Cybersecurity for Small Businesses

All about me...

Steven D. Pressman (steve@alpinecyber.com)

10 years with Lockheed Martin
    Staff Computer Systems Analyst

2 years with The SI Organization
    Chief Solutions Architect

Alpine Cyber Solutions
    President and Chief Solutions Architect

Certifications:

Certified Information Security Professional (CISSP)
GIAC Certified Enterprise Defender (GCED)
AWS Certified Developer – Associate
AWS Certified SysOps Administrator – Associate
AWS Certified Solutions Architect – Pro
AWS Certified Security – Specialty

Agenda

- Why do you Need Cybersecurity?
- What are some “Must Do” controls?
- What are some things you should do as you grow?
- Tips for Software Developers (if applicable)

Why do you Need Cybersecurity?

Breaches are Expensive

Why?

- Average breach in the US costs the victim $8.64M!
  - More if you're in Healthcare or Education
- Customer data is the biggest target
- SMBs (< 500 employees) are particularly under attack
  - Up 55% since 2016

* Source: 2019 Ponemon Institute Report

Customer Requirements

Why?

- Third Party Security Requirements are becoming more common
  - Questionnaires are “easy” if you are doing the right things
  - Vulnerability assessments are going to become more common
- Customers don’t want exposure in their supply chain
  - Risky engagements include:
    - Software vulnerabilities (i.e. NotPetya)
    - Customer Data Exposures (i.e. British Airways)
    - Direct Network Access (i.e. Target)
- Sometimes customers just want to know that their data

Regulatory Compliance

Why?

Some Regulatory Standards - Each carries its own rules and penalties:

- PCI DSS - Payment Card Industry Data Security Standard
- HIPAA (not HIPPA) - Health Insurance Portability and Accountability Act
- CIPA - Children's Internet Protection Act
- FERPA - Family Education Rights and Privacy Act
- GLBA - Gramm Leach Bliley Act [applicable to Title IV participating institutions]
- GDPR - Not security, but privacy. For anyone doing business with Europeans
- And many many more...

What are some “Must Do” controls?

Encrypt

- Don’t deliver to customers in clear text
  - Use encrypted email
  - Use third party encrypted storage (i.e. ShareFile, Google Drive, etc.)
- Don’t store customer or employee data in clear text
  - Encrypt all systems at rest and in transit
  - Watch for where you’re storing reports and extracts
- Don’t send passwords or customer data inside your team without encrypting
  - Slack and Teams are not safe on their own
  - Share credentials in a secure password vault (i.e. Dashlane, Lastpass, etc.)
  - Share sensitive data with GPG encryption (NOT HARD)

Educate

- Humans are your biggest exposure
  - Mistakes in data handling
  - Misconfigurations of systems
  - Malicious insider events
- Train your people on the risks
- Do it regularly
- Easiest path is a “show me” method -- Phishing attacks
  - Good phishing programs are regular (i.e. at least monthly)
  - Good phishing platforms will train users as well -- not just “catch them”

Use the Cloud (SaaS)

- Enterprise capabilities are at your fingertips, for reasonable monthly prices
- Comprehend your risk
  - Read the EULA
  - Watch the news - with a dose of logical skepticism
- Examples
  - Mail/Productivity (i.e. Microsoft 365, G Suite)
  - Accounting (i.e. Quickbooks, Wave)
  - Payroll/HR (i.e. ADP, Paylocity, Bamboo, Workday)
  - Collaboration (i.e. Slack, Microsoft Teams)
  - Tools (i.e. LucidChart, Jira/Confluence, DocuSign)

Use the Cloud (PaaS/IaaS)

Must Do

- Platforms and Infrastructure may be critical to your business - or not
- Comprehend your risk as always
  - Remember - misconfiguration is rampant in this space
- Be cautious when implementing -- get help if you need it
  - User groups FTW (shameless plug)
- Secure all of your environments (even dev)
- Examples
  - AWS
  - Azure

Secure your Access

- Use a company-wide password vault system (i.e. Dashlane, Lastpass)
- Minimize passwords and mistakes by centralizing your identity store (i.e. Microsoft Azure AD, G Suite, AWS SSO)
- Enforce multi-factor authentication whenever possible
- Maintain a solid offboarding process to avoid stragglers

End User Computing

- Depending on the type of business, this can be extremely challenging
- Always secure your endpoints
  - Anti-virus at a minimum (consider next-gen capabilities as you grow)
  - Encrypt your hard drives (yeah, again)
  - Implement config control where possible (i.e. JAMF, Intune)
  - Consider less-than-admin permissions...
- Three different paradigms:
  - Company Laptops
  - BYO
  - Virtual Desktops

EUC - Company Laptops

Must Do

- **Pros**
  - Independence for employees to bring their work with them
  - Sense of investment in the employee
  - Able to control the asset
- **Cons**
  - Expense
  - Theft
  - Misuse
  - Your data and your customers’ data are physically out of your control

EUC - BYO

Must Do

- **Pros**
  - Independence for employees to bring their work with them
  - Expense avoided
- **Cons**
  - Unable to control the asset or the data on it
  - Theft
  - Misuse - are you even allowed to call it that?
  - Your data and your customers' data are physically out of your control

EUC - Virtual Desktops

Must Do

- **Pros**
  - Your data and your customers' data never leaves the data center
  - Mostly ubiquitous access
  - No physical asset to control
  - Nothing to steal
  - Misuse is very unlikely
- **Cons**
  - Possible access/connectivity issues at customer locations
  - Expense, if not properly controlled
- **Options** - Amazon Workspaces, Citrix

Mobile

Must Do

- Business decision as to whether to provide phones/tablets to employees
- Either way, if customer data can be on employee (or contractor) devices, consider MDM
  - Rescind customer data from devices
  - Enforce encryption/passcode/screen lock
- Don’t overdo it
  - Overly draconian controls rarely work, and people tend to rebel

Patching

Must Do

- Most important thing you can do for free
- Put it on your calendar
- Includes:
  - End user devices
  - Servers
  - Mobile devices
  - Networking equipment
  - IoT devices

Policies

Must Do

- Nobody wants to do it, but the bigger you grow, the more important it becomes
- Defines the whats, hows, and whys of all of the recommendations in this presentation
- Address all of the following categories (ref: NIST 800-171)

Access Control	Media Protection
Awareness & Training	Personnel Security
Audit & Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification & Authentication	Security Assessment
Incident Response	System & Communication Protection
Maintenance	System & Info Integrity

Policy (cont'd)

Must Do

- Not all of the NIST sections need a huge amount of detail
- Distill the "most important" or actionable pieces into an Acceptable Use Policy (AUP)
- Record employee/contractor acknowledgement of the policies - just in case
- Cover your actual business practices (i.e. Practice what you Preach)
- Ensure all employees have read the policy
- Spot-check to ensure compliance
- Review the policies regularly (at least annually) to ensure they're still applicable

- Note: This is not the fun part! But this is the basic underpinning of all cybersecurity, and will make you a hero to your customers

What are some things
you should do as you grow?

Assess

Should Do

- Get another set of eyes on your security practices and data exposures
- Your “IT Guy” is usually the wrong person to do this
  - Nobody wants their mistakes exposed
  - Most IT professional (especially MSPs) have a very flimsy grasp on actual risk
    - I hate generalizations, but this has proven true too frequently
- Find someone who knows the systems you use, and can identify those risks
- Do this at least every year or two

SIEM

- Not in scope for a lot of small businesses
- As you grow, you will have more systems
  - Aggregate security data
  - Pull from cloud system sources, too
    - Microsoft Security Center
    - Cloud system logs (i.e. CloudTrail, CloudWatch)
- Visibility to your risks is beyond valuable

Summary

Summary

- Security is not optional - there are catastrophic risks to ignoring it
- Start with the policies, and build from there
- Think before you implement
  - Weigh risk vs reward for anything you implement
  - Pay special attention to those things that expose customer information
- You cannot do it alone. Do what you do well, and outsource the rest
  - User Groups
  - Vendors/MSSPs

ALPINE CYBER

Managed Security, Cloud & IT Services

www.alpinecyber.com

meetup.com/gpawsug

berks.psu.edu/fundamentals-cybersecurity
abington.psu.edu/ce-business-it/cybersecurity-fundamentals

Backup Slides

Software Development Concerns

If you have a software product...

- Scan code every commit with a SAST (i.e. Checkmarx, Veracode)
- Scan deployed servers/environments monthly with a vulnerability scanner
- Consider a penetration test every release
    - New code means new possible exposure
- Prioritize security workoff in every sprint
    - All “Medium” or higher findings should be worked as a top priority
- Encrypt all the things
- Keep security a priority