The Challenge of Ensuring Business Security in Information Age

Marius PETRESCU[1]
Delia Mioara POPESCU
Nicoleta SÎRBU

Abstract

Every day, thousands of businesses rely on the services and information ensured by information and communication networks. As the dependence on information systems grows, so the security of information networks becomes ever more critical to any entity, no matter if it is a company or a public institution. The asymmetrical threat posed by cyber attacks and the inherent vulnerabilities of cyberspace constitute a serious security risk confronting all nations. For this reason, the cyber threats need to be addressed at the global level. Given the gravity of the threat and of the interests at stake, it is imperative that the comprehensive use of information technology solutions be supported by a high level of security measures and be embedded also in a broad and sophisticated cyber security culture.

This paper provides arguments regarding the need to implement coherent information security policies at national level, based on cooperation between public and private sectors and in coordination with international initiatives in the field. Since information security is vital for developing and running an efficient business, this study may constitute a strategic approach to improve the information security posture of Romanian organizations.

Keywords: *information security, information security risk management, security threats, confidentiality, integrity, availability*

JEL classification: D81, A12

1. Introduction

Information and communications technology has developed enormously in speed and capability over the past fifty years, dramatically altering the way people interact with each other and their environment. Except for isolated networks of extreme sensitivity, the need to interconnect and exchange information supersedes the need for security measures capable of repelling all attack. Arguably the most significant development that these advances have led to is the emergence, over the past two decades, of cyber space – the new domain of computer facilitated

[1] **Marius PETRESCU**, Valahia University, Târgovişte
Tel.: +4 0245206104, Fax : +4 0245206104
Delia Mioara POPESCU, Valahia University, Târgovişte
E-mail: depopescu@yahoo.com, Tel.: +4 0245206104, Fax : +4 0245206104
Nicoleta SÎRBU, Valahia University, Târgovişte
E-mail: nicoleta.sirbu@gmail.com, Tel.: +4 0245206104, Fax : +4 0245206104

communication that is essential for the economic, social and political health of advanced nations.

Developments in information and communication technology are gathering pace and so is the degree to which we utilize them. Businesses are increasingly interconnecting their own information systems in order to deliver more effective services to each other. Multi-national companies, such as telecommunications companies themselves, are consolidating critical parts of their organizations into countries where costs are low, relying on networks to connect back to their home-countries.

Critical national infrastructures – all the systems we rely on like utilities, food distribution, transport, the health service and the financial system – depend more and more on the Internet. National interests are becoming ever more reliant on all the components of cyber space and this dependence is one that is far-reaching, affecting the individual citizen, almost all aspects of government, industry, national infrastructure, transportation and the way economy operates.

The governments themselves are reliant on information and communication technology and, through programs such e-governance provides efficient services to the public. All of these activities rely on the Internet and exploit the benefits of cyber space – and more will follow. However, along with its incontestable advantages, information and communication technology raises a number of security challenges. These challenges are related on one hand to the threats posed by the cyber space and, on the other hand by vulnerabilities intrinsic related to the information and communication networks, as well as due to the human factor involved in the information processing cycle.

In this context, managers should be aware of just how critically dependent their business is on information and communication infrastructure and that the effective and secure functioning of cyber space is of vital importance. They should be aware of the need to implement appropriate security controls in order to ensure business continuity. What is important to underline is that a collective effort is necessary in order to create a secure information and communication environment. All players accessing the global information and communication infrastructure have to be aware of their responsibilities and have to play by the rules of information security, since the global security posture of an information and communication infrastructure is as strong as its weakest link. A general social awareness of threats in cyberspace and the state of readiness to meet them should be fostered, as important prerequisites for ensuring information security.

2. Business security is dependent on information security

The dependence of the daily functioning of society on information technology solutions makes the development of adequate security measures an urgent need.

Information and communication networks are increasingly intertwined in our current activities. Some of these information and communication systems, services, networks and infrastructures form a vital part of world's economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. For example, according to statistics in the UK, some 90 per cent of the high street purchases are transacted by plastic which depends on wired and wireless communication to work. That is in addition to £50 billion of consumer purchases and sales through e-commerce that takes place wholly online (Digital Britain, 2009). The information and communication networks are typically regarded as critical information infrastructures (Commission of the European Communities, 2009) as their disruption or destruction would have a serious impact on vital societal functions.

Information security is one of the important components of the security system for any organization and for this reason it must be considered an integral part of an organization management system. Information security is done using the main management mechanism for the organization's security and should consist of protecting both the inside information flow and the communication with outside entities in order to guarantee that the organization can reach its mission.

3. Understanding information security

Information security rests on confidentiality, integrity, and availability. The interpretations of these three aspects vary, as do the contexts in which they arise. The needs of the individuals, customs, and laws of the particular organization dictate the interpretation of an aspect in a given environment.

- Confidentiality. Confidentiality is the concealment of information or resources. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry.
- Integrity. Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication).
- Availability. Availability refers to the ability to use the information or resource desired. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable.

4. Typical threats related to information and communication networks

A threat is a potential violation of security. The violation need not actually occur for they're to be a threat. The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for).

Threats may be divided into four broad classes: disclosure, or unauthorized access to information; deception, or acceptance of false data; disruption, or interruption or prevention of correct operation; and usurpation, or unauthorized control of some part of a system.

These four broad classes encompass many common threats. The threats are ubiquitous, and they have to be well identified and quantified by security managers in order to be able to reduce their potential impact on affecting information security.

The main types of threats identified for information and communication networks during the recent years are:

- Snooping, the unauthorized interception of information is a form of disclosure. It is passive; suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information.
- Modification or alteration, an unauthorized change of information, covers three classes of threats. The goal may be deception, in which some entity relies on the modified data to determine which action to take, or in which incorrect information is accepted as correct and is released. If the modified data controls the operation of the system, the threats of disruption and usurpation arise.
- Masquerading or spoofing, an impersonation of one entity by another is a form of both deception and usurpation.
- Repudiation of origin, a false denial that an entity sent (or created) something, is a form of deception.
- Denial of receipt, a false denial that an entity received some information or message, is a form of deception. Integrity and availability mechanisms guard against these attacks.
- Delay, a temporary inhibition of a service, is a form of usurpation, although it can play a supporting role in deception.
- Denial of service, a long-term inhibition of service, is a form of usurpation, although it is often used with other mechanisms to deceive. The attacker prevents a server from providing a service.

Cyber-attacks have risen to an unprecedented level of sophistication. The recent large scale cyber-attacks on Estonia, Lithuania and Georgia are the most widely covered examples of a general trend (Ministry of Defense Estonia, 2008).

The World Economic Forum estimated in 2008 that there is a 10 to 20% probability of a major critical information infrastructures breakdown in the next 10 years, with a potential global economic cost of approximately 250 billion US$ (COM (2009) 149). In accordance with international statistics, the online fraud generated £52 billion worldwide in 2007 (UK Prime Minister, 2009).

According to 2008 CSI Computer Crime & Security Survey (Richardson R., 2008), the most expensive computer security incidents were those involving financial fraud with an average reported cost of close to US$ 500,000. Every information system owner must acknowledge the risks related to the disturbance of the service he provides. Up-to-date and economically expedient security measures must therefore be developed and implemented.

5. Management methods and techniques applied to ensure information security

In order to implement an efficient and effective information security system, managers should develop an information security risk management process. This process is essential in order to balance the risks to which the organization's information are exposed to, with the costs of the security measures. The main methods applied within the context of the information security risk management process are:

- Risk identification - Before risks can be managed, they must be identified. Identification surfaces risks before they become problems. Risk identification is achieved by employing different techniques, such as application of a systematic process that encourages project personnel to raise concerns and issues.
- Risk analysis - Analysis is the conversion of risk data into risk decision-making information. Techniques throughout which risk analysis may be carried out should be carefully selected and tailored according to organization's objectives and specific tasks. Thus, there are:
  - Quantitative techniques, which involve two main parameters: the probability for a negative event to occur and the potential losses. The problem with this technique is that the occurrence probability is difficult to be correctly estimated, so that the overall results obtained are not always exact. In addition, this technique treats discreet negative events, whereas most of the events are inter-related.
  - Qualitative techniques are based on an inter-related set of elements consisting of threats, vulnerabilities and security measures. These techniques are more frequently used, being more flexible to accommodate different types of environments.
- Planning - Planning turns risk information into decisions and actions. Planning involves developing actions to address individual risks, prioritizing risk actions, and creating an integrated risk management plan. The plan for a specific risk can involve various techniques (like mitigating the impact by a contingency plan, avoiding the risk, accepting risk and taking no further actions, studying about it to get more information etc). The key to risk action planning is to consider the future consequences of a decision made today.
- Tracking - Tracking consists of monitoring the status of risks and the actions taken to ameliorate them. Appropriate risk metrics are identified and monitored to enable the evaluation of the status of as well as of risk mitigation plans. Tracking serves as the "watchdog" function of management.
- Controlling - Risk control corrects deviations from planned risk actions.
- Communication - Risk communication is essential for the awareness consolidation of each member of the organization. Without this component, one cannot talk about a viable risk management process.

All methods and techniques that are part of the information security risk management are based on a team effort and close cooperation between specialists in different security field and managers.

Conclusions

Information and communication networks became an essential component of out daily activity and have a fundamental role in the future global development. As underlined before, cooperation between public and private sectors is essential in order to achieve efficiency in deterring cyber threats. The partnership works by exchanging information on cyber attacks, disaster recovery or physical attacks. The drivers for this information exchange are the benefits of members working together on common problems and gaining access to information which is not available from any other source, namely competitors and national security agencies (ENISA, 2009).

Organizations must lead a coherent response to the security challenges that arise from these threats and risks and a strategic approach is fundamental to achieving this aim. Government and businesses must work together to provide more secure products and services, to operate their information systems safely and to protect individuals' privacy.

REFERENCES

1. Commission of the European Communities, (2005). *Green Paper on a European Programme for Critical Infrastructure Protection*
2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure, (2009). *Protecting Europe From Large Scale Cyber-Attacks And Disruptions: Enhancing Preparedness, Security And Resilience,* (COM (2009) 149)
3. Digital Britain: The Final Report, (2009). (Cm 7650), available at http://www.official-documents.gov.uk/document/cm76/7650/7650.pdf
4. European Network and Security Information Agency, (2009). *Good Practice Guide, Network Security Information Exchanges*
5. Ministry of Defense Estonia, (2008). *Cyber Security Strategy*, Tallin
6. Rădoi, M. & Negrescu, I., (2010). *Pro CERT.RO*, Intelligence, Year 6, Number 17, martie - mai 2010, pp.40
7. Richardson R., (2008). *CSI Computer Crime & Security Survey*, available at http://cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf;
8. Sweden Emergency Management Agency, (2010). *Information Security in Sweden, Action Plan 2008-2010*
9. UK Prime Minister, (2009). *Cyber Security Strategy of the United Kingdom*, presented to the Parliament by the Prime Minister