How Much Security Is Enough?

University of British Columbia

March 22, 2007

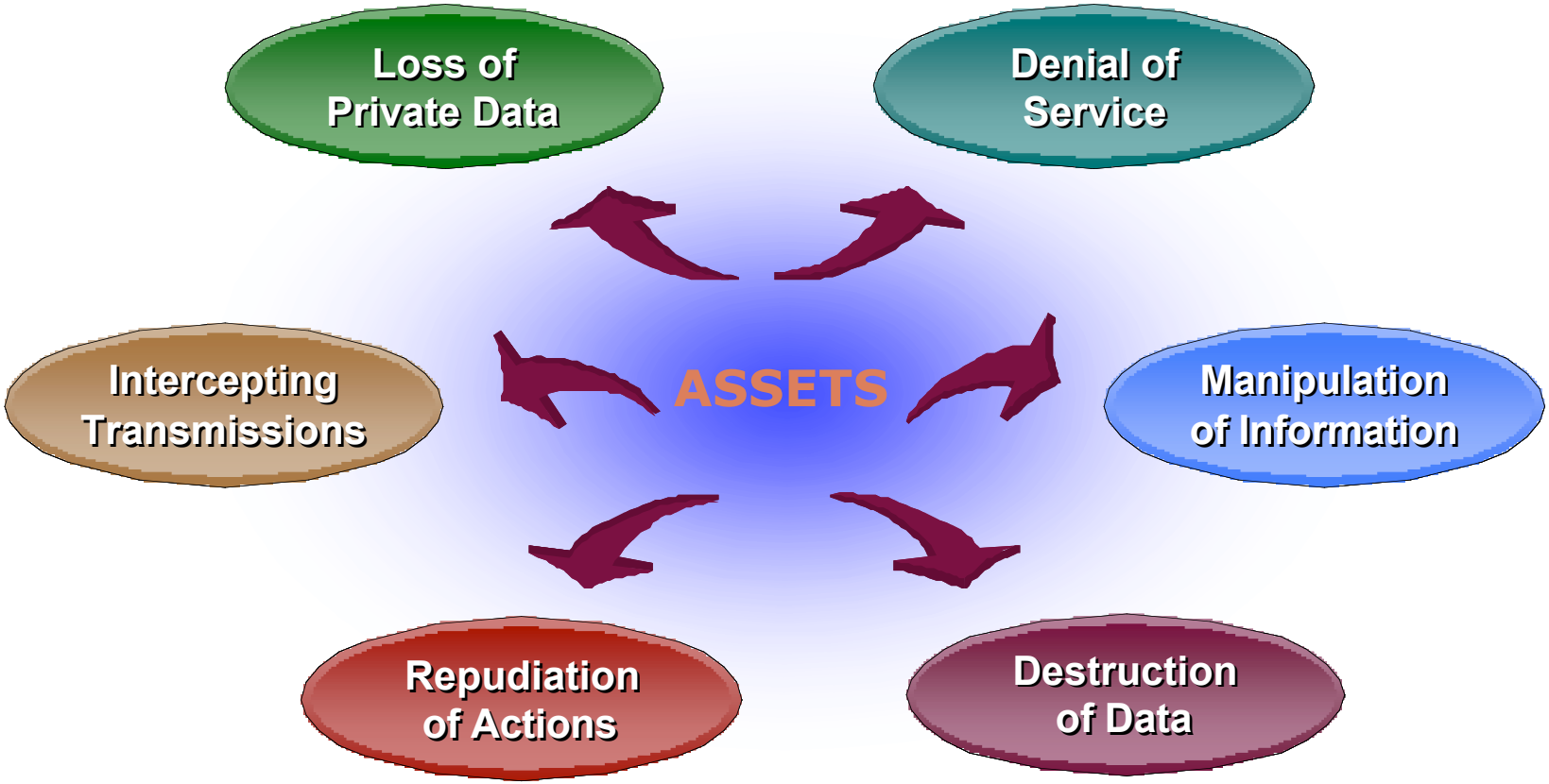
Agenda

Enterprise Information Security Framework

- What are the challenges?
- What problem are we trying to solve?
- Overview of enterprise information security
- Creating an enterprise information security program in support of risk, legal and regulatory obligations
- Information security control frameworks
- Measuring maturity of the program

The Challenges

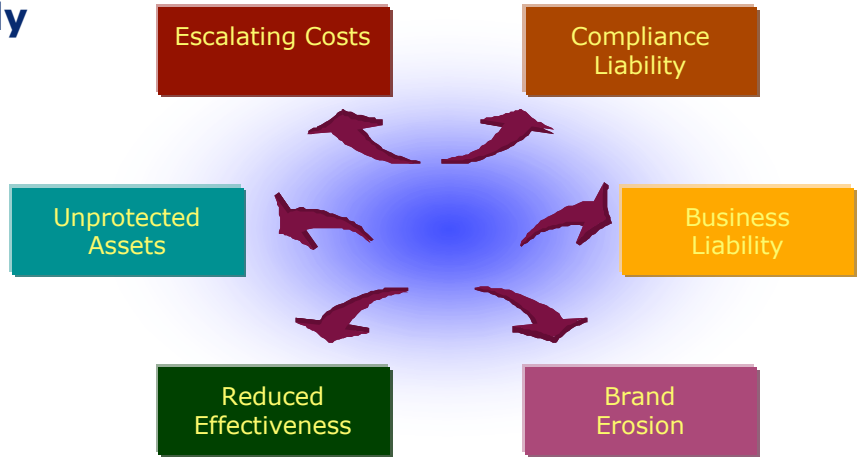
What are you trying to protect?



Security challenges faced by organizations

Organizations are constantly challenged with information security issues with ever increasing threat profiles. Faced with these challenges, organizations continue to ask themselves;

- Are our Information security initiatives **aligned** with our **business needs**?
- Are our **customers' and trading partners'** information security initiatives and requirements **compliant and compatible** with ours?
- Are our information **security practices** providing adequate assurance to **meet regulation or compliance requirements**?
- Are we perceived as a **responsive organization** meeting the needs of our stakeholders, our customers, and trading partners?
- Do our information security controls align with **industry-related and internationally accepted guidelines**?
- Are we aware of our **security risks** and are they being **effectively managed**?
- Are we **measuring the effectiveness** of our information security Investments?



Bottom Line…..Are We Secure?

Stumbling blocks arise when the security program is not aligned with business needs.

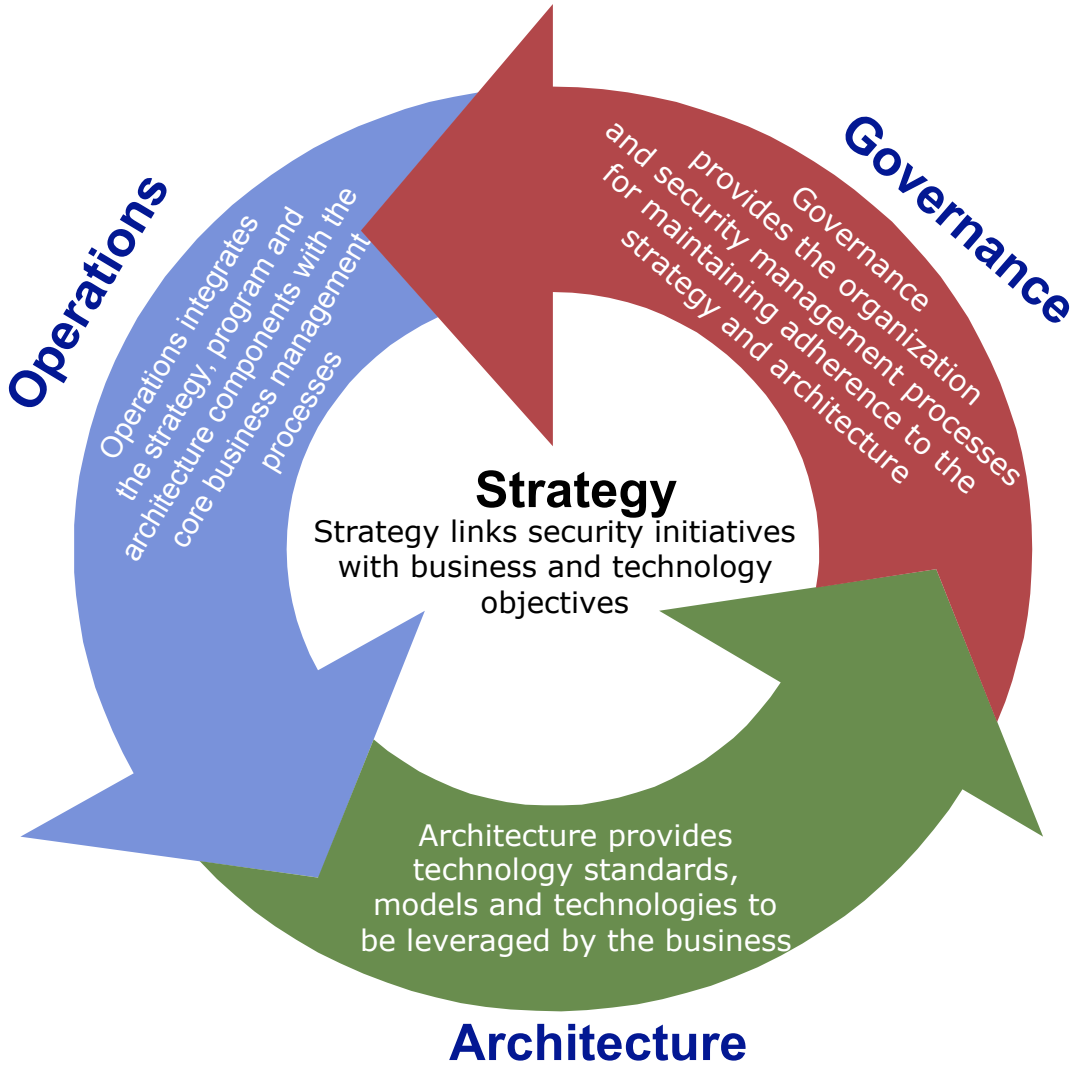
Most Enterprise Security Initiatives Fail Due to Lack of Buy-In

- Lack of demonstrated ROI
- Poor definition of success
- No real business alignment
- No long-term strategy to decrease the level of overall security risk and exposure
- No framework within which to design and deploy solutions for new problems
- Technically led, IT-based security projects
- Low prioritization of security as compared to business initiatives
- Lack of appreciation for the importance of security in today's enterprise
- Immaturity of technology solutions

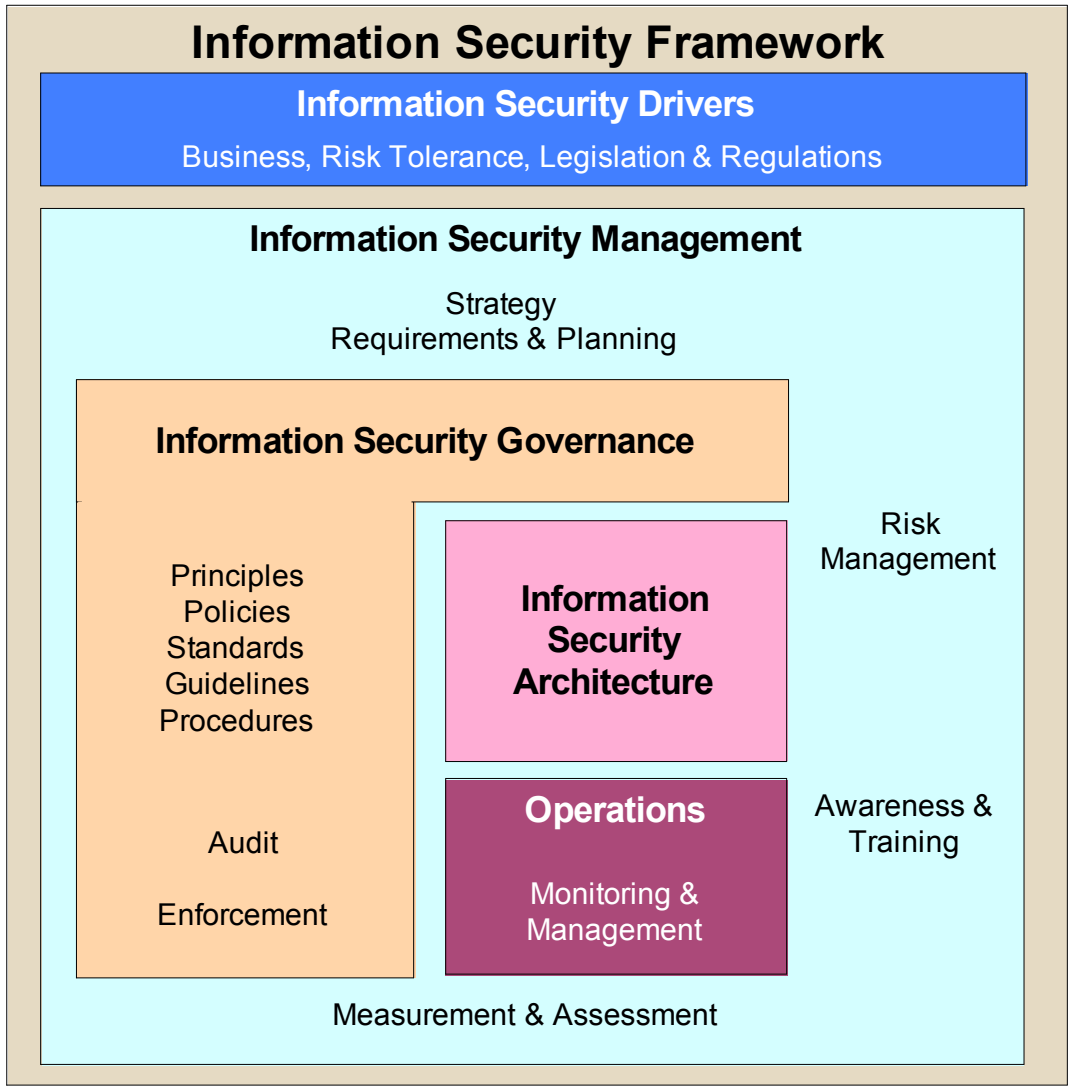
Overview Security Management

A sound enterprise information security strategy should have proper balance and integration with the security governance, architecture and operations

A security strategy is supported by three critical components …



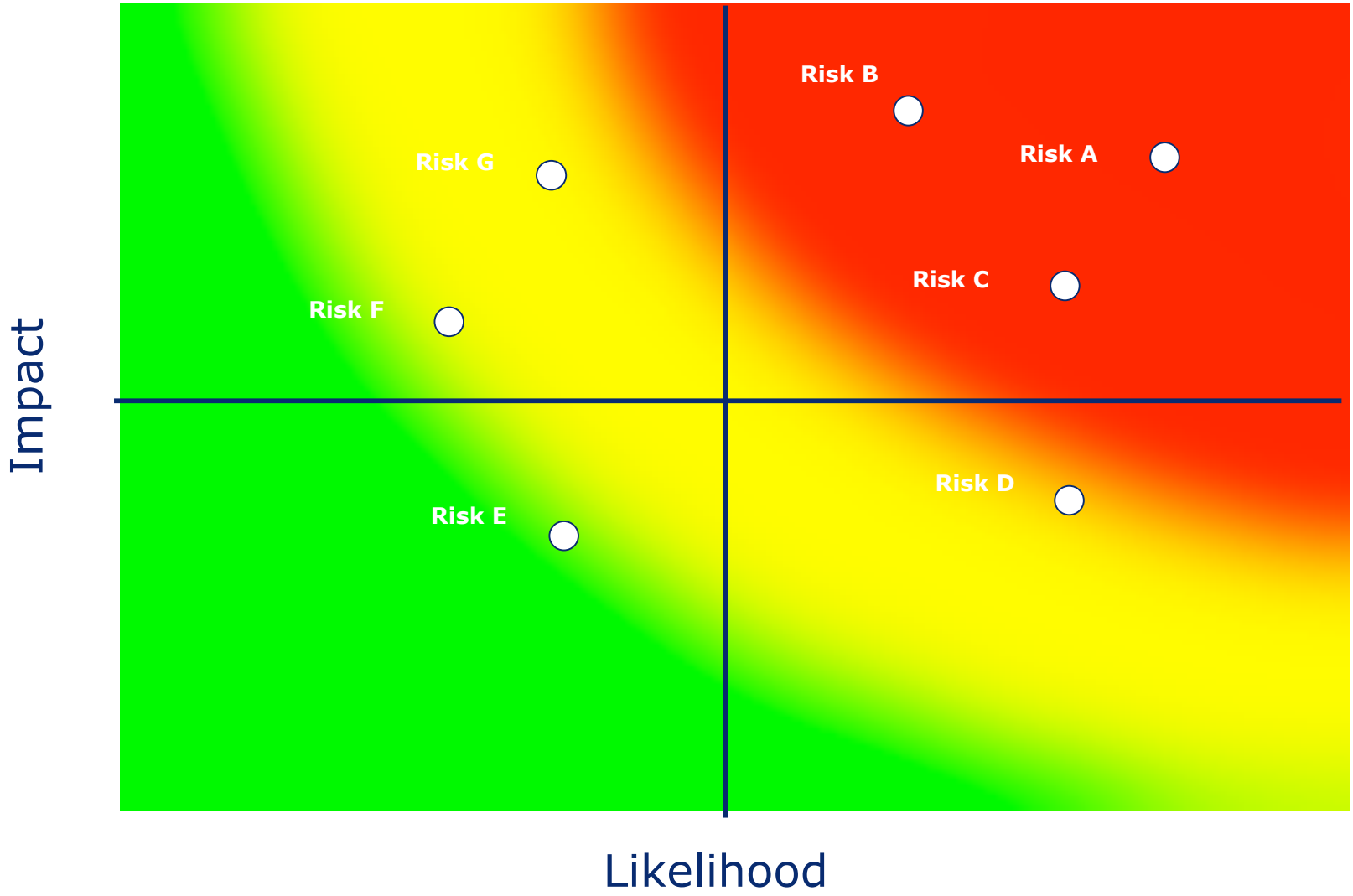
What does the information security program look like? – Define the Information Security Program Framework



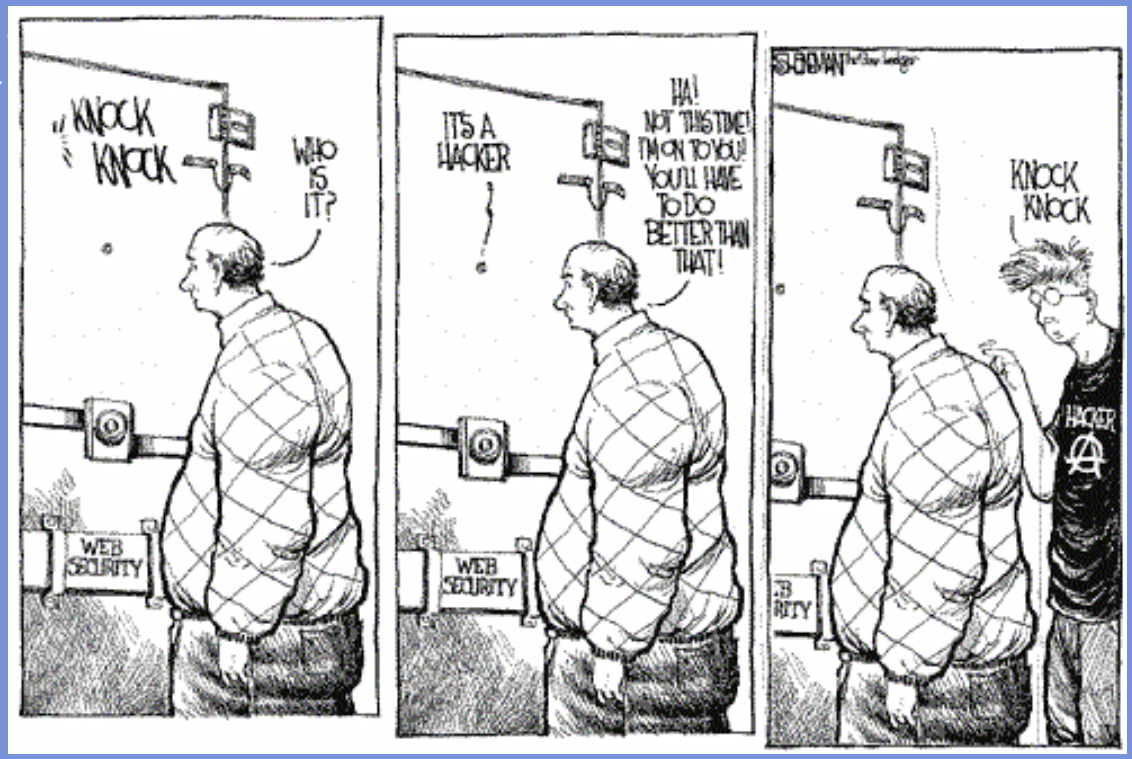
Security Risk Management

Security Risk Management

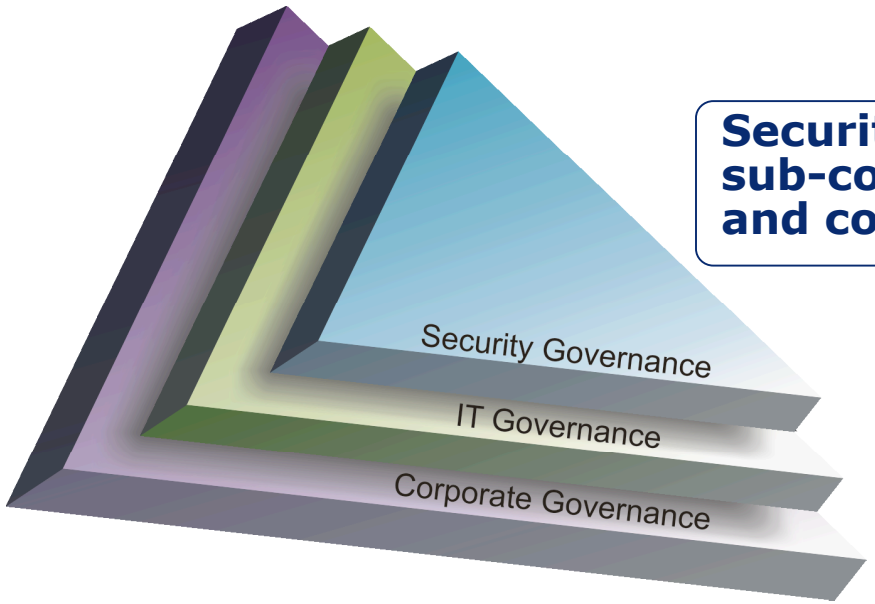
Typical Risk Profile



Information Security Control Framework



The Information Security Governance Framework is Built on the Corporate and IT Governance Framework



Security Governance is a sub-component of overall IT and corporate governance

Eleven Key Domains of ISO/IEC 17799:2005

Security Policy
- Outlines BMO's expectations for security
- Demonstrates management support & commitment

Organizing Information Security
- Management structure for security
- Security responsibilities
- Establish incident response process

Asset Management
- Inventory of BMO's information assets
- Identify appropriate level of security

Human Resources Security
- Security is a key component of HR & operations
- Job descriptions & responsibilities
- Job screening

Physical & Environmental Security
- Policy that protects infrastructure, physical plant & employees
- Building access; maintenance

Communications & Operations Management
- Preventing security incidents through preventative measures (A/V; logging & monitoring etc.)
- Incident response procedures

Acquisition Development & Maintenance
- Ensure security is an integral part of any network deployment / expansion

Compliance
- Complying with any applicable regulatory & legal requirements

Access Control
- Access control to the network & application resources
- Password management, authentication & event logging

Security Incident Management
- Complying with any applicable regulatory & legal requirements

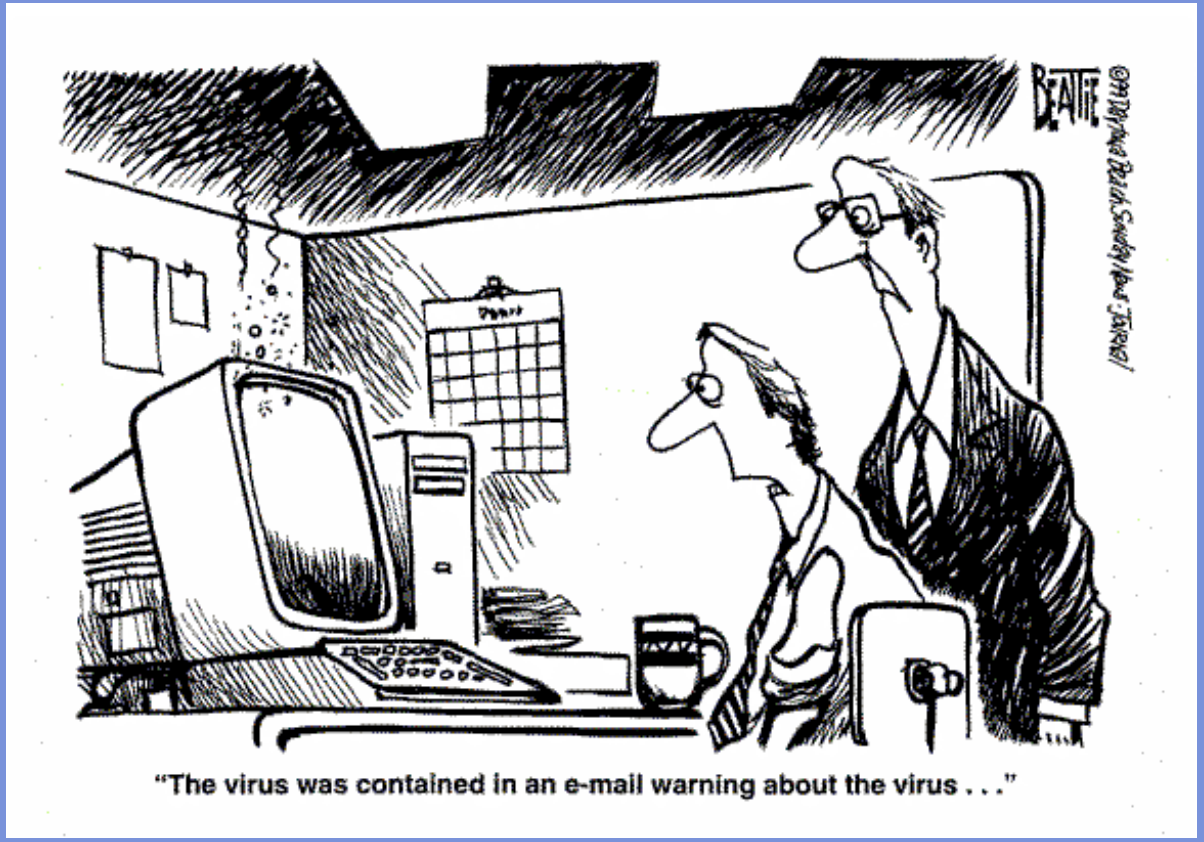
Business Continuity Management
- Planning for disasters
- Recovering from disasters (natural & man-made)

Many Frameworks

- ISO-Information Security Guidelines (ISO-17799, ISO27xxx)
- Control Objectives for IT (CoBiT)
- IT Infrastructure Library (ITIL)
- Information Security Forum Standard of Good Practice (ISF)
- Systems Security Engineering - Capability Maturity Model (CMM)
- General Accepted Information Security Practices (GAISP)
- National Institute for Standardization of Technology (NIST)
- …..

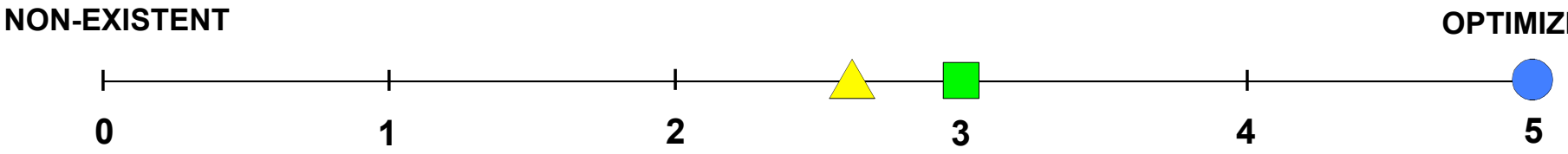
Choose one framework that meet most of your needs and supplement it with other frameworks as appropriate

Measurement



"The virus was contained in an e-mail warning about the virus . . ."

Information Security Governance Maturity Model



Average in Manufacturing Industry (2.7)

Manufacturing Industry Best Practice (3.0)

Banking Industry Best Practice (5.0)

0 - Non-Existant	- Management processes are not applied at all
1 - Initial	- Processes are ad hoc and disorganized
2 - Repeatable	- Processes follow a regular pattern
3 - Defined	- Processes are documented and communicated
4 - Managed	- Processes are monitored and measured
5 - Otimized	- Best practices are followed and automated

- The Maturity Model is sponsored by the IT Governance Institute.
- It is used to rank an organization's practices and standards against industry best practices and standards from a maturity perspective.
- It can be used to help guide the organization to improve the overall information security posture.
- The long range plan should be to implement the policies, practices and processes to arrive at a ranking of 5 – Optimized.

Final Thoughts

Practical Realities

- Senior management commitment is critical

  … without it there is little acceptance and funding for the program
- The risk profile is unique for each organization (e.g. country, regulatory environment, industry, organizational culture and risk appetite) and continuously changes

  … so is the security program
- Develop a business aligned security vision, strategy and roadmap

  … this helps to communicate direction and set priorities
- Demonstrate value to your "customers" through enablement

  … through enablement, service-orientation and small/quick wins
- Security is a broad domain and no-one knows it all

  … leverage other resources to compliment your strengths