# Rats in the Cellar and Bats in the Attic

## Anatomy of Security Awareness Testing

***A facilitated discussion***

Wisconsin Bankers Association Technology Conference
September 27, 2010


Mark T. Chapman, MSCS, CISSP, CISM
Chapman Technology Group, Inc.
www.bizoptix.com
mchapman @ ctgi.net

Ken M. Shaurette, CISSP, CISM, CISA
FIPCO
www.fipco.com
kshaurette@fipco.com


RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

*By now, technical vulnerability scanning. penetration testing and even social engineering should be easy.*

*(Speaker shares a few quick anecdotal stories about mice, bats and other creatures in a "vulnerable" cabin in Northern Wisconsin.)*

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Approach

This will be a facilitated discussion covering areas such as vulnerability scanning, penetration testing and social engineering.

Bring your personal experiences and preferences along for discussion.

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Ground Rules for Discussion

- This is supposed to be a **discussion**.
- Please “cleanse” your stories to **protect the victimized**.
- No advertising.
- Find something or someone to **disagree** with today.

RISKOPTIX™ COMPLIANCE SIMPLIFIED

FIPCO® FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Agenda

- **Planning**
- **Discovery**
- **Analysis**
- **Penetration**
- **Reporting**


RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Planning

- Identify the Specific Purpose
- Define the Scope
- Earn Management Buy-In
- Decide to In-Source or Outsource
- Anticipate the Benefits
- Anticipate the potential fallout

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Specific Purpose

- Demonstrate Due Care
  - Infrastructure Patching
  - Intrusion Prevention
- Security Awareness
- Discovery
- To Justify Funding

*<u>Hint:</u>*
*You must understand the specific purpose of the security awareness testing*

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Scope

- What is the **scope**?
- Do you identify "**trophies**"?
- What is **the *right* scope**?
- Keep me out of **Jail**!
- **Ethics** and Governance.
- What potential **side-effects** are allowed?
- **"Selling"** the scope.

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Earn Management Buy-In

**Motivators:**

- **Compliance / Fear**
- **Means to justify other initiatives**
- **New Management Eager to Learn**
- **“True Believers”**

**Challenges:**

- **“It costs money”**
- **“I already know the risks better than anyone”**
- **“We have more important things to do”**

**Results:**

1. **Go through the motions**
2. **Do it right**

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# In-Source or Outsource?

- Current Capability
  - Do we have the capability or can we train in-house?
  - Can we identify a firm with **independent**, **knowledgeable** and **trustworthy** resources?
- Future Capability
  - Turnover of trained employees
  - Dependence on consultants - costs

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Anticipated Benefits

- To **learn** something new
- To **validate** or quantify a concern
- To **standardize communication** of vulnerabilities
- To establish **common language** and tools
- To **satisfy the auditors** and regulators
- To improve employee awareness and standard operating procedures when handling customer data.

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

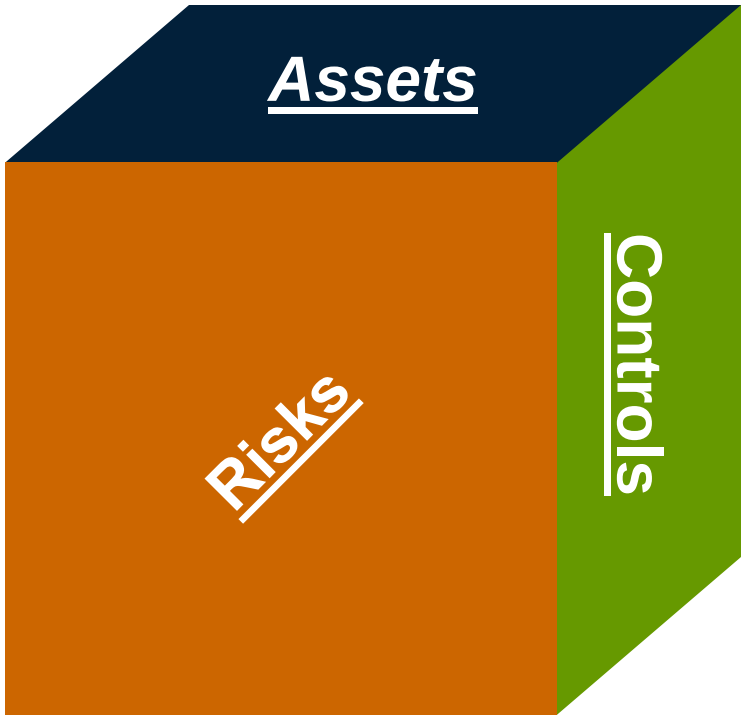
# Automation

- Specialized Software
  - **Discovery/Mapping** Tools
  - **Audit** Tools
  - **Vulnerability** Assessment Tools
  - **Penetration** Testing Tools
  - **Web Application** Testing Tools
  - **Source Code** Review Tools
  - **Social Engineering** Tools
  - **Websites**

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Assessment Universe




3-Dimensions*

- Assets
- Risks
- Controls

* Technically, there is a fourth dimension,
Instead of “Time” it is “Testing” which gets into
Risk Monitoring and Risk Management.

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Asset Universe

## Scope

- ☑ Business Functions
- ☑ Fixed-Assets
- ☑ Strategies
- ☑ Brands
- ☑ Contracts
- ☑ Cash
- ☑ Intellectual Property
- ☑ Products
- ☑ People

## Granularity

*How many levels of assets do we want to consider?*

- ☑ Buildings
- ☑ Rooms
- ❑ Individual Bricks

## Detail

*How much information do we want to understand for each asset?*

- ☑ Asset Type
- ☑ Asset Owner
- ☑ Importance
- ☑ Dependencies

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Risk Universe

## Scope

- ☑ Power Outage
- ☑ Pandemics
- ☑ Water Damage
- ☑ Fraud
- ☑ Computer Hacking
- ☑ Employee Turnover
- ☑ Tampering

## Granularity

*How many levels of risks do we want to consider?*

- ☑ City-Wide Blackout
- ☑ Accidental Power Disconnect
- ❑ Mouse Chews Through Power Cord

## Detail

*How much information do we want to understand for each risk?*

- ☑ Risk Type
- ☑ Threat Source
- ☑ Likelihood
- ☑ Impact

RISKOPTIX™ COMPLIANCE SIMPLIFIED

FIPCO® FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Controls Universe

## Scope

- ☑ Financial
- ☑ Physical
- ☑ Technological
- ☑ Reputation
- ☑ Legal
- ☑ Insurance

## Granularity

*How many levels of controls do we want to consider?*

- ☑ Use a Framework
- ❑ Individual “Bricks”

## Detail

*How much information do we want to understand for each control?*

- ☑ Control Owner
- ☑ Effectiveness
- ☑ Compliance Info
- ☑ Assessment Criteria

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Discovery

- Where should discovery start?
- Mapping the scope.
- Should it be “blind” or “informed”?
- Where should discovery stop?

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Analysis

- Two approaches:
  - Focus on the most urgent or most important.
  - Consider how many holes it takes to sink a ship.
- Where are you coming from?
  - Technology Focus
  - Business Focus
  - Both

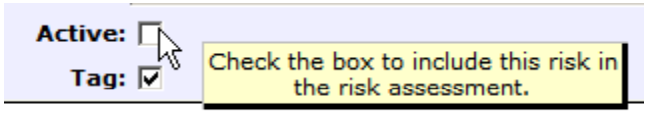
RISKOPTIX™ COMPLIANCE SIMPLIFIED

FIPCO® FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Is There Anything to Attack?

**Goal:**

To combat the natural exponential growth of assessment efforts by reducing the number of **low-priority** assets, risks and controls.




**Approach:**

Select a threshold for exclusion from further risk assessment efforts while documenting decision. Retain all excluded data to accommodate priority changes and to reduce duplicate analysis next time.

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Penetration

- **How easy** is it to get in?
- **How far** do you go?
- What potential **side-effects** are allowed?

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Reporting

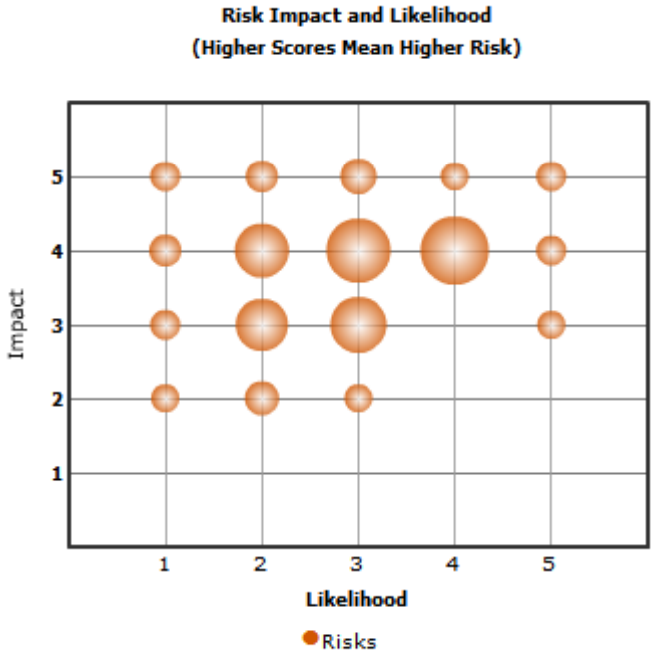
- How to inform management about the findings?
- Evaluate Intended Specific Purpose.
- Write the “Final Report”.
- Track Actions Over Time.
- Evaluate Project Effectiveness.

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# How Do You Measure Success?

- By the **size** of the report?
- By the **dollar**?
- By the number of **trophies**?
- By the **speed** of execution?
- By the **business impact**?
- By the **understandability** of the report?
- By **passing** future audits?



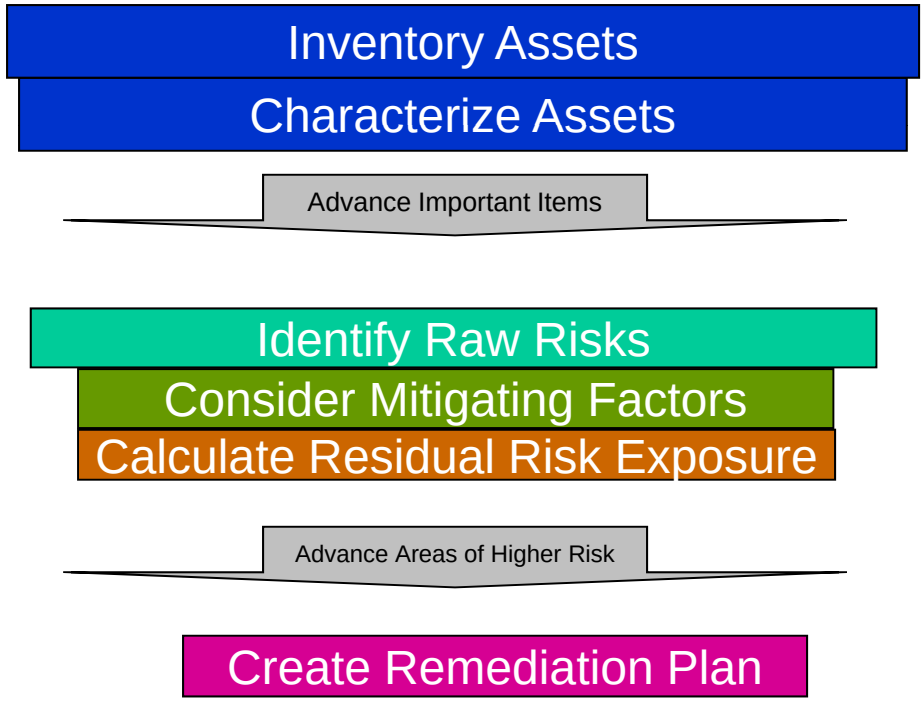

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Intended Specific Purpose

Any Assessment can only “Hit the Mark” if it serves a purpose:

- Audit Planning
- Budgeting
- Compliance
- Disaster Planning
- Policy Writing
- Risk Management
- Remediation
- Vendor Selection
- Remediation Planning

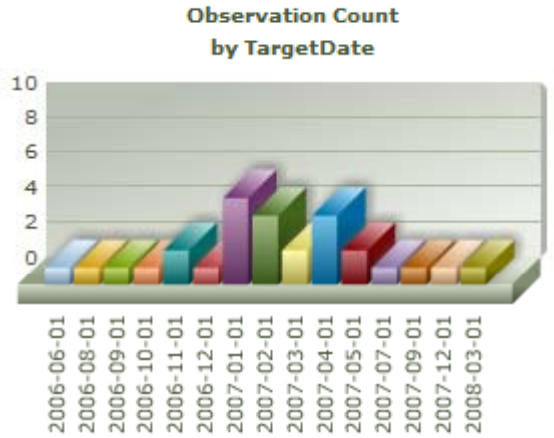



RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Write the “Final Report”

- Do not
  - Think “bigger is better”
- Do focus on
  - Process used (brief)
  - Discoveries (trophies)
  - Trends
  - *Actions* (proposed, planned or completed)




RISKOPTIX™ COMPLIANCE SIMPLIFIED

FIPCO® FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Evaluate Effectiveness

- What did you learn through the process?
- What unexpected benefits did you realize?
- How did you keep the process from getting too detailed or out of control?
- How can you improve the process next time?
- These reports look scientific and absolute - how did you handle the inherent subjectivity?
- Did you achieve your objectives?

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# A Few Resources

www.identitytheft.info/criminal.aspx

www.identitytheft.info/internetsecuirty.aspx

www.fipco.com/Web/ProductsServices/ITAuditSecurity

RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®

# Questions?


mchapman @ ctgi.net

(262) 546-1867

kshaurette@fipco.com

(608) 441-1251


RISKOPTIX™
COMPLIANCE SIMPLIFIED

FIPCO®
FINANCIAL INSTITUTION PRODUCTS CORPORATION®