CM2206
Business Strategy and Information Systems. Week 9

An Introduction to the Business Model for Information Security

Yulia Cherdantseva, COMSC, Cardiff University

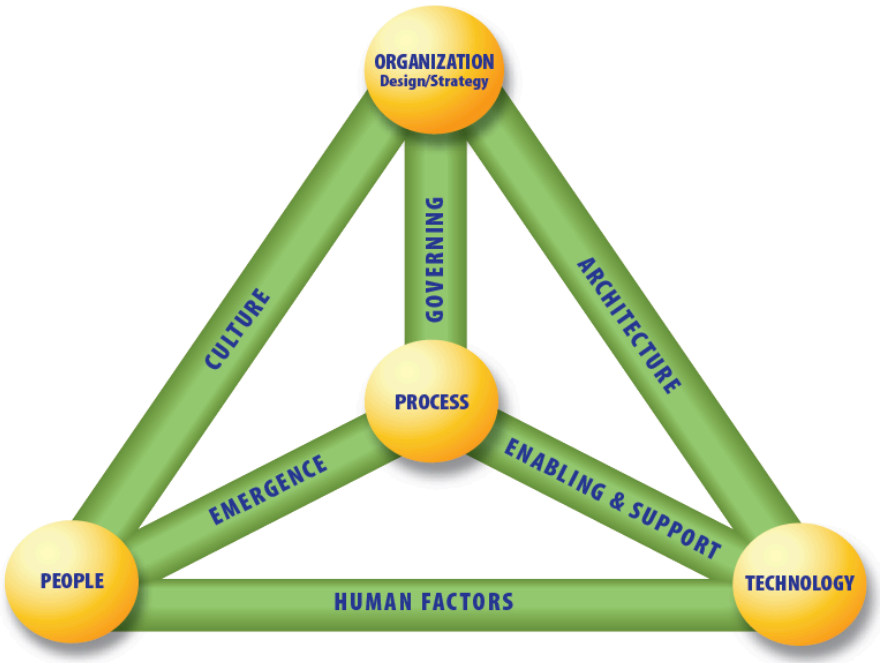
The Model

The Business Model for Information Security (BMIS) began life as a model for systemic security management, created by Dr. Laree Kiely and Terry Benzel at the USC Marshall School of Business Institute for Critical Information Infrastructure Protection. In 2008 ISACA acquired from the university the rights to develop the model to help embed its concepts in information security practices globally.
The BMIS exploits system thinking in order to structure the complex and dynamic field of information security. The model promotes a holistic, dynamic, business-oriented approach to information security which includes consideration of the interactions within the system, understanding the hidden conceptual problems and finding the best possible solutions.

Structure of the Model

As illustrated in figure 1, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections. All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

Figure 1—The Business Model for Information Security



Source: Adapted from the USC Marshall School of Business Institute for Critical Information Infrastructure Protection

The Elements

The four elements of the model are:
1. Organization Design and Strategy -An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal. An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how). Design defines how the organization implements its strategy. Processes, culture and architecture are important to determining the design.

2. People -The people element represents the human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases. Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:
• 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)
Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.

3. Process - Process includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections. Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.
To be advantageous to the enterprise, processes must:
• Meet business requirements and align with policy
• Consider emergence and be adaptable to changing requirements
• Be well documented and communicated to appropriate human resources
• Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. Technology -The technology element is composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risks. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.
Technology is often seen by the enterprise's management team as a way to resolve security threats and risks. While technical controls are helpful in mitigating some types of risks, technology should not be viewed as an information security solution.
Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology, some have not learned to use it and others feel it slows them down. Regardless of the reason, information security managers must be aware that many people will try to sidestep technical controls.

The Intentional Information Security Culture

A critical piece of the model that differentiates it from many others is the importance it places on organizational culture. Creating an intentional security culture is a primary objective for the model, as applied to information security. To create this intentional culture many things need to be instituted:

- **Awareness campaigns—**Campaigns can consist of general information security awareness activities and targeted educational sessions for specific audiences. These sessions are good opportunities to begin to inform departments of their information security responsibilities. The human resources function may be responsible for initial awareness training for new employees; that training should incorporate material that demonstrates security's importance to the enterprise.

- **Cross-functional teams—**Risk councils and security steering committees are examples of different functional areas working together to improve the enterprise's overall security posture. These are not the only examples: the human resources function is heavily involved in entrance and exit policies, and business owners need to be involved with management of their data. The use of cross-functional teams encourages communication and collaboration and reduces departmental isolation and duplicated efforts—in turn, reducing costs and improving profitability.

- **Management commitment—**As noted previously, one of the unique attributes of this model is its focus on organizational culture. Culture constitutes the reasoning behind the method by which things get done. If the senior management team does not genuinely support the information security program, it can discourage any other employee's sense of obligation or responsibility to the program. Therefore, it is critical for the enterprise's senior management team—including the board of directors and all executives—to accept ownership for information security and genuinely support the program.

The intentional information security culture focuses on the enterprise's governance needs. This type of culture has several important characteristics:

- Alignment of information security and business objectives
- A risk-based approach
- Balance among organization, people, process and technology
- 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

1. 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

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.

Additional information

1. Full description of The Business Model for Information Security (BMIS)
http://www.isaca.org/Knowledge-Center/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09-Research.pdf

2. The Evolution of Information Security Goals from the 1960s to today
http://users.cs.cf.ac.uk/Y.V.Cherdantseva/LectureEvolutionInfoSecGOALS.pdf

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	