulnerability Assessment and Remediation
  - Use a Security Content Automation Protocol (SCAP) validated scanner weekly; fix the issues that you find (https://scap.nist.gov/)
- (5) Controlled Use of Administrative Privileges
  - Least privilege and need to know; audit all use of credentials

CSCs 6-10

- (6) Maintenance, Monitoring, and Analysis of Audit Logs
  - Log everything, use a SIEM (security information and event management) or something to look for anomalies
- (7) Email and Web Browser Protections
  - Use spam and AV filtering, perform URL filtering, and lock down browsers
- (8) Malware Defenses
  - Use AV s/w, consider ETDR (Endpoint Threat Detection and Response)s/w, and lock down removable media
- (9) Limitation and Control of Network Ports
  - Minimize ports, protocols and services; use host-based firewalls
- (10) Data Recovery Capability
  - Back up critical data, move backups offsite, and actually test the recovery process/success rates

CSCs 11-15

- (11) Secure Configurations for Network Devices
  - Know all devices; keep them updated; use strict change management; 2 factor authentication for admins
- (12) Boundary Defense
  - Whitelist if possible but at least blacklist known bad IPs; Use firewalls & proxies; 2 factor authentication for remote users
- (13) Data Protection – One Drive
  - Know what data is important & encrypt it; encrypt laptops and mobile devices
- (14) Controlled Access Based on the Need to Know
  - Only allow people what they need (seriously)
- (15) Wireless Access Control
  - Hide SSID, WPA2 encryption, Mac address filtering (only known devices), offer Guest Wifi for visitors

CSCs 16-20

- (16) Account Monitoring and Control
  - Use an enterprise IDAM (Identity and Access Management) service or s/w; Use locking screen savers; Use 2 factor authentication – PASSWORDS!!!!
- (17) Security Skills Assessment and Appropriate Training to Fill Gaps
  - Training on hiring; training once per year using a service or tool; train your IT and InfoSec people via a yearly class and/or conference
- (18) Application Software Security
  - Update all 3rd party applications; use web application firewalls; test your applications; developers should not have production access; train your developers in secure coding (there are courses)
- (19) Incident Response and Management
  - Your going to be breached – HAVE A PLAN and test it!
- (20) Penetration Tests and Red Team Exercises
  - Consider hiring an outside firm to conduct pen testing; at least use vulnerability scanners with your staff

Wrap Up

- There's no way to teach cyber in one presentation.
- Hire a qualified CIO and CISO (make sure the CIO reports to the CEO)
- Have written policies and train/test your people on them
  - People are your weakest link so a awareness program is key…
- Pick a methodology (I like the CSCs) and create a strategy
- Mandate a way for proof that things are being done correctly
- Talk to the IT people at the bottom about their concerns and act to fix things
- **Plan for your breach…** What's your plan? Who's doing what? Who can make what decisions? Who's talking to legal/insurance/regulators? Do you have up to date contact info for everyone? How can issues be reported? Practice your plan…

Thank You & Q/A

Rick Balzer, President IntelesysOne
rbalzer@intelesysone.com
888-546-8353
www.intelesysone.com