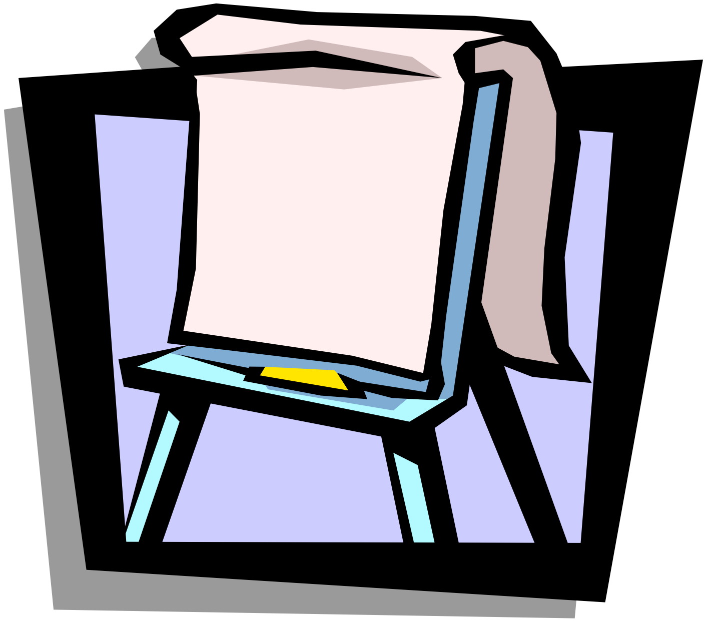
INFORMATION SECURITY SearchSecurity.com INFORMATION SECURITY DECISIONS

Creating Successful Information Security Governance Using a Risk-based Approach

Eric Holmquist
VP, Director of Operational Risk Management
Advanta Bank Corp.
eholmquist@advanta.com

Agenda

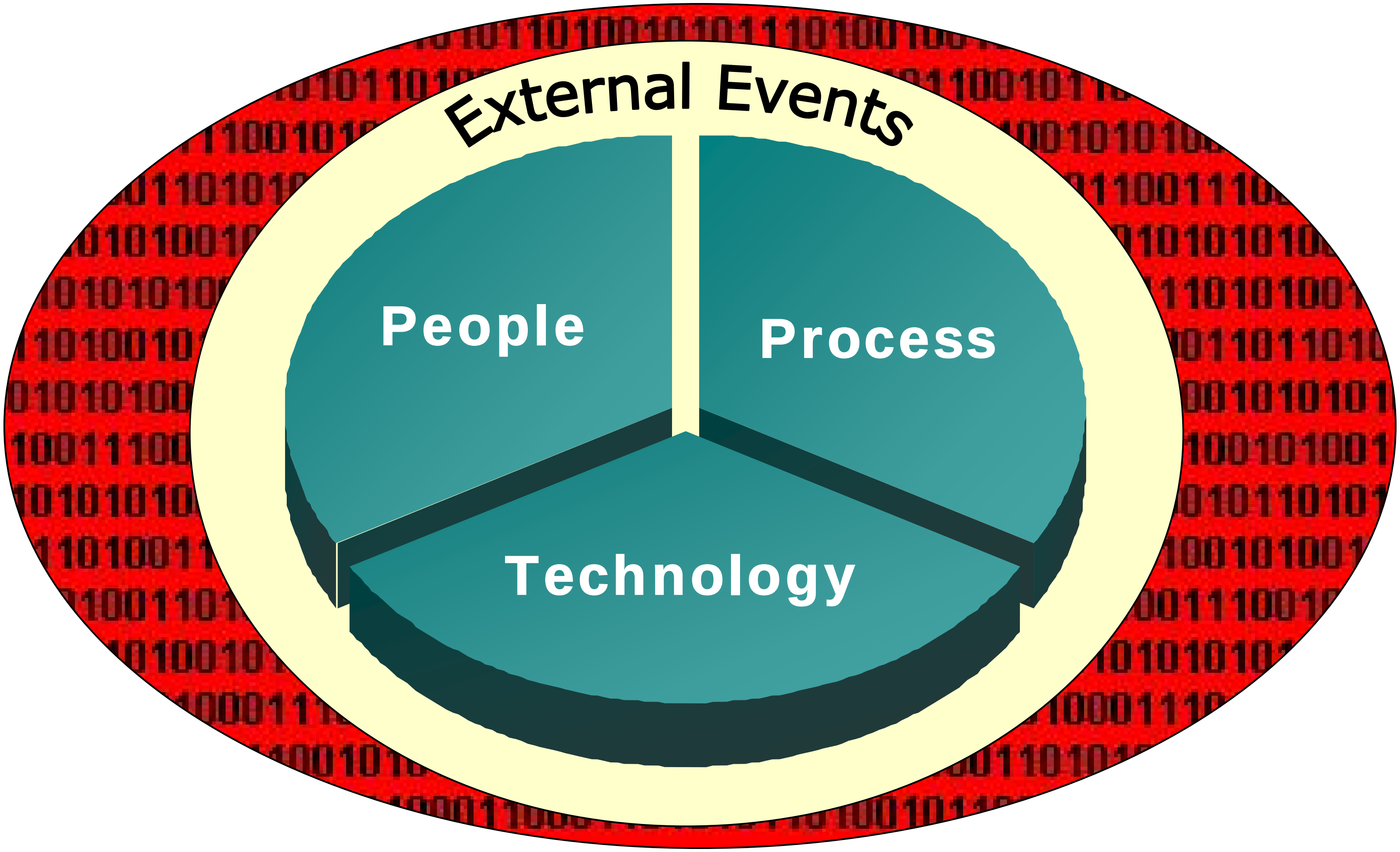
- What is a risk based approach?
- IS Governance.
- Assessing IS risk.
- Other tactical points.
- Q&A.



Where Do We start?

Information security must be approached as a business issue not a technology issue. Once we agree on this then we can consider using risk management practices.

Information Security



External Events

People

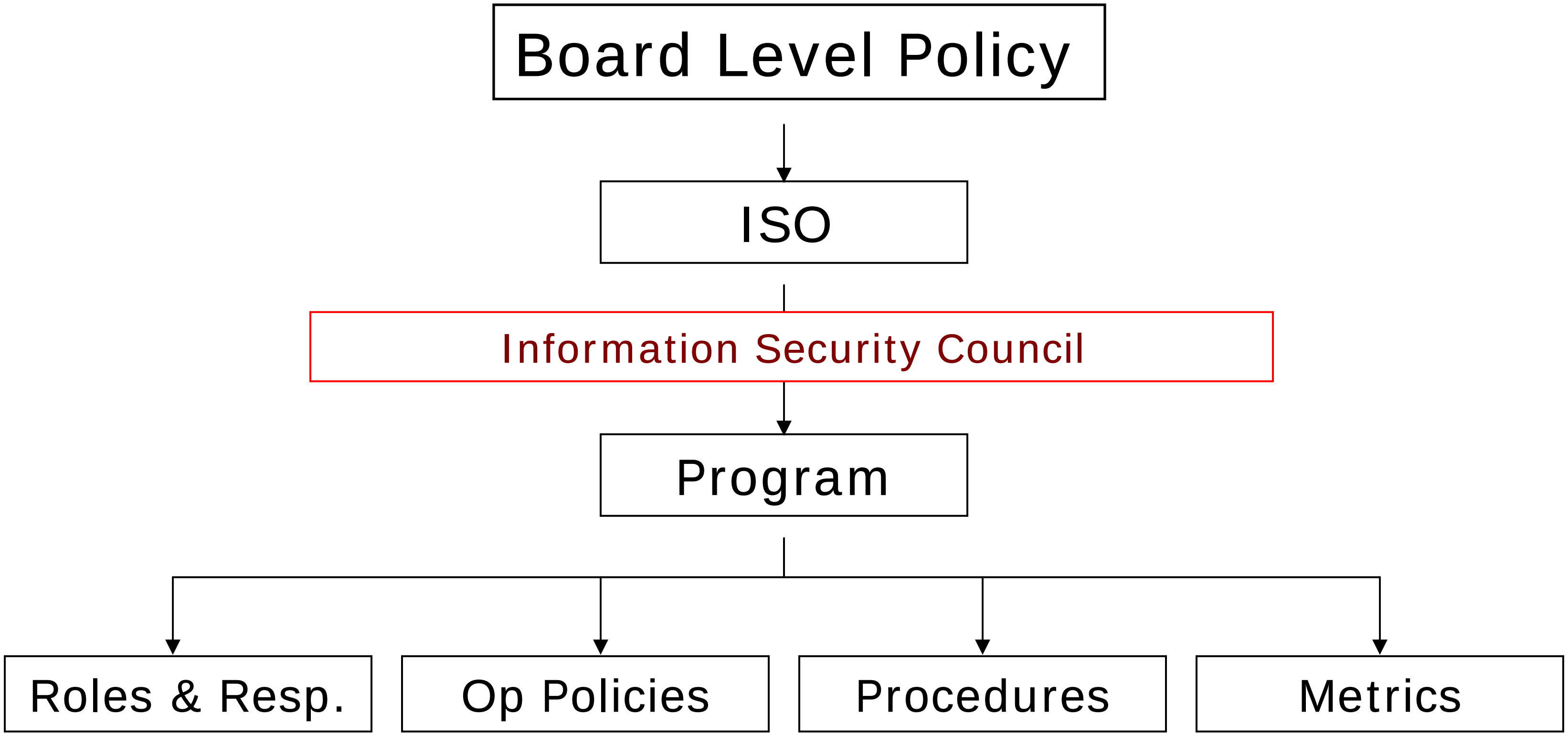
Process

Technology

Taking a Risk Based Approach Means:

- Cross functional governance
- Comprehensive risk assessment methods
- Dynamic risk measurement methods
- Ownership and accountability
- Effective communication
- Ensuring ability to quickly respond
- Meaningful reporting mechanisms
- Historical loss data is of almost no value

Governance Structure



Board Level Policy

ISO

Information Security Council

Program

Roles & Resp.

Op Policies

Procedures

Metrics

Information Security Policy

- Board level policy
- Establishes issue as business risk
- Defines the role of the CISO
- Sets mandate for program
- Establishes program expectations
- Not detailed on program specifics

Information Security Program

- Regulatory requirement
- Supports issue as business risk
- Documents major components
- Eliminates unspoken assumptions
- Sets clear responsibilities
- Defines risk-based approach
- Establishes training curriculum
- Supported with operating policies

Engaging Senior Management

- Starts with education and awareness.
- Once educated, solicit active input.
- Language is the key!!!!

Information Security Council

- Give it authority to set policy
- Get senior participation
- Make it cross-disciplinary
- Make it visible
- Make it safe

Build a Big Army

- Create a culture of cooperation
- Build social intolerance to data exposure
- Make disclosure safe
- Don’t underestimate people’s “gut”
- Make it everyone’s responsibility
- Reward creativity

Using a Risk Based Approach

- Everything starts with the risk assessment
- Manage to assessed risk, not perceived risk
- Have to understand inherent vs. residual risk
- Insiders are exponentially more of a threat than outsiders
- Managing a control is not managing a risk
- Ability to respond quickly and effectively is critical – Time is not on your side!

Assessing Risk

- **Approach 4 ways**
  - Information systems
  - Electronic data
  - Physical files
  - Third parties
- **Focus on accountability**
- **Some overlap, but each has distinct owners**
- **Use self-assessments vs. loss date or scenarios**

Risk Quantification

- **Risk is quantified in four broad categories**
  - What's at risk?
    - Customer, corporate, operational, prospect, third-party
  - What would be the impact?
    - Financial, operational, regulatory & reputation
  - What could be the source?
    - Internal, external & natural disaster
  - What can we mitigate?
    - Prevention, monitoring & recovery

Data Breach Response Program

- Must have a first-day checklist
- Must have a clearly defined primary coordinator
- All staff must know who the primary coordinator is
- Event notification list
- Link with larger incident response program
- Data breach exercise is imperative

Monitoring and Reporting

- **Information security by nature defies M&R.**
- **There is a limited amount we can monitor.**
    - However, data trends can be meaningful
- **Tie into KRI program – what can we track?**
- **The real value may be in the visibility.**
- **Reporting must be timely, clear, root-cause focused and actionable.**

And Finally…

- Everything starts with strategy
- Training is absolutely critical
- You’re not focused enough on internal risk
- You’re not focused enough on residual risk
- In the end, the worst possible answer to assessing information security risk is…

Questions / Discussion