Influence and Implementation

Wes Earnest

April 2017

GSEC/GCIA/GCIH/
GWAPT/GPEN/GCCC/GSNA/
PMP/CISA/CISM/CGEIT

Objective

- What does it mean to "successfully implement information security"?
- How practical is information security in small organizations?
- How can I influence my organization to improve information security?

InfoSec in a Small Company

Cyber security is critical to any business enterprise, no matter how small. However, leaders of small businesses often do not know where to begin, given the scope and complexity of the issue in the face of a ***small staff*** and ***limited resources*** (US-CERT)

Bank Background

- Small town community bank
- Established in the late 1800s
- Legacy systems
- Flat network
- Antiquated core banking system

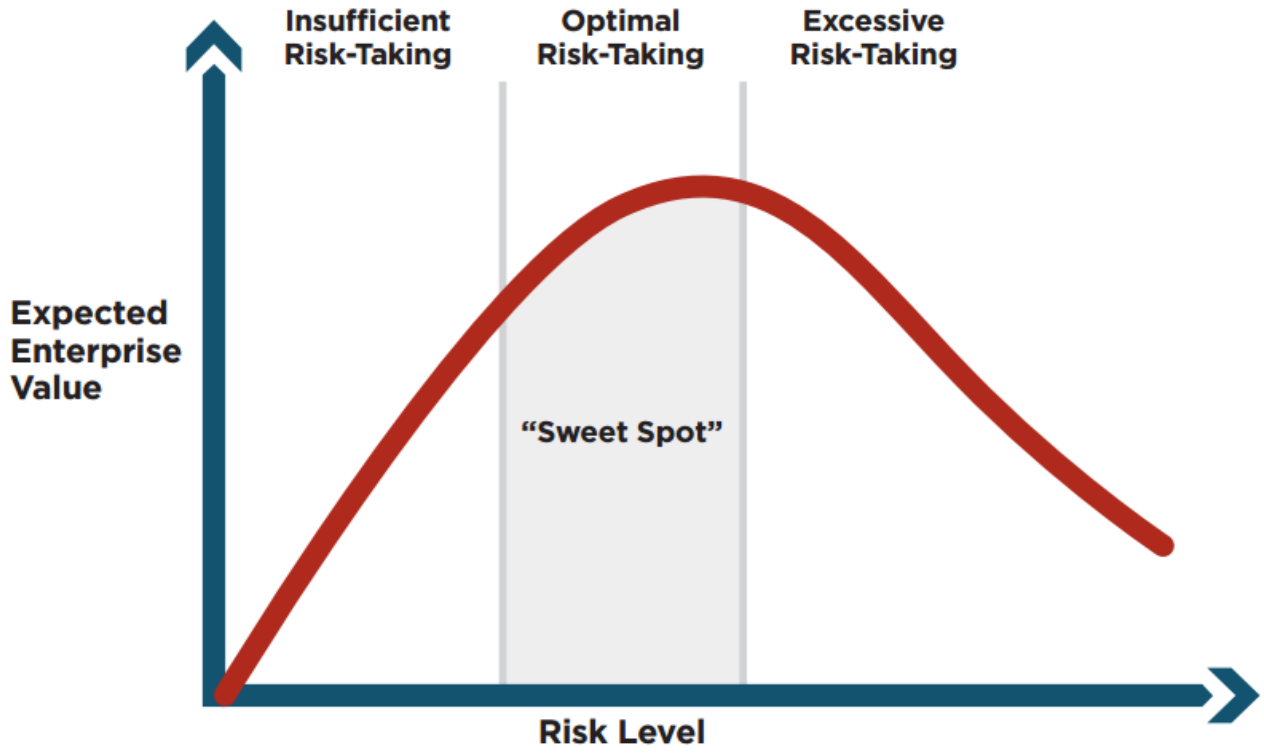
Us vs. Them

"The board and senior management are **responsible** for ***understanding the risks*** associated with existing and planned IT operations, ***determining*** **the risk tolerance** of the institution, and ***establishing and monitoring*** policies for risk management" (FFIEC, 2004)

Decision Making

- Important to ***understand*** the current state
- Who made the ***decision*** to implement bad security?
- **Active vs Passive** decision making
- Mapping past decisions to the bank's ***identity***
- **Continuous improvement**

Mitigating Risk



(Curtis, 2012)

Business Risk Manager

Only 1 in 10 security leaders have successfully made this transition from ***technology expert*** to ***business risk manager*** and can ***effectively communicate IT risks*** to business peers. (Symantec 2012)

Real World Case Study

- Minimum 15 Character Passwords
- VDI Workstations for All Employees
- Network Segmentation
- Vendor Management Process
- Complete Replacement of Core Banking System

Building Credibility

- Implementing 15 Character Passwords
  - User Awareness Training
  - Communicating Risk
  - Creating a Paradigm Shift
  - **Increased Productivity**

Workstation Life Cycle Management

- Upgrading from Windows XP to Windows 7
  - Migrate from physical workstations to VMWare Virtual Desktops
  - Standardized Configurations
  - Remove Local Admin and Shared Accounts
  - Consistent Application Inventory
  - Consistent Patch Management
  - Improved Incident Response

Network Segmentation

- Understanding Baseline Traffic
- Network Security Monitoring
- Limiting Lateral Movement
- Micro Segmentation

Vendor Management

- Federal Reserve Guidance on Managing Outsourcing Risk
- Broad definition of "Service Provider"
- Opportunity for improvement
  - Require security review / risk assessment of vendors
  - Require language in contracts for vulnerability remediation

Core Banking System

- Request for Proposal
- Looking for ways to generate value for business operations
  - Vendor consolidation
  - Process efficiencies
- Contract negotiations
  - Defining "security vulnerability"

Summary

- Implementing information security is more than just turning on a set of controls
- Small businesses can afford great information security, because it can generate value
- Influencing the decision making process (effective communication)