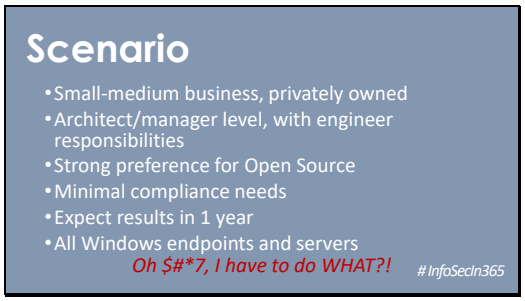
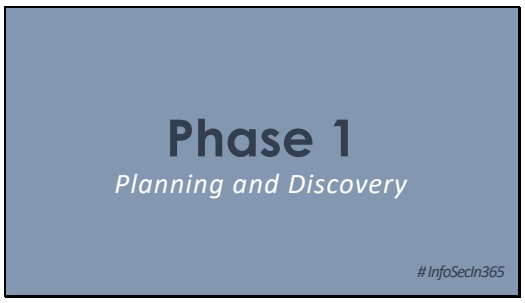
Slide 1

Slide 2



Slide 3



Slide 4

Framework

- Pick a framework
  - ISO 27000 *($)*
  - NIST CSF
  - CIS Controls (formerly SANS Top 20)
- Compliance needs will substitute for framework
- Use as basis for System Security Plan

 # InfoSecIn365

Slide 5

Resource Assessment

Do I start buying things now?

- Financial
- IT Infrastructure
- Technical resources
  - Determine who you can "borrow"
- Organizational OSINT
- Meet and greet

 # InfoSecIn365

Slide 6

Business Objectives

- Risk Assessment
- Business Impact Assessment
- Evaluate Disaster Recovery capabilities
  - DR simulation
  - RTO/RPO/WRT
- Data Classification
  - Keyword searches
  - Metadata tags
  - Department-by-department

 # InfoSecIn365

Slide 7

Evaluate User Education

- Phishing Simulation
  - Knowbe4 *($)*
  - PhishMe *($)*
  - SANS Securing the Human
- Surveys/Quizzes
  - StaySafeOnline.Org
- Use results for targeted user training

 # InfoSecIn365

Slide 8

Asset Discovery

- Hardware
- Software
- Tools
  - NMAP
  - Vulnerability Assessment System (VAS)
  - Active Directory
  - Microsoft Baseline Configuration Analyzer

 # InfoSecIn365

Slide 9

Threat Modeling

- Know what you're protecting
- Know what you're protecting against
- Intel sources:
  - US-Cert lookup for similar companies
  - CISO roundtables (avoid FUD)
  - Conferences/meetups (avoid FUD)
  - Forensics in your network + incident reports

 # InfoSecIn365

Slide 10

Gap Analysis

- Use framework
- Doesn't need to be with an auditor
- Deliverables
  - Compliance checklist against framework
  - Project plan/POA&M

A pen test IS NOT a Gap Analysis

 # InfoSecIn365

Slide 11

REST!!!!

- "Exhaustion is what our culture views as courage"
- Set goals, then reduce them by 25%
- Don't overcommit
- Try not to take work home
- Take your vacation time

 # InfoSecIn365

Slide 12

Talk with Management

- Avoid FUD
- Present findings
- Discuss potential costs / resource issues
- Increase buy-in
- Pitch security as a sales tactic

 # InfoSecIn365

Slide 13

Phase 2

Analysis and Documentation

#InfoSecIn365

Slide 14

Vulnerability Assessment

Do I start buying things now?

- Implement prior to patching to show reduction in vulns from patching
- OpenVAS
  - VulnWhisperer (ELK)
- Generate differential reports
- Shodan lookup for external ports
  - (should be able to see from your firewall rules)

#InfoSecIn365

Slide 15

Patching

- Automated for endpoints, manual for servers
- Gather team from IT for server patching
- WSUS can be high-maintenance if you don't have experience
- Every MS(S)P will have a patching software
- Placed right after Vulnerability Assessment so you can document the results

#InfoSecIn365

Slide 16

Widespread User Education

- StaySafeOnline.org
- SANS Securing the Human
- Security Policies
  - SANS
  - Charles Cresson *($)*

 # InfoSecIn365

Slide 17

Incident Response Prep

- Policies/procedures
- Breach Reporting
  - At what point
  - Compliance requirements?
- Establish CERT Team
  - Legal/HR/PR/Management/Infosec/IT

 # InfoSecIn365

Slide 18

Change Management

- Not necessarily your job…but it will be if it doesn't happen
- Even track changes that you don't think require approvals
- Tools
  - Excel
  - Intranet/SharePoint
  - Google Form
  - Helpdesk

 # InfoSecIn365

Slide 19

Talk with Management

- CIS 1-3,10,17,19 partially implemented by this point
  - Not all sub controls
- Incorporate some training
- Get feedback on user pain
- Review security policies, get approval

#InfoSecIn365

Slide 20

Do I start buying things now?

Phase 3

Mitigation and Remediation

#InfoSecIn365

Slide 21

Least Privilege

- Discovery
  - PowerShell
  - Talk to people
  - Bloodhound
- AD Admin Delegation
- ProcMon for removing Local Admin
- Reduction of privileged AD accounts

#InfoSecIn365

Slide 22

Easy Wins

- Firewall rule closures
- Session lockout
- Pre-logon advisory
- Add encryption into PC build checklist
- Account Auditing
  - Based on last logon
  - Work with HR

 # InfoSecIn365

Slide 23

Replacement/Renewals

- Good chance to increase security with easy wins
- NGAV
  - Does more than just AV, not much more $
  - "Poorman's App Whitelisting", Removable Media Control
  - Bit of an upfront effort
- Network refresh
- WAPs with RADIUS

 # InfoSecIn365

Slide 24

(Maybe)

- Change service account and admin passwords
  - (very important, but very time consuming)
- Principle of least Functionality / Hardening
- SIEM
- (N/H)I(D/P)S
- LAPS

 # InfoSecIn365

Slide 25

Talk with Management

- Reiterate that just because little to no money has been spent, not the expectation going forward
- Get input on potential budget $ and priorities
- Revisit MSSP for SOC

#InfoSecIn365

Slide 26

Phase 4

Looking Forward

#InfoSecIn365

Slide 27

Measure Progress

- Distribute survey
  - Measure user pain/perceived improvements
  - Allow Suggestions
  - Self Assessment
- Differential reports
  - Perform another Gap analysis
  - Vulnerability Scan
  - Redistribute survey from beginning to measure improvement in user awareness

#InfoSecIn365

Slide 28

Budget Preparation

- Set Priorities based upon findings in last slide
- Re-evaluate threat model, risk assessment
- Suggestions
  - MFA
  - Network overhaul (chances are you have a flat network with L2 switches)
  - Suggestions from Renewals/Replacements

 # InfoSecIn365

Slide 29

Talk with Management

- Present Budget
- Infosec as profit center
- Present % compliance improvement goals
- Present differential reports
- Explain advanced concepts

 # InfoSecIn365

Slide 30

tl;dr

(too long; didn't read)

 # InfoSecIn365

Slide 31

tl;dr

- Set priorities based upon business objectives
- Threat model all the things
- Discover all the things
- Educate all the users
- Backup all the things
- (Don't necessarily) open source all the things
- Buy all the things … eventually

#InfoSecIn365

Slide 32

Oh $#*7
I have to do WHAT?!
365 days to build a security program

@HomeBrewedSec
#InfoSecIn365