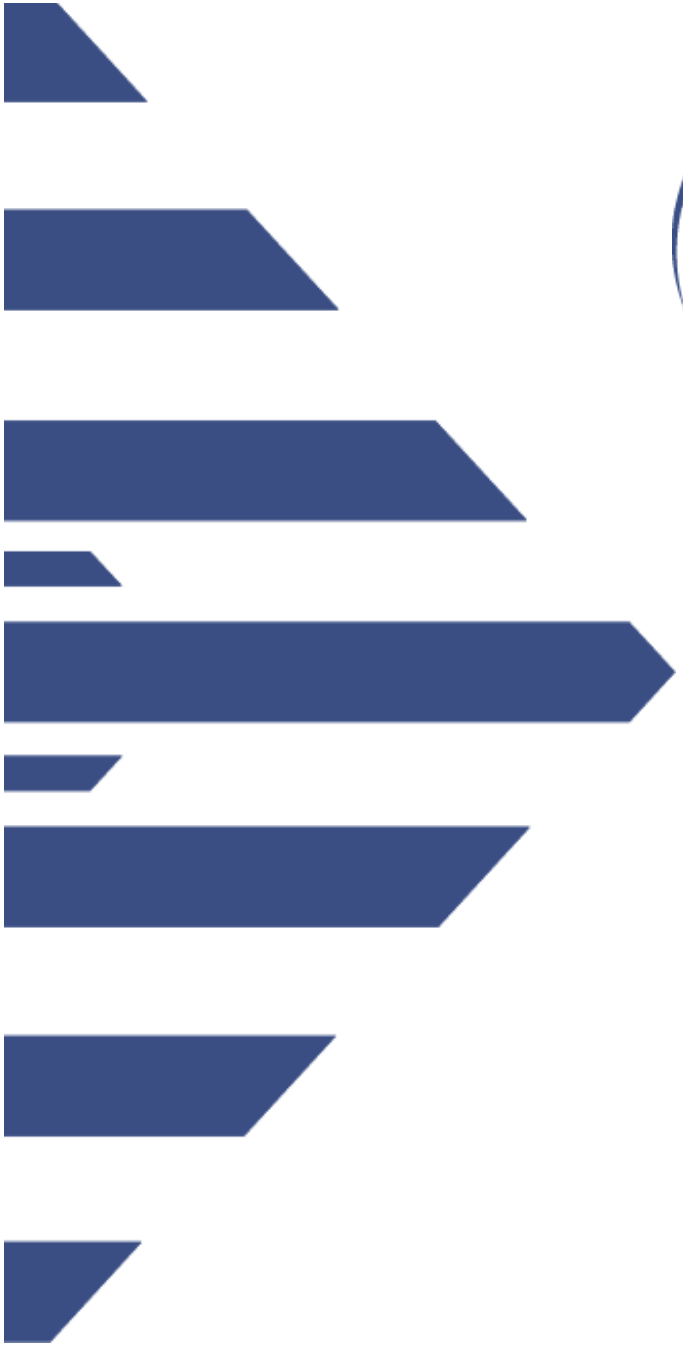


The Art of Information Security Governance

Qatar Information Security Forum
24 February 2008

Julia H. Allen

Agenda

The Risks

Governance Defined

Implementing Security Governance

Process Maturity

Prioritizing Security Investments

Questions To Ask

Agenda

The Risks

Governance Defined

Implementing Security Governance

Process Maturity

Prioritizing Security Investments

Questions To Ask

Recent Security Breaches

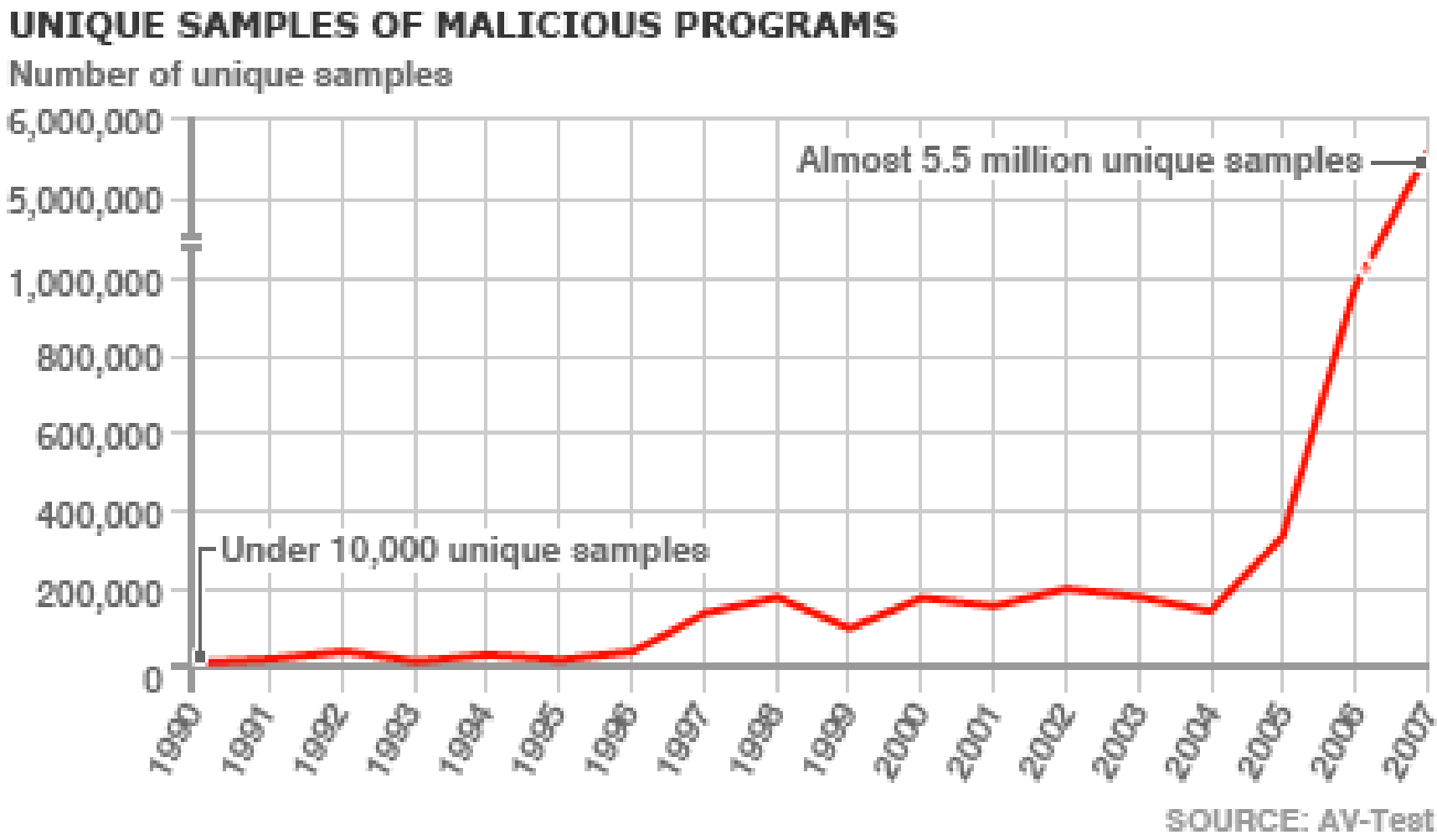
Societe Generale insider fraud (January 2008)

- Separation of duties
- Password controls
- Transaction tracking to individual workstations (and monitoring)

Middle east Internet outage (business continuity, operational resilience) (January 2008)

UK HM Revenue & Customs security breach due to loss of 25M child benefit records (HMRC chairman resignation) (October 2007)

Malicious Software on the Rise



http://news.bbc.co.uk/1/hi/technology/7232752.stm

What Is At Risk?

- Trust
- Reputation, brand, image
- Competitive advantage; market & investor confidence
- Ethics and duty of care
- Relationships with business partners
- Customer retention & growth
- Business continuity & resilience
  - Ability to offer, fulfill transactions

ITU Perspective

"Gaps in access to, and the use of, ICT do not only hinder countries' socio-economic development, but can also diminish the effectiveness of cooperation in building confidence and security in the use of ICT and promoting a global culture of cybersecurity.

Our developing and least developed countries are increasingly at risk."

Sami Al Basheer Al Morshid

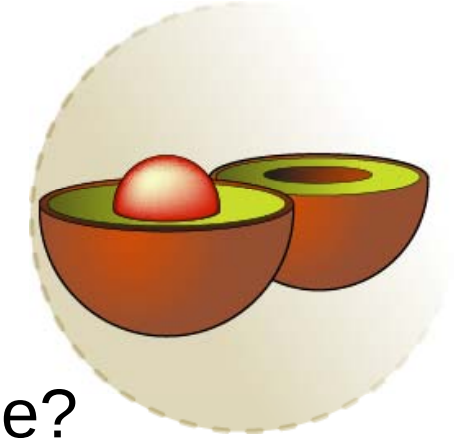
Director, ITU Telecommunication Development Bureau

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/cybersecurity-watch-september-2007.pdf

Operational Risk – Core Concerns

Are you confident that your security program is sufficient to protect against

- failed internal processes?
- inadvertent or deliberate actions of people?
- problems with systems and technology?
- external events?



Are your business continuity plans sufficient?

According to Basel II, operational risks are risks of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

http://www.bis.org/publ/bcbs107.htm

A Resilient Business Is Able To. . .

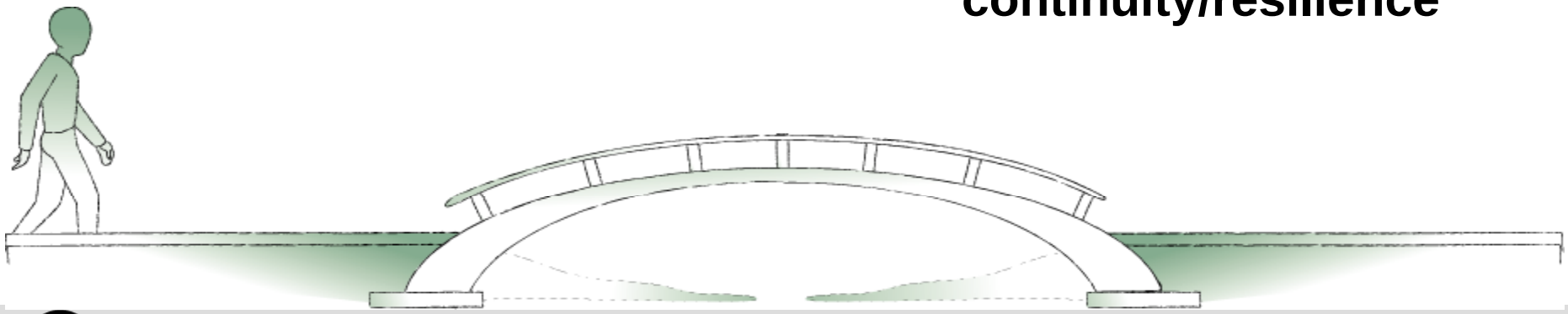
- withstand disruptions and adapt to new risk environments [1]
- be sensing, agile, networked, prepared [1]
- dynamically reinvent business models and strategies as circumstances change [2]
- have the capacity to change before the case for change becomes desperately obvious [2]
- sustain the mission in the face of operational risks

[1] "Enterprise Resilience: Managing Risk in the Networked Economy" by Randy Starr, Jim Newfrock, and Michael Delurey, strategy + business Reader, issue 30, Booz-Allen.

[2] "The Quest for Resilience" by Gary Hamel and Lisa Valinkangas, Harvard Business Review, September 2003.

Shift the Security Perspective

	From	*To*
Scope:	**Technical problem**	**Business problem**
Ownership:	**IT**	**Business**
Costs:	**Expense**	**Investment**
Execution:	**Intermittent**	**Integrated, continuous**
Approach:	**Practice-based**	**Process-based**
Objective:	**IT security**	**Business continuity/resilience**



Agenda

The Risks

Governance Defined

Implementing Security Governance

Process Maturity

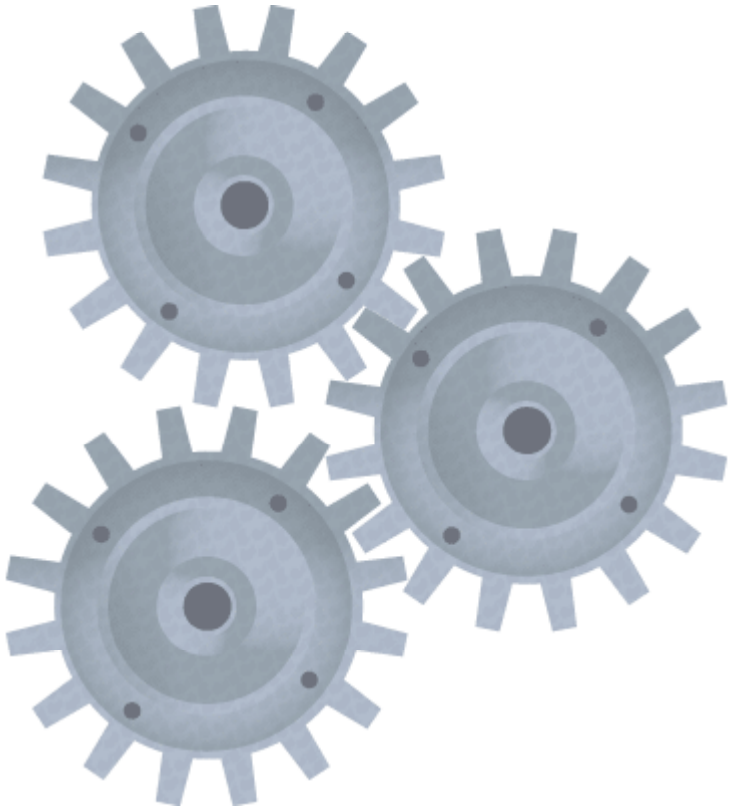
Prioritizing Security Investments

Questions To Ask

Governance Defined

Senior leader responsibilities

- Provide strategic direction
- Ensure objectives are achieved
- Ascertain that risks are managed appropriately
- Verify that resources are used responsibly



International Federation of Accountants. *Enterprise Governance: Getting the Balance Right*, 2004. http://www.ifac.org/Members/DownLoads/EnterpriseGovernance.pdf

Information Security Governance Defined - 1

Directing and controlling an organization to establish and sustain a culture of security in the organization's conduct (beliefs, behaviors, capabilities, and actions)

Information security governance means viewing adequate security as a non-negotiable requirement of being in business.

Allen, Julia. *Governing for Enterprise Security* (CMU/SEI-TN-023), June 2005. http://www.cert.org/governance.

Information Security Governance Defined - 2

. . . the process of establishing and maintaining a *framework* and supporting *management structure and processes* to provide assurance that information security strategies

- are aligned with and support business objectives
- adhere to policies, standards, and internal controls
- provide assignment of authority and responsibility

all in an effort to manage risk.

Bowen, Pauline, et al. *Information Security Handbook: A Guide for Managers* (NIST Special Publication 800-100), October 2006. http://csrc.nist.gov/publications/nistpubs/index.html.

Characteristics of Effective Security Governance - 1

Managed as a business-wide issue

- Horizontally, vertically, cross-functionally

Leaders are accountable

- Visible, own their risks, conduct regular reviews

Viewed as business requirement

- Aligns with business objectives and policies

Risk-based

- Reputational, operational, financial
- Tolerances established and reviewed

Roles & responsibilities defined

- Clear segregation of duties

Characteristics of Effective Security Governance – 2

Addressed & enforced in policy

Adequate resources committed

- Includes authority to act, time to maintain competence

Staff aware & trained

- Awareness, motivation, compliance expected

Addressed throughout system development life cycle

- Acquisition -> retirement

Planned, managed, & measured

- Part of strategic, capital, operational planning & review cycles

Reviewed & audited by oversight committees

- Desired state examined, sustained

Agenda

The Risks

Governance Defined

Implementing Security Governance

Process Maturity

Prioritizing Security Investments

Questions To Ask

Why a Framework for IS Governance?

Increasing operational risk exposure

Growing market demand for senior leadership attention and duty of care

Need for implementable guidance

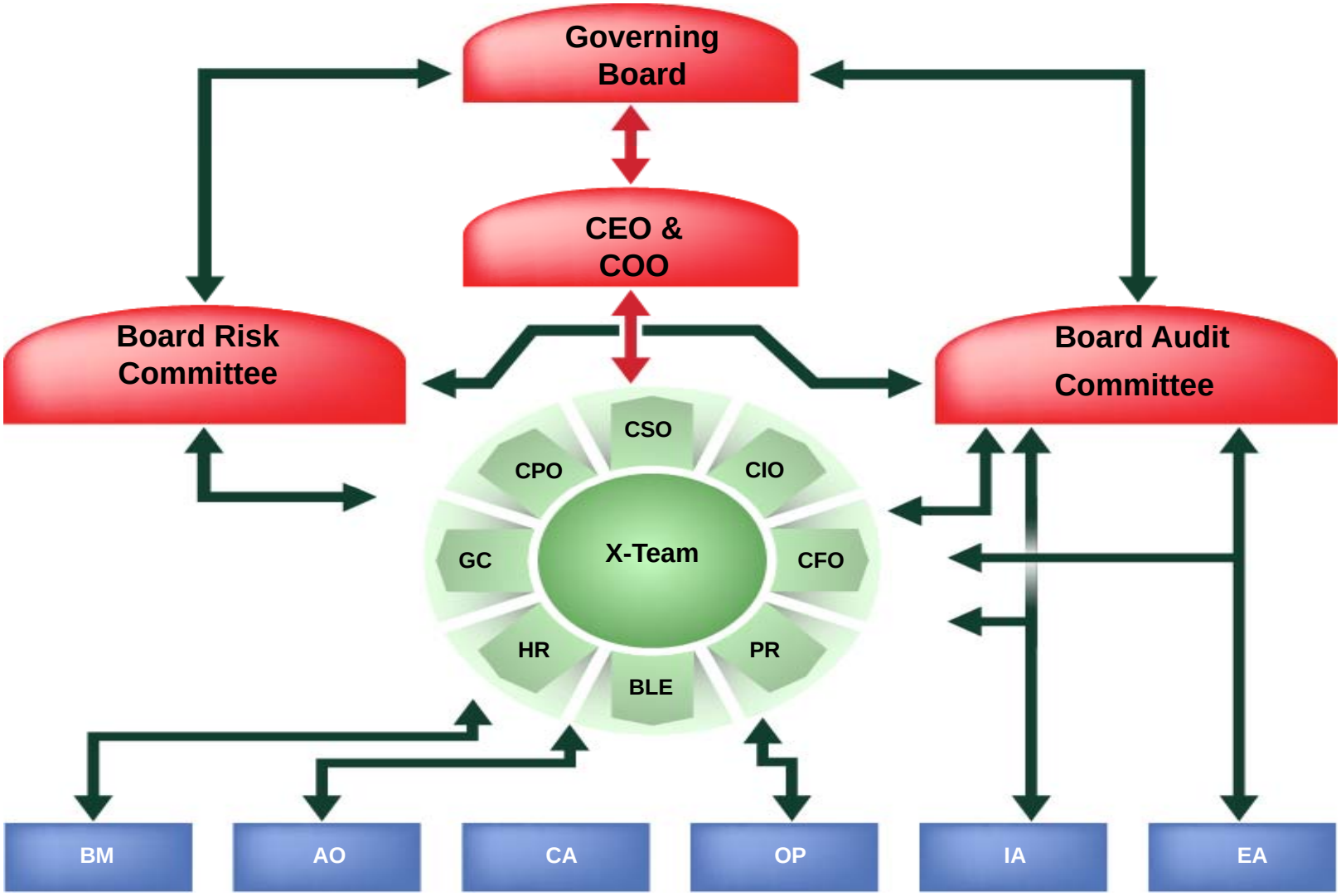
To define:

- A structure that engages the entire enterprise
- Clear roles, responsibilities & accountabilities
- Actionable steps and outcomes

http://www.cert.org/governance

Information Security Program

Governance Structure



Security Governance Key Roles

CEO	Chief executive officer
COO	Chief operating officer
C(I)SO	Chief (information) security officer
CIO	Chief information officer
CFO	Chief financial officer
CPO	Chief privacy officer
GC	General counsel
BLE	Business line executives
HR	VP, human resources
PR	VP, public relations

Security Governance Supporting Roles

BM	Business Manager (reports to BLE)
AO	Asset Owner
CA	Certification Agent
OP	Operational Personnel
IA	Internal Audit
EA	External Audit

Board Risk Committee

Mission

- Protect shareholder/stakeholder investment
- Protect assets, people, processes, products, reputation from risk

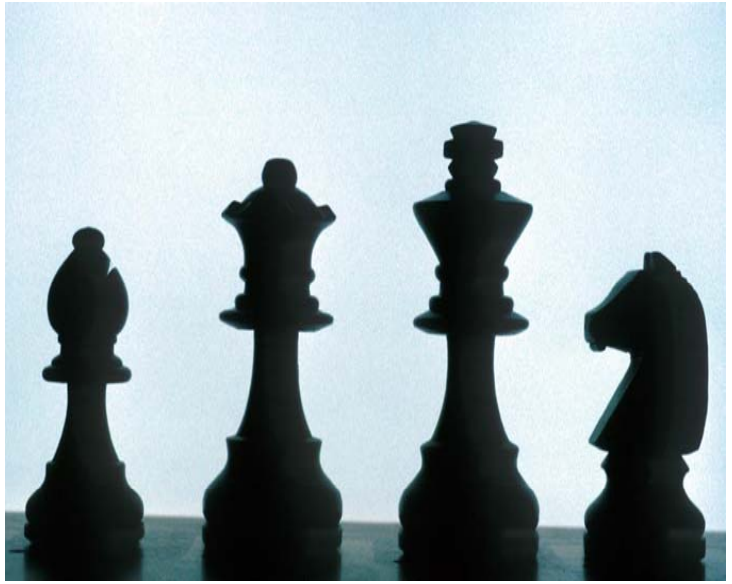
Objectives

- Establish IS Program governance structure; allocate responsibilities; oversee security
- Set cultural and managerial tone
- Determine risk thresholds/tolerances

Cross-Organizational Team (X-team)

Mission

- Develop and coordinate the security program
- Coordinate and respond to security risks and incidents



Objectives

- Ensure security risks are addressed
- Ensure that the security program is integrated with day-to-day business
- Manage the security of digital assets in accordance with plans and strategies

IS Governance Implementation Framework

Ordered Categories and Activities

- Governance
- Integration
- Implementation
- Capital Planning, Reviews, & Audits

Activities are repeated at designated intervals

Some activities are continuous, ongoing

Governance Activities

Establish organization structure

- Assign roles & responsibilities
- Ensure segregation of duties

Develop top-level policies

Inventory information assets

- Establish ownership & custody

Determine standards/compliance requirements

- Address cross border data flows & privacy

Result = Information Security Strategy

Integration Activities

Categorize assets

- Level of risk & magnitude of harm

Conduct risk assessments

Select security controls & key performance indicators

- Draw from standards & best practices

Develop supporting plans & requirements

- Incident response, crisis communications, business continuity, disaster recovery, service provider reqmts.

Result = Information Security Plan

Implementation Activities

Develop & execute security implementation & training plans

Enforce policies

Test controls (take corrective action when necessary)

Result = Implemented IS Plan

Capital Planning, Reviews, Audits

Determine security business case, ROI, & funding

Conduct formal reviews of the IS program

Conduct formal audits of the IS program

Result:

- A sustainable IS program
- Confidence that the IS program ensures an adequate level of security

Agenda

The Risks

Governance Defined

Implementing Security Governance

Process Maturity

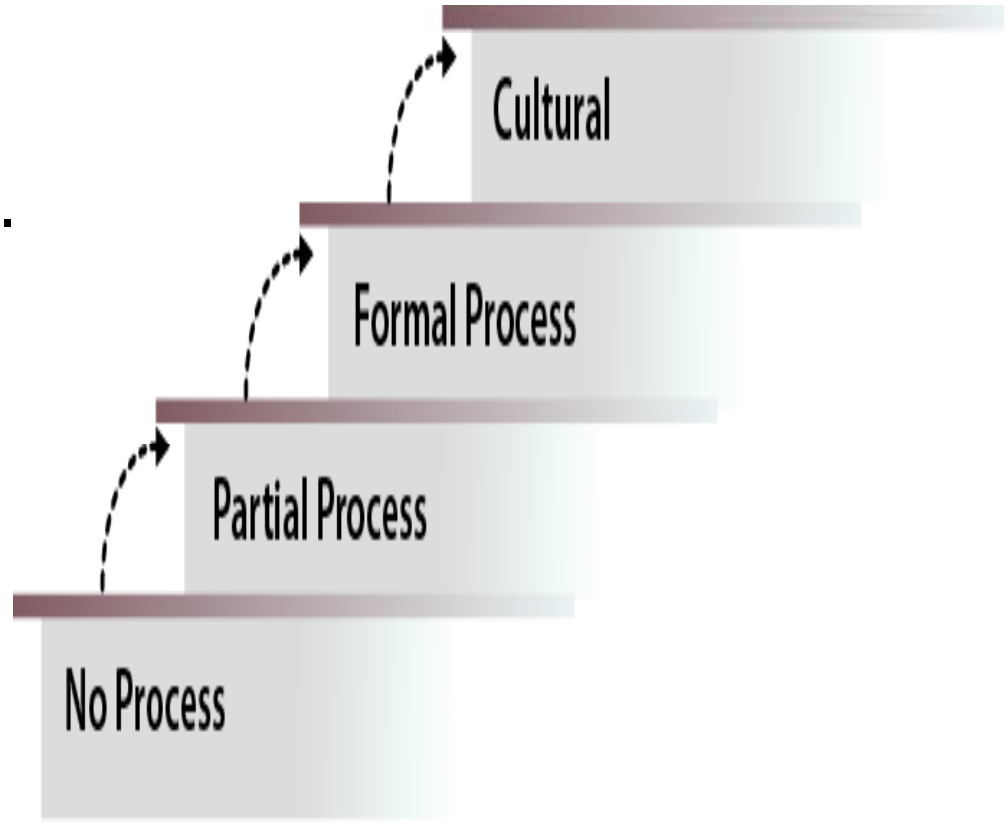
Prioritizing Security Investments

Questions To Ask

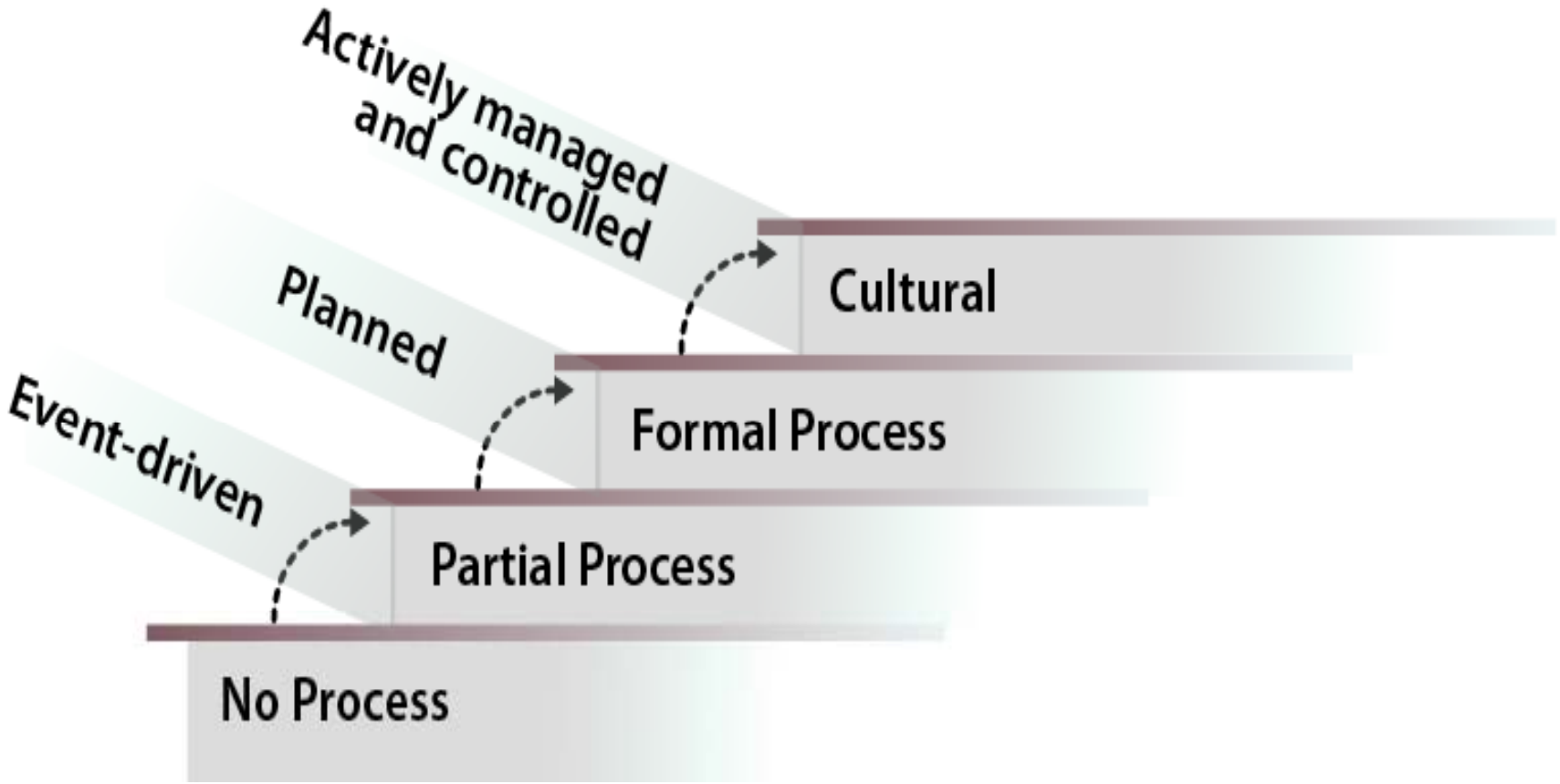
How Mature Are Your Processes?

Most organizations have some process for governing operational risk (including security).

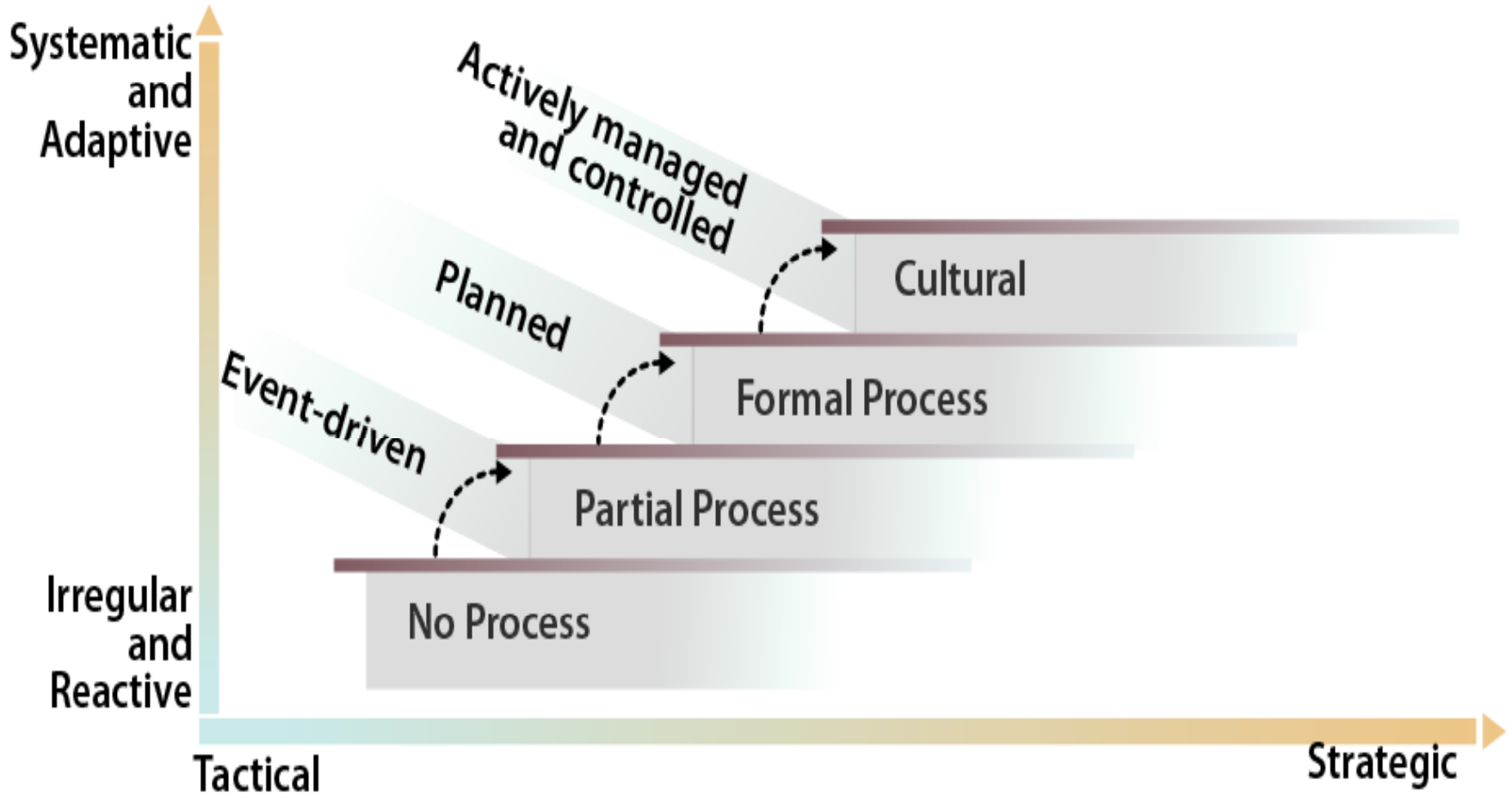
Processes may not be effective for meeting business goals.



Increasing Levels of Competency



Toward Continuous Improvement



Competitive Maturity Assessment: Best-in-Class - 1

70%: established, consistent security policies

70%: executive as primary owner for security governance & risk management

78%: leaders regularly informed of IT-dependent risks

67%: controls implemented for monitoring policy requirements & ensuring they are satisfied

67%: all information for audit & reporting identified

Aberdeen Group. “Security Governance and Risk Management: The Rewards of Doing the Right Things and Doing Things Right.” November 2007. Survey of 140 organizations, range of roles, market sectors, countries.

Competitive Maturity Assessment: Best-in-Class - 2

Compared to one year ago:

63%: reduced the number of actual security incidents

70%: reduced the average time to address incidents

48%: reduced the total cost to address incidents

74%: reduced audit failures (instances of non-compliance)

Agenda

The Risks

Governance Defined

Implementing Security Governance

Process Maturity

Prioritizing Security Investments

Questions To Ask

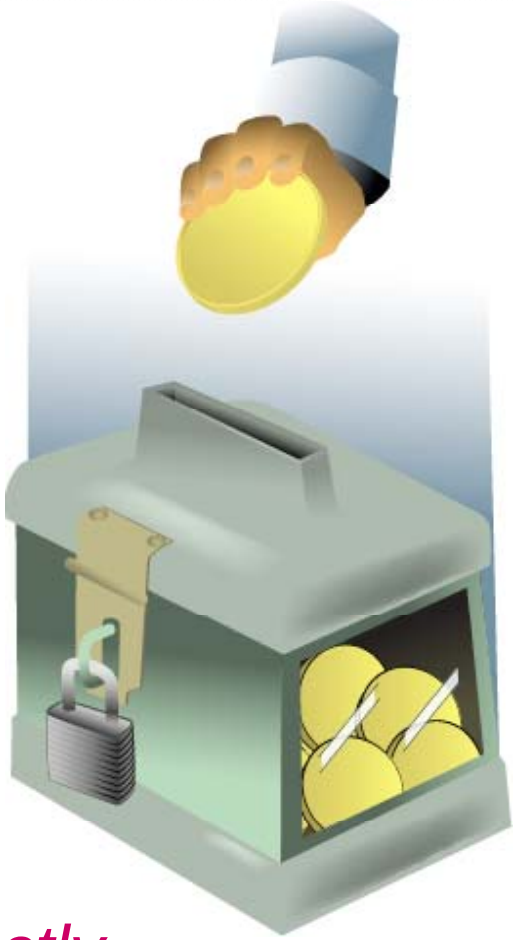
Prioritizing Security Investments

Make security investment decisions in the same fashion as other business investment decisions

Use business-based criteria

Engage leaders in establishing criteria priorities

Track performance & regularly report results



Ensure that investments in security directly support business objectives.

Decision Categories - 1

Cost: What is the estimated total cost to accomplish this task? (initial, life cycle, cost of not doing, savings)

Criticality & Risk: Degree to which investment in meeting business objectives & risk management goals (mainstream, degree of risk mitigated)

Decision Categories - 2

Feasibility: Likelihood of investment success (first attempt, subsequent attempts, leadership turnover, roll back)

Positive Interdependencies: Reasonable changes to existing processes? Pave the way for future work? (ability to accomplish other tasks, use existing performance measures, use existing knowledge & skills)

Decision Categories - 3

Involvement: Level of required involvement and buy-in (narrow, broad, third parties, review, audit)

Measurability: How measurable is the investment outcome? (tangible, intangible)

Time & Effort Required: Level of staff hours & time to break even (senior leadership time, buy-in time, demonstration of results, breakeven)

Agenda

The Risks

Governance Defined

Implementing Security Governance

Process Maturity

Prioritizing Security Investments

Questions To Ask

Security Strategy Questions

What needs to be protected? Why does it need to be protected? What happens if it is not protected?

What potential adverse consequences need to be prevented? At what cost? How much disruption can we stand before we take action?

How do we determine and effectively manage the residual risk?

Key Questions Senior Leaders Should Ask

Have we identified our critical information assets?

Do we conduct periodic risk assessments?

Do our written security plans & policies address these risks?

Have we implemented our security program? Do we monitor it? Do we regularly reassess it?

Have we addressed employee training issues?

Have we addressed information security for our service providers?

Are we prepared for a security breach?

Do we view security as part of our day-to-day business?

Smedinghoff, Thomas J. “Director Responsibilities for Data Security: Key Questions the Board Should Ask.” NACD Directors Monthly, April 2007.

Closing Thoughts

Because of its potential impact to business reputation, trust relationships, competitive advantage, and the confidence of investors and global trading partners, information security is no longer the sole province of the IT department.

Security is becoming a core competency for senior leaders, who need to ensure business resilience and continuity despite all kinds of threats.

Security is a business operation that should be run like a business operation. [3]

[3] Lindstrom, Pete. “Metrics: Practical Ways to Measure Security Success.” Spire Security, LLC, 2005. http://searchsecurity.techtarget.com/searchSecurity/downloads/EDITED_LINDSTROM_METRICS.pdf

For More Information

Governing for Enterprise Security:
www.cert.org/governance

Resiliency Engineering:
www.cert.org/resiliency_engineering

CERT Podcast Series: Security for Business Leaders: www.cert.org/podcast

Q-CERT: www.qcert.org

ITU: www.itu.int/cybersecurity/

Julia Allen: jha@cert.org