

eBCM Assurance: **INFORMATION SECURITY, CYBER IDENTITY AND CREDIBILITY MANAGEMENT**

LEARNING OBJECT #08

SECURITY

BASIS FOR TRUST AND CONFIDENCE IN eBUSINESS

Outline

- Introduction
- Value of ICT assets
- Value of ICT security issues (confidentiality, integrity availability)
- Threats to ICT security
- Possible channels of intrusion
- Common tools to ensure ICT security
- How to behave securely

Introduction

Establishing the necessary trust and confidence between business partners is to a very large extent a subjective issue affected by the reputation and image of the organisations or enterprises in question. This refers to the overall perceived credibility, which is essential, both in the traditional business as well as in the business practices with strong ICT penetration and network visibility. Understanding of possible threats and common tools to ensure ICT security is important in order to have stable eBusiness environment. The task of this LO is to describe the value of ICT assets and most common ICT security issues.

eBusiness is essentially the implementation of business processes by using ICT tools and internet services (selling and purchasing goods via internet). In case of eBusiness, all business processes will operate via internet and in web environment. All business services have to be connected and available via internet for its users. Its good quality is availability of people and clarity of management. For analysing business processes it is recommended to document all procedures and retain the possibility of later recheck. There are possibilities to transfer all business processes to the internet-based environment: Communication and forums, e-mail, evaluation, stock, purchasing, document management, project management, program management etc.

Value of security

ICT tools have to enable access, availability, control and confidentiality of the data. For avoiding errors and updating the data there is need to synchronise data periodically. To ensure ICT security in an enterprise, the ICT security policy should be specified for the whole organisation. ICT security policy is a documentation that prescribes the management of ICT properties in the organisation and in its IT systems. ICT properties are:

- Data (information, knowledge)
- ICT devices: computers, hardware etc
- Data communication channels
- Software

ICT implementation and adoption

Implementing the ICT security policy requires systematic activities in the whole enterprise. Ensuring ICT security presumes cooperation of ICT specialists, ICT managers, business managers and financial managers.

When ensuring system security it is very important to choose appropriate ICT solutions (eBusiness is always based on information system). When selecting the ICT solution the following should be considered:

- Can the development of the system be continued in the future?
- What kind of solution is best for the enterprise?
- How much do all resources (hardware, software, installation, integration, trainings etc) cost?
- How to integrate the eBusiness system with existing software (are there different software platforms: for stock, sales, accounting etc)?
- Which are additional requirements for authentication, encryption, data security etc.?
- Modelling and programming information system should be performed with security in mind.

Value of ICT assets as business critical

A mission-critical system is any system whose reliable performance is crucial to the successful performance of the organisation in which it is used, e.g. the web server of an eShop organisation would be considered mission-critical whereas an occasionally-used word processor might not be critical.

Mostly, we can live with the errors that occur in computer systems. We can restart, work round the problem, or even stop awhile. Unfortunately, these responses are not always acceptable if the following apply:

- The failure endangers human lives.
- The failure causes great economic damage.
- The inability of the information system to function would be socially irresponsible.

The hallmark of this type of system is that the system's mission is the reason that the system was created. Failure of this type of system is unacceptable. Such systems are mission critical. It is possible to recognise the value of system if we ask following questions:

- What happens if the system doesn't work correctly for a 1 minute / 1 hour / 1 day / 1 week (the question is how fast the system has to be corrected so that nothing serious happens)?
- What happens if system data is lost?
- What happens if system data becomes publicly accessible?

If an organisation can make business but has only suffers some inconvenience for a limited period of time if previously described damages occurs, then the system is not mission critical. Also speed and accuracy of systems providing necessary information is essential for making good decisions.

Value of ICT security issues (confidentiality, integrity, availability)

An efficient business relationship rests on trust and confidence between business partners where information security assurance is a key element. This goes for any business and even more so when conducted on the Internet as eBusiness.

Confidentiality is essential, i.e. that not everyone can read everything e.g. eInvoices, terms of sales, prices etc.

Integrity is usually the most important issue in eBusiness security. It is needed to create trust. Integrity, in terms of network security, means that information can only be accessed or

modified by those authorized to do so. Data with integrity has not been altered or destroyed without such authorisation.

Good and adequate data needs to be always ready for use. The *availability* of data is, for example, dependent on the stability and the operable time of systems and the possibility to track electronic messages. It is trustworthy if companies (or systems) can ask confirmation of reception and notification that messages have reached intended receiver.

Threats to ICT security

Cyber crime consists of specific crimes dealing with computers and networks (such as hacking) and the facilitation of traditional crime through the use of computers (i.e. child pornography, hate crimes, identity theft, and credit card account thefts). In addition to cyber crime, there is also “computer-supported crime” which covers the use of computers by criminals for communication and document or data storage. While these activities might not be illegal in themselves, they are often invaluable in the investigation of actual crimes. Computer technology presents many new challenges to social policy regarding issues such as privacy, as it relates to data mining and criminal investigations.

Identity theft and *identity fraud* are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Hacking is unauthorised use, or attempts to circumvent or bypass the security mechanisms of an information system or network. Hacking can be a threat to a user's computer systems because this can give to the *hacker* total control over the system where he can steal delicate or classified information, destroy, disrupt or carry out illegal activities on a network or computer system.

A *keylogger* sometimes called a keystroke logger, key logger, or system monitor, is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard. As a hardware device, a keylogger is a small battery-sized plug that serves as a connector between the user's keyboard and computer. Because the device resembles an ordinary keyboard plug, it is relatively easy for someone who wants to monitor a user's behaviour to physically hide such a device "in plain sight." As the user types the device collects each keystroke and saves it as text in its own miniature hard drive. At a later point in time, the person who installed the keylogger must return and physically remove the device in order to access the information the device has gathered. A keylogger program does not require physical access to the user's computer. Someone who wants to monitor activity on a particular computer can download it on purpose or it can be downloaded unwittingly as spy ware and executed as part of a root kit or remote administration (RAT) Trojan horse. The keylogger program records each keystroke the user types and uploads the information over the Internet periodically to whoever installed the program.

Threats from communication tools: MSN, Skype, etc – main recommendation is not to execute strange files. Threats from web-browser: spy ware, cookies etc – main recommendation is to set the web-browser so that cookies are not allowed.

Possible channels of intrusion

There are possible channels of intrusion that need to be secured, both technical and human:

- Wi-Fi - Wi-Fi is a wireless technology brand intended to improve the interoperability of wireless local area network products. Common applications for Wi-Fi include Internet and VoIP phone access, gaming, and network connectivity for consumer electronics such as televisions, DVD players, and digital cameras.
- VPN - virtual private network (VPN) is a communications network tunnelled through another network, and dedicated for a specific network. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption.

- WLAN - wireless LAN or WLAN is a wireless local area network, which is the linking of two or more computers without using wires.
- Bluetooth - Bluetooth is an industrial specification for wireless personal area networks (PANs). Bluetooth provides a way to connect and exchange information between devices such as mobile phones, laptops, PCs, printers, digital cameras, and video game consoles over a secure, globally unlicensed short-range radio frequency.
- Others (i.e. employees).

Common tools to ensure ICT security

Possible tools to improve ICT security and avoid attacks are use following solutions:

- Antivirus software – it is important to refresh the software regularly.
- Firewall.
- Spam-filter.
- Electronic identification/certificates.
- Encrypted authentication.
- Electronic signature and ID identification.
- Avoid from spy ware while surfing in the internet.

How to behave securely

To ensure ICT security in the organisation, ICT security policy should be specified. It is recommended to determine the main goals for implementation of ICT properties. ICT security policy should be regarded as information policy and marketing policy of the enterprise. It is also recommended to determine methods on how the security task is resolved in different cases (including risk analyses). An important part of ICT security policy is responsibility of every employee. ICT security policy includes and relates to the following:

- Security of hardware and software assume and include:
 - Identification and authentication.
 - Access adjustment.
 - Infrastructure of network.
 - Delete activities, malicious software (modification of the information).
 - Security of the computers (desktop and notebooks).
- Data communication security includes:
 - Network infrastructure.
 - Security of internet access.
 - Encryption and authentication of telecommunication.
 - It is not recommended to locate the web-server in a company's premises but to outsource the server hosting instead.
- Physical security includes:
 - Security of building, including protection of services.
 - Access to the computers and data sources (databases, information systems etc).
 - Discovering and reporting threats.
 - Device protection (thefts).
 - Regulating of services and maintenance.
- Security of documents and data sources (all kind of information carrier) includes requirements for
 - Data storage.
 - Data delivery.
 - Data removal.
- Safety of eBusiness procedure has to be regulated by internal rules:
 - Always create a backup copy
 - Create strategy for specific situations, main plans for specific cases
 - Work out instructions and documentation for ICT security policy

- Take care of training and awareness of employees. Decide how announcement of security incidents (intrusions, leak of data) should be regulated
- Safe way to use e-mail – main requirement is not to open or execute strange attachments. Do not publish an e-mail address in public web-sites.
- Using and holding the passwords – remember all passwords (access to the network and eBusiness systems).
- Electronic identification - Log out the computer after finishing job
- Delete data securely (do not send the file only to Recycle Bin, in this case the data is readable and recoverable).