



**REDSPIN**

SECURITY

COMPLIANCE

RISK MANAGEMENT

# Operational Integrity

## Cost Effective Security Strategies for Community Banks

John Abraham, President  
Redspin, Inc.





# Overview

---

## Objective

- Share what we have learned about practical security and regulatory compliance issues.

## Context

- Redspin is a 5 year old company
- We have completed hundreds of audits for small and large banks.



# Common Issues

---



# Issue 1 - External Threats

---

- ⊙ Threats
  - FW – intruders accessing network (improving)
  - Modems (same)
  - No DMZ (same, some improvement)
- ⊙ Status = improving
- ⊙ Note: risk is a function of complexity



# Issue 2 – Invite the Enemy In

---

- ⊙ Firewall is good, but employees can invite danger
- ⊙ Workstations
  - Virus protection (status = good)
  - Patching (status = improving)
  - Users have unfiltered Internet access (status = technology exists)
    - Web browsing, other Internet services
- ⊙ Recommendation
  - Consistent deployment strategy
  - Limit user capabilities (i.e. installation rights, browsing)
  - Process oriented patch management



# Issue 3 - Remote Access

---

- ⊙ Strong firewall, but....
  - Simple VPN authentication
  - Insecure partner/home networks
  - Lack of security policy
- ⊙ Note
  - Remote networks extend the perimeter of responsibility for bank security
  - Only as strong as weakest link



## Issue 4 – DMZ (or lack of)

---

- ⊙ What is a DMZ?
- ⊙ Assumption: ALL servers accessible from the Internet WILL get compromised.
- ⊙ Hosting public servers on internal network:
  - Is risky
  - Raises the bar on security management
  - Increases the impact of an incident



# Issue 5 – The Front Door

---

- ⦿ Confidential information leaves the building
  - Email (understand how interoffice mail is routed)
  - Laptops
    - Who uses, security policy, data storage
    - SB 1386 / AB 700 → encryption
  - PDA's



# Issue 6 – Trusting Partners

---

- ⦿ They don't trust you!
- ⦿ Do you trust them?



# Issue 7 – Business Continuity

---

- ⦿ Too complex
- ⦿ Are not kept up to date
- ⦿ BCP Needs to be tested
- ⦿ An opportunity to identify critical systems

# Framework for Improvement

---





# Avoid Complexity

---

- ⊙ Complexity = risk
- ⊙ Example
  - Technology: Fully meshed redundant gateway
    - Switch(2) -> rtr -> firewall(2) -> rtr -switch(2)
  - Result: Downtime
- ⊙ Lesson
  - Solving one problem can lead to others
  - Consider the complexity risk when deploying new technology



# The Importance of First Impressions

---

- ⊙ First impressions
  - A reliable indicator of the state of compliance
- ⊙ Regulators
  - Assume they can also
- ⊙ Example: don't disregard the minor details
  - The anatomy of an intrusion – a series of steps
  - What you think is unimportant may be significant



# More Process / Less Tech.

---

- ⊙ Security is a process
  - Not technology
- ⊙ Examples
  - IDS = only as good as:
    - Configuration
    - Process
      - Configuration refinement
      - Escalation procedures
  - Backup without media testing and proper storage
  - Strong passwords with post-it notes
  - Complex workstation config without automated deployment



# Consistent Approach

---

- ⊙ Moving Target
  - Examiners / trend-of-the-day
- ⊙ Example
  - IDS
  - Business continuity
  - Outsourced/shared email
- ⊙ Lesson
  - Do the right thing
  - Don't adjust strategy purely based on expected auditor focus
  - Maintain a consistent approach



**REDSPIN**

SECURITY

•  
COMPLIANCE

•  
RISK MANAGEMENT

---

{ end }