CISO 90 Day Plan

Nelson Chen, M.SC. IT
CISSP, CISA, CISM
Agenda

- Why are we here?
- Days 0 – 30
- Days 31 – 60
- Days 61 – 90
- Days 90+
- Infinity & Beyond
Avoiding Really Bad News!

<Your Company Name Here>
Data Breach!
Don’t be the Blocker!

MAYBE
Don’t be the Prophet of Doom
Toughest Part of the Job
CISO Post-Breach
Establishing Relationships & Trust
Selling CISO as a Service

- Business enablement
- FUD is not the only pitch
- Education
- Shared responsibility
- Get support and buy-in
- Add Value!
Taking Initial Inventory

• Organizational Structure - Who’s who
  – Execs, BU Leaders, IT Ops, Internal Audit
• Existing Policies, Processes, etc.
• Existing Technologies
• Where’s the Data?
• Historical Security Incidents
• Shadow IT
Leading Towards Better Security
Servant Leadership

Find yourself in the service of others

- Mohandas Gandhi
Security Surrounds us, Penetrates us and Binds us Together
Prioritizing & Project Kickoff
Back to Basics - CIA Triad

Keeping it secret
Keeping it together
Keeping it up

Central Oregon Community College
Fox-in or Fox-out?

Meet the new head of security.
Team or Committee?
Security Team Building

• BU InfoSec Officers – Legal, Finance, Sales, Marketing, HR, Development, IT, etc
• Committee driven
• Executive sponsor
• Internal audit is your friend
• Where are all the resources?
Security Committee Goals

• Business Security Mission Statement
• Aligning security with each BU
  - what are we protecting?
• Taking detailed inventory
  – Processes, Systems, Data, People
• Budgetize, Prioritize, Projectize
• Reporting directly to C-levels
Security Assessment & Gap Analysis

• Capability Maturity Model (CMMI)
• Cybermaturity Platform
CMMI – 5 Levels

Level 1
Initial
Processes are unpredictable, poorly controlled, reactive.

Level 2
Managed
Processes are planned, documented, performed, monitored, and controlled at the project level. Often reactive.

Level 3
Defined
Processes are well characterized and understood. Processes, standards, procedures, tools, etc. are defined at the organizational (Organization X) level. Proactive.

Level 4
Quantitatively Managed
Processes are controlled using statistical and other quantitative techniques.

Level 5
Optimizing
Process performance continually improved through incremental and innovative technological improvements.

CMMI Institute
How and Where to Focus?

The Cybersecurity Hub on Twitter
Critical Business Processes

Order to Cash

- Customer Order
- Order Fulfillment
- Delivery
- Invoicing
- Customer payments/Collection
- Cash Application
Patch Management is Paramount!
Data Inventory

- What, where, why, when & how
- Follow the data trail
- Backups
- End-user computers
- Storage media
- Archived applications
- What’s in the Cloud?
Data Classification

- Public, Internal, Confidential, Secret
- PII: Customer & Employee
- Defined Repositories
- Commensurate Security Levels
- Managed Data Life Cycle
Security Policy

- Compliance Driven
- Business Driven
- Ownership
- 3rd party
- Customer Input
- Training
- Controls Design & Mapping
  - Cloud Controls Matrix (CCM) - Cloud Security Alliance
Building Secure Foundations

61 - 90
Security vs Security Operations

Don't mind me...

CIPO

SecOps

Wordpress
Security Awareness Training

• Business Unit Relevance
• Joint delivery with BU-ISO
• Compliance driven
• Sec-Dev-Ops Training
• Relevant 3rd Party training
Application Security

- Every company is a technology company
- In-house vs 3rd Party
- Secure SDLC
- Training your Webapp!

Figure 27. Percentage and count of breaches per pattern (n=2,216)
Business Continuity

- Business Process Driven
- Disaster Recovery
  - Defined RTOs & RPOs
- Backup Strategy
- Denial of Service
- Testing
Prepare for the Worst
Data Breach Preparedness

• Breach Scenario Planning
• Table-top Exercises
• Decision Tree
• Detection & Logging
• Contact Lists
• Time-to-Notify
• Bitcoins?!
Customer-Facing Security

- Securing Client Services
- Supporting Sales
- Customer Security Compliance
- Vendor Security Questionnaires
- Legal Agreements – Security Language
Security is a Board-level Problem
And a message from the Office of the Privacy Commissioner of Canada:

• On November 1, 2018, Data Breach Notification Laws will be enforced in Canada.
KEEP CALM
DO THE
RIGHT THING
AND CYA
The Tribe Has Spoken ...

NOT ME
Chief I’m the Scapegoat Officer

Questions?