Julia Isakova
I.M. Lisovenkova , research supervisor
O.V. Petrova, language adviser
SHEI “National Mining University”, Dnipropetrovsk

Organisation of Information Security at the Enterprise

In the last years information security has become a more important issue for most large companies around the world. These companies have also understood that better security cannot be achieved by just installing another security hardware device like a firewall or an intrusion detection system. Even the most secure system would not give you any security if the people operating it have the wrong attitudes and don’t behave, as they should. It is a common understanding that information security heavily depends on the behaviour of the employees. Some say information security consists of 20% technical concepts and 80% human behaviour; some say the ratio is 10/90. Many organizations find it difficult and costly to handle the information security in a proper way. The question is whether organizations are able to handle these challenges.

Three widely accepted elements of information security are:

- confidentiality - confidentiality is the term used to prevent disclosure of information to unauthorised individuals or systems.
- integrity - in information security, integrity means that data cannot be modified undetectably.
- availability - for any information system to serve its purpose, the information must be available when it is needed.

Most definitions of information security tend to focus, sometimes exclusively, on specific usages and, or, particular media; e.g., "protect electronic data from unauthorized use". In fact it is a common misconception, or misunderstanding, that information security is synonymous with computer security.

Without protecting an intellectual property, a firm loses its global competitive position and ability to ultimately survive.

Obviously, competitors always have the opportunity to "reverse-engineer" a company's existing products and services to understand how they work and how they differ from the competitor's own offerings.

Second, it is essential that companies' financial systems not be hacked. Unfortunately, it is often company employees who, in the absence of tamper-proof internal controls, are often doing the hacking.

Third, hacking into a firm's customer information, including personal information and accounts is, potentially, another huge exposure risk. With the digitization of almost every kind of information, broad-based information-security management is both very challenging and absolutely essential.

The consequences of a failure to protect all three of these aspects include business losses, legal liability, and loss of company goodwill.

Having a security program means that enterprise taken steps to mitigate the risk of losing data in any one of a variety of ways, and have defined a life cycle for managing the security of information and technology within organization.

Basic constituents of the organization of information security at the enterprise are:

- management commitment. Management at all levels should actively support security within the organization with clear direction, demonstrated commitment, and explicit acknowledgement of information security responsibilities.
- allocation of responsibilities. All information security responsibilities should be clearly defined. This could include: identification and clear definition of assets and associated security controls for each information facility; and identification of the individual or individuals responsible for security for each information facility.
- coordination of efforts. Information security activities should be coordinated by representatives from different parts of the organization with relevant security roles and job functions.
- authorization processes. A management authorization process for new information processing facilities and capabilities, or for significant changes to existing facilities and capabilities, should be defined and implemented.
- confidentiality and non-disclosure agreements. Requirements for confidentiality and non-disclosure agreements should reflect the organization's needs for protection of information. Such agreements should be periodically reviewed.
- contacts with authorities. Appropriate contacts with external authorities should be maintained. This could include: development of policies, procedures and contact lists that specify when and by whom external authorities should be contacted; contacts with special interest groups. contacts and contracts with external parties. Agreements with third parties that involve accessing, processing, communicating or managing the organization's information or information processing facilities should cover all relevant security requirements.
- contacts and contracts with customers. All identified security requirements should be addressed before giving customers access to the organization's information or assets. Control considerations are similar to those for other external parties.
- independent review of information security. The organization's approach to managing information security and its implementation should be reviewed independently at planned intervals, and when there are significant changes to internal structure or the external environment.

The organization’s administrative structure and its relationships with external parties should promote effective management of all aspects of information security. This includes maintaining the security of the organization's information, its information processing facilities, and any information or facilities that are accessed, processed, communicated to or managed by external parties.