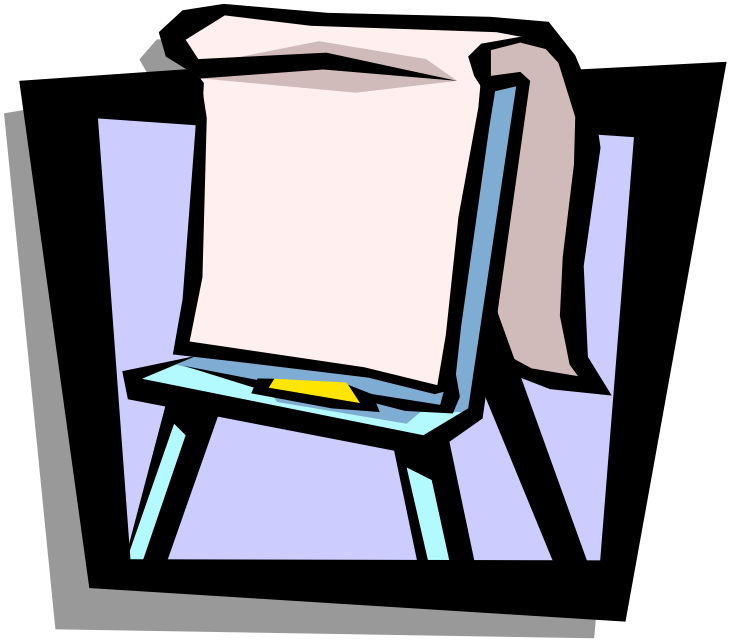
Information Security Risk Management Best Practices

Presented by:

Eric Holmquist
President
Holmquist Advisory, LLC
eric@holmquistadvisory.com
www.holmquistadvisory.com

Agenda

- Info Security Policy
- Assessing Risk
- Info Security Strategy
- Senior Engagement
- Insiders/Outsiders
- Incident Response
- Q&A



Info Security Policy

- Granularity: Board vs. Operating
- Fingerprints Matter
- Effective Training
- Enforcement is Critical
- Can’t Regulate Everything
- Policy vs. Standard vs. Guideline

Info Security Policy

- Board
  - Program requirement
  - Defines roles & responsibilities
  - Reporting
- Operating Examples
  - User administration
  - System administration
  - Change control
  - Usage (systems, social media, etc.)
  - Retention

Assessing Info Security Risk

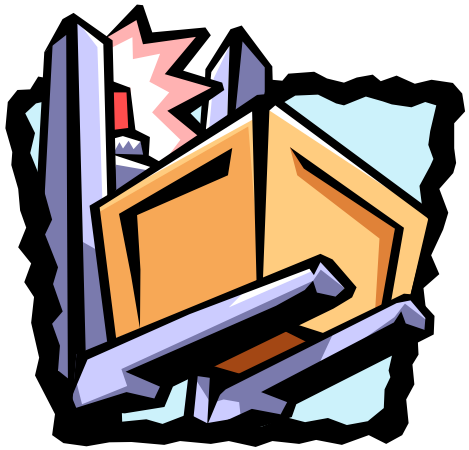
- The key is in capturing the complexity
- This is a relative risk exercise, not an absolute
- The overwhelming make-or-break factor is the organization's willingness to be honest
- What you think you "know" can, and probably will, work against you with dangerous consequences
- This exercise is quite a bit easier, and harder, than you think

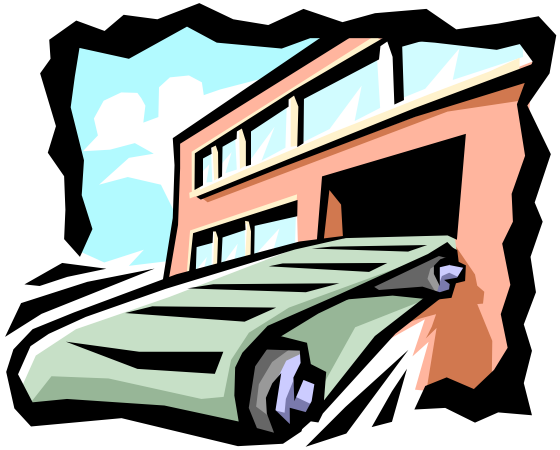
Four Focal Points

- Internal Systems
  - Owner: IT
- Applications / Data
  - Owner: Business or IT
- Physical Records
  - Owner: Individual Departments
- Third Parties
  - Owner: Relationship Managers

Data Inputs

- Classification – (type and sensitivity)
- Quantity – (large, moderate, small, none)
- Access method(s) – (Who, how, why, when)
- Threats – (“What could go wrong?” exercise)
- Vulnerabilities – (The biggest moving part)





Risk Mitigation

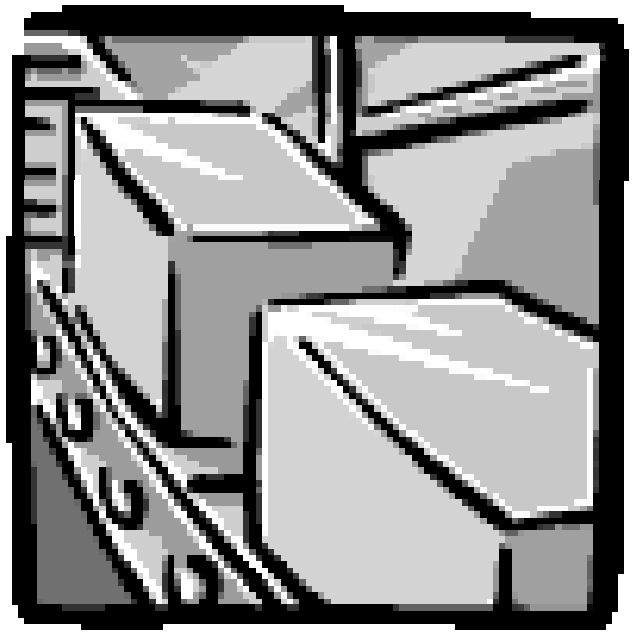
- Internal controls
- Governance
- Testing
- Training
- Insurance
- Monitoring
- Recovery

Note that some apply individually and some apply globally. This must be factored in.

The net of mitigation is the residual risk.

Outputs

- Residual risk ratings
  - Ideally by system, app/data, physical sites, third party
- Documentation
- Reporting
- Strategic plans



Info Security Strategy

- Be very clear on responsibility
- Requires a base understand of risk
- Drive from the risk assessment
- Must demonstrate clear value
- Don’t band aid program
- Strategy & compliance
- Align with Corp. strategy?

Management Engagement

- Language, language, language
- Awareness breeds engagement
- Must be safe to be ignorant
- Info must be digestible
- What is the value proposition?
- Competition is your friend
- Your ace in the hole: fear

Threat Management

- Internal
  - The message: 1) We're watch and 2) we'll prosecute
  - Why we do training
  - Monitoring
  - Auditing
- External
  - The castle walls are probably high enough
  - Third parties are a bigger source of risk

Incident Response

- Unpreparedness is inexcusable!
- Who will:
  - Run point?
  - Communicate with execs, media, regulators, investors, customers, staff?
  - Oversee account fraud alerts and risk mitigation?
  - Coordinate with law enforcement?
- Learn from prior events
- Test, test, test

Final Thoughts

- Program can’t be managed to the 80/20 rule
- Single best thing you can probably do to improve your program is fix your data inventory
- The second best thing is fix your policies
- Third is tighten up vendor management
- Fourth is improve your documentation
- Fifth is develop and publish residual risk ratings
- Finally, get more people in the conversation