Information Security

Yulia Cherdantseva

Cardiff University

y.v.cherdantseva@cs.cardiff.ac.uk

Outline

- Importance of Information Security (InfoSec)
- Brief History
- InfoSec as an Integral Part of Corporate Governance
- InfoSec as a multidimensional discipline
- The Business Model for Information Security (BMIS)
- Case-study and Discussion

Importance of InfoSec

- Information is recognised as a key asset by many organisations
- The growing dependence of organisations on IT infrastructure
- The impact of security breaches today have more tangible, often the devastating effect on business
- The average cost of the worst security incident in large companies increased from £170,000 (2008) to £690,000 (2010)

The Early Years of Computer Security

The main focus of Computer Security, a predecessor of InfoSec, was Reliability of rare and high-priced machines.

In the 1970s the shift in the focus from protection of computers to protection of information marked the emergence of InfoSec.

THE CIA-TRIAD

Goals:

- unauthorised information release (Confidentiality);
- unauthorised information modification (Integrity)
- unauthorised denial of use (Availability).

- The CIA-triad was not intended to be a precise and comprehensive definition of InfoSec.
- The definition was intended to convey the overarching goals of InfoSec to business and engineering management in a terminology that will be easy to understand.

Information Security as an Integral Part of Corporate Governance

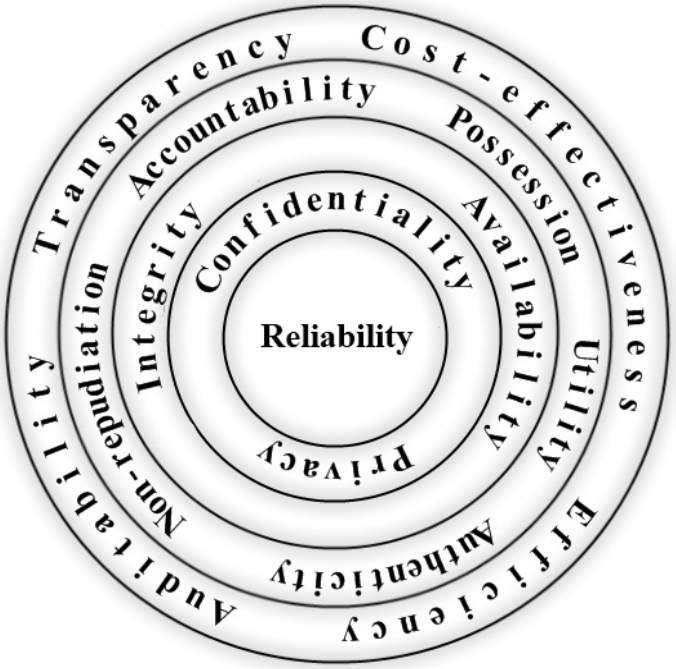
- ✓ the Turnbull Guidance
- ✓ the American Institute of Certified Public Accountants (AICIPA) standards
- ✓ the King report on Corporate Governance
- ✓ the OECD Principles of Corporate Governance
- ✓ the 8th audit directive of the European Union
- ✓ the Sarbanes-Oxley Act

- InfoSec was previously deemed to be low level activities and the responsibility of the technical personnel
- The documents attracted the managers' attention to risk management, the effectiveness of internal controls and to InfoSec in general

INFORMATION SECURITY AS AN INTEGRAL PART OF CORPORATE GOVERNANCE

- The ultimate goal of Corporate Governance is effective and secure business performance.
- InfoSec no longer puts the main emphasis on Confidentiality.
- Validity (as conformance to reality), Completeness and Accuracy of information become essential.
- The business needs give rise to additional security goals: Transparency and Auditability.
- Efficiency and Cost-effectiveness of security measures - became new, additional goals of InfoSec.

The broader scope of InfoSec



THE TRANSITION OF INFOSEC FROM A PURELY TECHNICAL TO THE MULTIDIMENSIONAL DISCIPLINE

- The Strategic/Corporate Governance Dimension;
- The Governance/Organisational Dimension;
- The Policy Dimension;
- The Best Practice Dimension;
- The Ethical Dimension;
- The Certification Dimension;
- The Legal Dimension;
- The Insurance Dimension;
- The Personnel/Human Dimension;
- The Awareness Dimension;
- The Technical Dimension;
- The Measurement/Metrics (Compliance monitoring/ Real time IT audit) Dimension;
- The Audit Dimension.

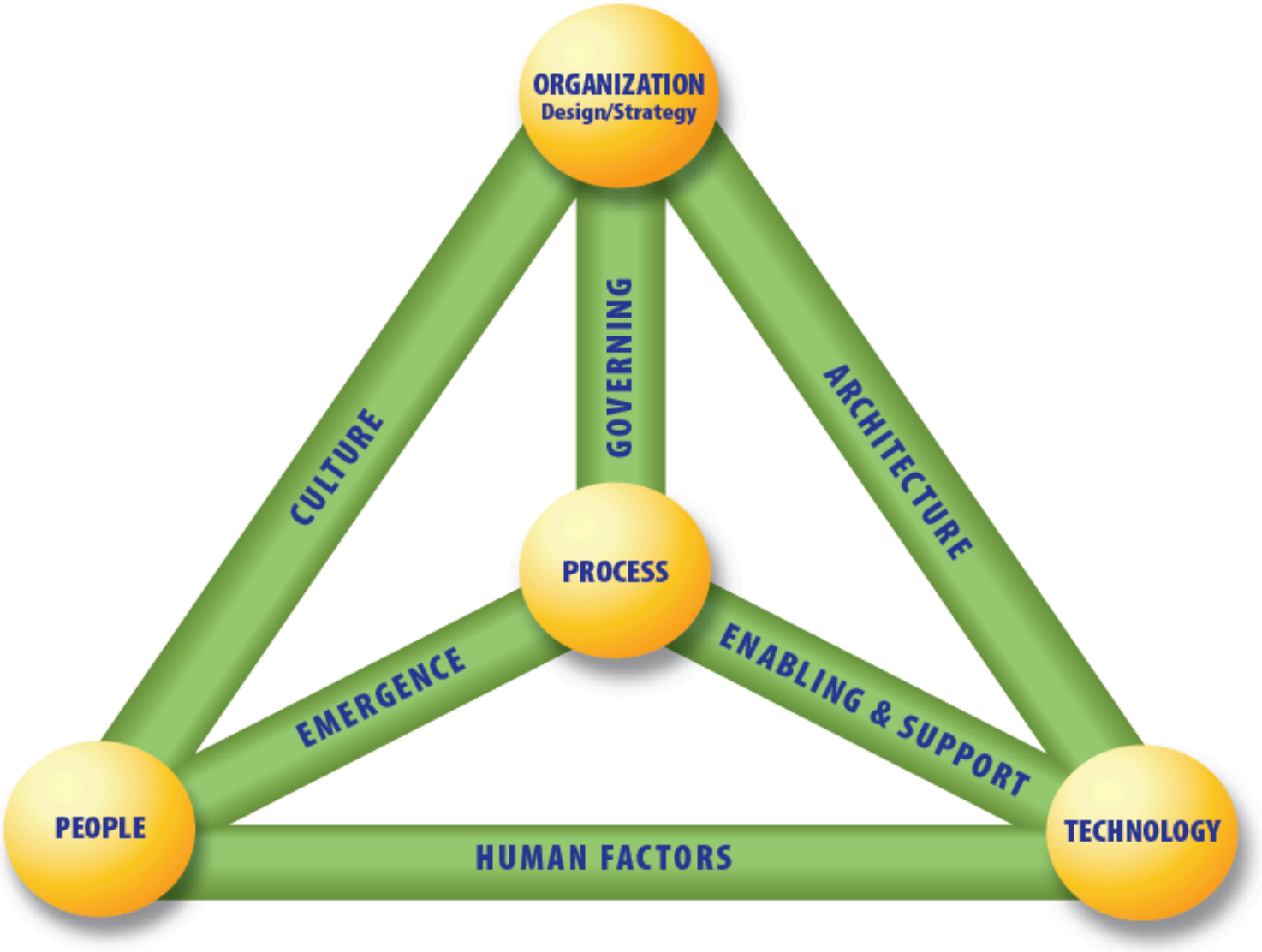
A PARADIGM SHIFT IN INFOSEC TOWARDS A COHERENT APPROACH TO INFORMATION PROTECTION

Technology alone is insufficient for solving complex tasks of InfoSec.

Business needs, the human factor, economic incentives and organisational aspects should be taken into account in order to achieve an adequate protection of information.

A comprehensive, multidimensional approach to the protection of information is required.

Business Model for Information Security (BMIS)



BMIS EXPLOITS SYSTEMS THINKING

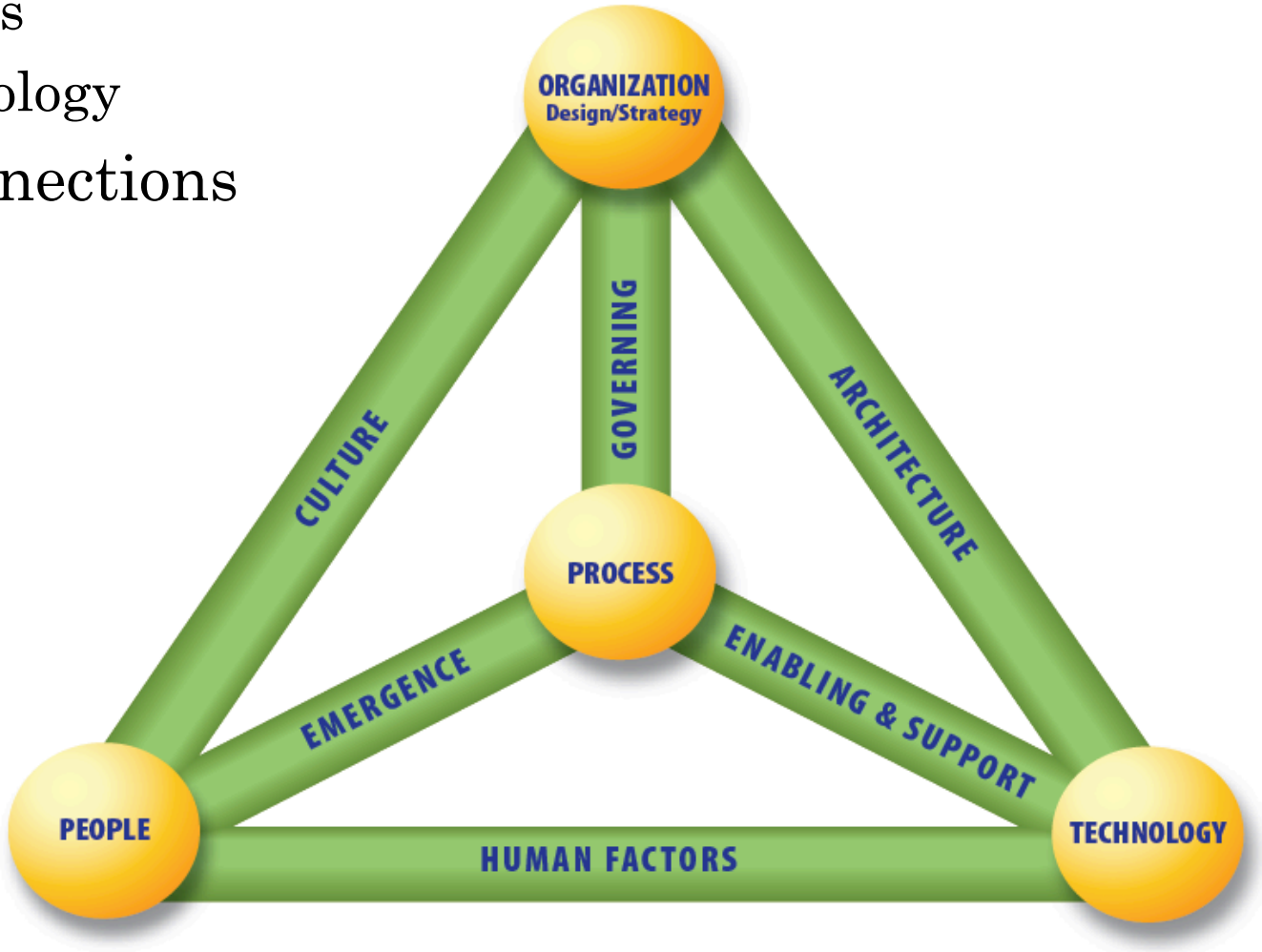
- The essence of systems theory is that a system needs to be viewed holistically —not merely as a sum of its parts—to be accurately understood.
- A holistic approach examines the system as a complete functioning unit.
- Looking at information security in pieces (people, process, technology) has not proven to be an effective method to manage a security program.

The BMIS

- The model takes a business-oriented, holistic and dynamic approach to managing information security.
- The model can be used regardless of the size of the enterprise or the information security framework.
- The model is independent of any particular technology or technological changes over time.

Structure of the Model

- 4 elements
  1. Organization Design and Strategy
  2. People
  3. Process
  4. Technology
- 6 interconnections



Four Elements of the Model

1. Organization Design and Strategy

An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued.

Design defines how the organization implements its strategy. Processes, culture and architecture are important to determining the design.

Four Elements of the Model

2. People

The people element represents the human resources and the security issues that surround them.

- Recruitment strategies (access, background checks, interviews, roles and responsibilities)
- Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)
- Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees)

Four Elements of the Model

3. **Process**

Process includes formal and informal mechanisms (large and small, simple and complex) to get things done.

4. **Technology**

The technology element is composed of all of the tools, applications and infrastructure that make processes more efficient.

The Intentional Information Security Culture

- Awareness campaigns
- Cross-functional teams
- Management commitment

Important characteristics:

1. Alignment of information security and business objectives
2. A risk-based approach
3. Balance among organization, people, process and technology
4. Allowance for the convergence of security strategies

CASE STUDY

In early 2005, the sales division of a Fortune 50 company was experiencing significantly declining sales. While the sales division believed it was due to increased market competition and pricing pressures from their customers, the security group believed that lack of proper security procedures was contributing to the decline. As specific factors in the decline, they named the loss of proprietary data by traveling sales personnel, vulnerable network security systems and procedures, and a refusal by the sales force to adhere to corporate security guidelines and policies. There was a fundamental lack of alignment between the security function and the line sales force with regard to people, processes, organization and technology, and it was inhibiting the ability of the company to meet its sales and corporate goals.

During this time, the company decided to enhance the role of the chief security officer (CSO) to accommodate the changing demands of its customers and the global security challenges facing the enterprise. Around the same time, the global head of sales was replaced and a new executive with a broader perspective of the company's challenges was promoted from within to take over the sales function. The CSO knew that there were significant issues within the sales group but had not been able to initiate any change due to its past leadership and culture. As part of the process for improving the security of critical sales and marketing information within the corporation, the new head of sales and the CSO jointly agreed to sponsor the implementation of the Business Model for Information Security.

QUESTIONS FOR DISCUSSION

- The goal is to create a mind shift within the sales organization with regard to technology, process, people and organization—a shift from a functional security culture to an intentional security culture. Describe the intentional security culture. Fill in the right column of the table in Figure 2

- The challenge would be to effectively instill an intentional security culture within a sales organization that did not view security as necessary to their jobs. Think about actions that should be undertaken to instill an intentional security culture.

Figure 2—Shifting From Functional to Intentional Security Culture	
From	**To**
Move Technology	
• Unsure about the level of security the technology provides • Seeing security-related technology as disruptive and cumbersome to use	
Move Process	
• Security brought in when there is a suspected breach • Security maintains expert knowledge.	
Move People	
• Security as an entity that enforces compliance • Security as a functional expert	
Move Enterprise	
• Limited visibility or awareness of security issues • Security structure focused on technical expertise	