Pilova D.
National Mining University

INSIGHTS INTO ENTERPRISE ECONOMIC SECURITY

Economic security has become one of the most urgent issues for many enterprises. It is an essential requirement for doing business in a globally economy and for achieving organizational goals and mission.

Security lives in an organizational and operational context, and thus cannot be managed effectively as a stand-alone discipline. Because security is a business problem, the organization must activate, coordinate, deploy, and direct many of its existing core competencies to work together to provide effective solutions. And to sustain success, economic security at an enterprise level requires that the organization move toward a economic security management process that is strategic, systematic, and repeatable—in other words, efficient at using security resources and effective at meeting security goals on a consistent basis. Managing for economic enterprise security defines a disciplined and structured means for realizing these objectives.

Thus, enterprise economic security is its ability to respond to the general influence of environment's threats with the use of corporate resources on the basis of acceptance of management decisions, which are adequate to the given conditions.

Most common threats of enterprise economic security are:

✓ customer data is compromised and it makes the headlines;

✓ enterprise's brand and reputation are negatively affected by a security breach, resulting in a loss of investor and consumer confidence and loyalty;

✓ sensitive intellectual property (such as trade secrets and new product information) is stolen by a competitor or made public;

✓ organization is found to be non-compliant with regulations (national, state, local) as they relate to the protection of information and information security;

✓ enterprise's network goes down because of a security breach and it's impossible to detect a security breach.

Increasingly, an organization's ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network connectivity and services. Having a reputation for safeguarding information and the environment within which it resides enhances an

organization’s ability to preserve and increase market share.

Establishing and maintaining confidence in an organization’s security and privacy posture increase the likelihood that customers will refer others to the products and services offered by the organization. In addition, being viewed as an ethical organization with a culture of doing the right things and doing things right (including security) has tangible value in the international marketplace, as does being able to reliably demonstrate compliance and duty of care with respect to applicable regulations and laws.

Enterprise risks include financial (including credit), legal and compliance, operational, market, strategic, information, technology, personnel, and reputation. Enterprise security risks that derive from these may include those that damage stakeholder trust and confidence, affect customer retention and growth, violate customer and partner identity and privacy, disrupt the ability to offer and fulfil business transactions, adversely affect health and cause loss of life, and adversely affect the operations of national critical infrastructures.

Enterprises might consider how investment in security can enable an organization to act on new opportunities to better achieve business objectives that may include:

- ✓ enabling new types of products and services;
- ✓ communicating with customers in a reliable, cost-effective, and timely manner;
- ✓ causing transactions to occur with greater integrity and privacy, thus ensuring business throughput, customer satisfaction, and customer confidence, which can all help create and sustain customer loyalty;
- ✓ enabling new types of customer/supplier engagement; interacting in a more timely and reliable way with the organization’s supply chain;
- ✓ providing more secure access by internal and external staff to enterprise applications.

Clearly an organization cannot protect and prevent everything. Interaction with key stakeholders is essential to determine the organization’s ability to tolerate risk and appetite to tolerate the impact if the risk is realized. In effect, security as a component of risk management involves a process of determining what could go wrong, the likelihood of such an event occurring, the impact if it did, and actions to mitigate or minimize both the likelihood and the impact to an acceptable level with an acceptable range of variation.

The answers to these questions can help organizations determine how much to invest, where to invest, and how fast to invest in economic security-governance actions. They serve as one means to identify security risks to the enterprise and quantify the degree of risk exposure. In the absence of answers to these questions (and a process for periodically reviewing and updating them), an organization may find it difficult to define and deploy an effective security strategy and thus unable to effectively govern for enterprise security.