An integral framework for information systems security management

Business use of Internet has exposed security as one of the key-factors for successful online competition. Contemporary management of E-business security involves various approaches in different areas, ranging from technology to organizational issues and legislation. These approaches are often isolated, while management of security requires an integrated approach. This article presents an attempt at management of E-business systems security that is based on integrating existing approaches in a balanced way. To foster practical use of the conceptual model in this paper, brief background knowledge in related areas is given.

Keywords: information systems, security management, methodological framework.

Introduction

Security of information systems (IS) is becoming a part of core business processes in every organization. Companies are faced with contradictory requirements to deal with open systems on the one hand and assure high protection standards on the other. Appropriate treatment of related issues is far from trivial and requires a wide spectrum of knowledge, ranging from technology and organization to legislation. There are various approaches in the literature, some of them being almost exclusively technical, e.g. [Stallings, 1999], some of them hardly mentioning security issues, e.g. [Harmon, 2001], some of them covering mainly human factors in organizational issues, e.g. [Wysocki, 1997], and some of them covering only legal issues, e.g. [Powers, 2001]. Therefore, a coherent conceptual model is needed to manage E-business systems security effectively by deploying existing approaches in a balanced way. Accordingly, this paper addresses these topics through integration of relevant areas, and it bridges the gaps between practitioners of various profiles that are involved in IS security.

To protect information, an organization has to start with the identification of threats related to business assets. Based on threats analysis, a layered multi-plane approach is proposed. The first plane is focused on interactions, starting with security mechanisms and therefore deploying security services which are linked to human-machine interactions. Finally, human interactions have to be covered. In parallel, to make things operational, it is necessary to address another perspective, which includes technological, organizational and legislative planes (Figure 1).

The detailed methodology, based on the above model, is presented in this paper with diagrams. These diagrams state inputs, processes and outputs, which capture necessary business activities for management of IS security. They are explained in the text, which includes the background knowledge that is necessary to understand related issues.

The paper is organized as follows. In the next section, systems development and maintenance is covered, which includes...
threats analysis, security infrastructure, public key infrastructure and additional elements of security infrastructure. It addresses practitioner’s dilemmas about costs, outsourcing, complementary and substitutive technologies. In the third section, security policy is covered. It concentrates on human resources management issues with addressing of organizational and legislative issues, including continuity planning, auditing and inter-organizational issues. This section is a kind of a template that a practitioner can follow to set up a sound security policy in an organization. Finally, there is a conclusion in the last section. The whole paper is based on best practices, main international standards and international, EU and US regulations.

1. Make a complete record of organization’s assets and resources.
2. Identify threats by taking motivation of a potential attacker and the human factor into account. Avoid common assumptions that only bright and knowledgeable people can exploit security bugs, and that attackers are always motivated by illegal tendencies.
3. For each threat in Step 2 define its possibility E(x).
4. Determine damage costs D(x) related to each threat.
5. Evaluate risks by calculating expected damage - D(x)*E(x).
6. Define an action plan by setting priorities, where investment for preventing threats should not exceed damage costs.
7. Decide for arrangements with insurance companies to complement the organization’s own measures and to compensate damage in worst-case scenarios (Figure 3).

One should not overlook the fact that threats also include non-operational IT infrastructure because of improper design that leads to overload and technical failures. Finally, expertise should not be limited just to computer-related issues, but also to general business risks, e.g. costs caused by interrupted operations.

Although the procedure looks straightforward, threats analysis is not a trivial task. The main problem is to determine E(x). Due to the nature of security business, a large number of attempts remain undiscovered and getting accurate figures is close to impossible. Therefore, an organization should use various sources: its own data, data collected by other professional organizations and data obtained by hired system attackers. A promising approach is to deploy techniques that are used to stimulate innovation processes [Likar, 2001] by focusing on security threats.
Security infrastructure — from mechanisms to services

OSI standards [ISO, 1995a] form the technological basis of security for contemporary networked E-business systems. They distinguish between mechanisms and services. Mechanisms consist of symmetric and asymmetric cryptographic algorithms, one-way hash functions and physical mechanisms. The main representatives of symmetric cryptographic algorithms today are Triple-DES [NIST, 1999] and AES/Rijndael [Foti, 2001]. Among asymmetric algorithms, RSA [RSA Labs, 2002] is a major player, while for devices with low processing capabilities like smart cards, elliptic curve-based systems are used, e.g. ECDSA [ANSI, 1998]. Secure Hash Algorithm or SHA-1 [Eastlake, 2001] is an emerging standard among one-way hash functions.

Cryptographic algorithms are needed to transform plaintext into ciphertext and vice versa. These transformations make it impossible for an attacker to obtain plaintext from a ciphertext without knowing a key, which is a sequence of bits and serves as a parameter for transformation. While symmetric algorithms use principles that have been known for a long time (substitutions, permutations, etc.), asymmetric algorithms use results from theory of computational complexity (factorization problems, discrete log problems, etc.). In principle, the longer the key, the safer the transformation. As symmetric and asymmetric algorithms are based on different mathematical principles, it is hard to make direct comparisons about the strengths of those algorithms. As a rough rule, Figure 4 assumes that best currently known attacks can be used [Fumy, 2000]. For highly sensitive information today one should use 2 K bits for RSA and 128 bits for Triple-DES [Schneier, 1996]. For elliptic curve (EC)-based systems, keys can be significantly shorter — having RSA encryption with 768 bits long keys, a comparable strength can be achieved with approx. 128 bits for EC-based system, while 2 K bits of RSA gives strength that is roughly comparable to 200 EC bits.

Symmetric algorithms use the same keys for encryption and decryption, while asymmetric ones use one key for encryption and another for decryption. Only the owner knows the first key, called a private key, while the second one can be communicated to anyone and is called a public key. When the owner of a private key encrypts a message, anyone knowing the corresponding public key can decrypt it. Consequently, the recipient can be assured of a message’s origin and integrity and this is the basis for digital signature. Additionally, when a
message is encrypted with a certain public key, only the owner of the corresponding private key can decrypt it to access the contents. These properties of asymmetric mechanisms constitute the basis of modern security services. However, there are drawbacks; the first is computational complexity. These algorithms are significantly slower compared to symmetric algorithms of a similar strength. Secondly, in order for a user to know that a particular public key indeed belongs to the person claimed, a trusted third party called certification authority (CA) has to be introduced. CA issues a certificate that is a digitally signed electronic document, which assures binding between an entity and the corresponding public key. A certificate can be verified by anyone knowing CA’s public key. However, every cryptographic document has a limited life span because of growing processing power and it may happen that the old key becomes insufficiently long sooner than expected. Besides, a private key may be compromised. Finally, a user may be using a certificate in a way that he/she was not supposed to. Thus, each CA maintains a certificate revocation list (CRL) that should be checked every time a certificate is used.

Another important family of cryptographic primitives comprises one-way hash functions. They process a text of arbitrary length to an output of fixed length. Despite knowing the output of one-way hash function, it should be computationally infeasible to find any input that maps to the same output. Besides, it should be computationally infeasible for an arbitrary output to find two inputs that map to this output. Put simply, one-way hash functions produce a fingerprint of a document and these fingerprints are actually used for digital signatures. The procedure goes as follows. A document is hashed and its hashed value is encrypted with a private key. The encrypted hashed value is attached to the document and it presents its signature. The recipient produces
a hashed value of a received document and decrypts the received signature with the public key. If those values match, the digital signature is verified.

Protocols that use cryptographic primitives are called cryptographic protocols. They are used to implement security services, which are:

- authentication that provides for the authentication of the communicating peer entity
- confidentiality that protects the data from unauthorized disclosure
- integrity that detects any modification, insertion or deletion of data
- access control that provides against unauthorized use of resources
- non-repudiation that provides the recipient with the proof of origin and the sender with a proof of delivery, where false denying of the message content is prevented
- auditing that enables administrative recording of events for detection of suspicious activities, analysis of successful breaches and evidence for resolving legal disputes

To provide authentication, asymmetric algorithms are used, because of their low key-management complexity. Because of computational complexity, symmetric algorithms are used for protecting sessions once entities have been authenticated. However, certificates have to be introduced in this scenario. The ultimate certificate and certificate revocation list specification for a business environment is X.509 standard, version 3 [ITU, 2000]. Main certificate fields are serial number, issuer (i.e. trusted third party), subject (i.e. an owner of a public key), the public key itself, validity and signature of a certificate. Other fields are required for processing instructions, while extensions are needed to support other important issues, which are yet to be resolved: automatic CRL retrieval, their storage point and distribution, security policy issues, etc. Before using a public key, the validity of a certificate has to be checked against the corresponding CRL. These checks currently have to be done manually, which is very frequently neglected in today's E-business environments.

Regarding security policies (discussed in more detail in the following sections), it should be evident to a user of a certificate in what context a certain public key may be used. For example, an employee may not be allowed to sign contracts above a certain amount.

Distribution of public keys is done through a global distributed directory. The most frequently proposed system for this purpose is X.500 directory [ITU, 1997c]. Protocols to access its content (certificates, CRLs) are directory access protocol or DAP [ITU, 1997c] and lightweight directory access protocol or LDAP [ITU, 1997c]. The so called Registration Authority (RA) that identifies users and submits certificate requests to CA, serves as an interface between the user and CA. In addition, a synchronized time base system is needed for proper operations. All these elements, together with appropriate procedures, form a so-called public key infrastructure (PKI).

Setting up a PKI
Implementation of a PKI should address a wide variety of issues:

- Operational procedures – registration, initialization, certification, key generation, key recovery and compromise, key update and expiry, cross-certification, and revocation.
- Supporting protocols – operational and management protocols, time stamping.
- Staff-related issues – education and training.
- Hardware and software-related issues – flexibility, scalability, ease of use, costs, interoperability and standardization.
- Consultancy for specific issues – name space management, certificate paths, trust models, etc.
The central point in establishing PKI is CA (Figure 5). It all starts with issuing a certificate to a physically identified user who knows the corresponding private key. Malicious actions by CA operators should be minimized as much as possible. Therefore it is a common practice that a user generates a key pair to ensure that a private key is known only to him/her. However, many threats still exist that should be minimized [Roe, 1993]:

- loss of confidentiality of private keys, including compromise of local key storage, interception during transmission from key storage unit to the processing unit, and compromise of the key generation process
- modification of data, which includes modification of certificate contents and modification of attributes prior being packaged in a certificate
- masquerade, which should consider both parties, users and CAs
- false repudiation, which includes user denying requesting a certificate or requesting a certificate revocation
- misuse of privilege, which includes CA issuing incorrect certificates or revocation lists

In the past, trust models used to be an important topic that addressed questions like what kind of CAs, would exist, what their relationships would be, etc. Efforts were made to standardize these models by introducing so-called policy CAs, organizational CAs, etc. However, after years of operations of established commercial CAs it is evident that they operate as isolated certification islands — there is almost no cross-certification.

Procedures for initial key exchange have to be defined before certificates can be issued. Initially, a user physically contacts RA, where he/she is identified on the basis of a valid document and signs a request. The subsequent procedure may vary and it is defined locally. In Web environment, a common business practice goes as follows. CA maintains a Web server that supports SSL protocol [Freier, 1996] and has installed CA's certificate. A user, who has enrolled at RA, is sent two secret strings through two different channels, e.g. email and ordinary mail. After obtaining these strings, a user connects to the server through the browser, which automatically activates SSL, and establishes a secure session. Based on the data about CAs certificate a user can be assured of being connected to CA's server — usually this is done by checking key fields and a fingerprint of a certificate (a fingerprint can be obtained at RA during initial registration). Afterwards a confidential exchange of subsequent data, along with integrity, is enabled. After checking CA's certificate, a user enters his/her personal data and secret sequence strings, which authenticate the user to the server. Then the server triggers a browser to produce a key pair and a public key is transmitted over the network for signing. When the certificate is produced, a
user can download it to his/her computer, as every certificate is a public document. Once a certificate is signed, it is necessary to provide means to revoke it. For this purpose, procedures for revocation have to be defined and CRLs have to be maintained in accordance with [ITU, 2000]. In the case of compromised private key, the following procedure can be done over the network — a user makes a request for revocation with the serial number of a certificate and signs it with a compromised private key.

CAs are expected to stay in business for a long period. Therefore, they should define procedures for changing their keys. Most commonly, existing digital documents will have to be re-signed, together with their old signatures using new keys. Other procedures should include operations for employees and physical access to CAs computing resources. Educational and training requirements also have to be considered seriously.

PKI standardization efforts started in the first half of 90s and these issues are now very complex. PKI standards that are mainly concerned with technological part of operations are defined by Internet Engineering Task Force. As an introductory reading to the wide variety of IETF PKI standards, PKI roadmap is recommended [Aresenault et al., 2002]. It addresses and references in detail the related approaches and methodologies mentioned above.

When to outsource PKI operations CA operations are very sensitive and require significant knowledge, manpower and financial investments; it is vital to evaluate the total costs of ownership. The first decision is about outsourcing these operations. Basic questions to be answered are: what are the risks associated with outsourcing? Will certificates be issued only to employees, or also to suppliers and customers? Will the organization use certificate services also for signing the code? What is the expected total number of certificates to be issued?

The structure of costs then has to be defined precisely. These costs can be grouped into six main categories [Aberdeen Group, 1998]:

- PKI systems: user and server certificate fees, certificate hardware and software platforms, CA and directory software.
- Client software: client software acquisition and distribution.
- Maintenance: hardware, software, disaster recovery systems.
- Services: PKI design and planning, installation and configuration, integration and testing, training, root key notarization, cryptography health checks, audit and certification, disaster recovery services, secured facilities and procedures for logical and physical protection.
- Staffing: start up engineering costs, integration and testing, project rollout, project management, info-systems administration, certificate repository and maintenance, PKI procedures, help desk, training, security monitoring and audit.
- Risk management: transaction insurance, financial and legal liability assistance.

According to the Aberdeen group, three-year total costs of ownership range from approximately $3 to approximately $22 per seat for 500 000 users and from $50 to approximately $200 per seat for 5000 users.

Additional elements of security infrastructure

PKI is only a part of a wider security infrastructure. This subsection gives an extensive overview and a brief explanation of security applications that are needed to establish security infrastructure. Every security infrastructure will be largely based on such commercially available solutions. Being familiar
with these building blocks and related security issues is thus essential for security practitioners.

**IPSec**
The old IP version 4 protocol has many well-known vulnerabilities. It is possible for a user to pretend to be another user. The communication can be monitored and the data modified. It is possible to overtake the session etc. To prevent these and other threats, new standards for security enhancements were defined in the mid-90s. Today these have grown into a large family of standards, so it is suggested that a reader takes [Thayer, 1998] as an entry point to IPSec. IPSec is becoming a common practice in business environments, but it is quite limited to closed administrative environments with little inter-organizational use, due to open PKI issues [Gutmann, 2002].

IPSec assures security within IP layer, providing the following security services: authentication, confidentiality, connectionless integrity, and access control. Limited traffic flow confidentiality is possible too. This is achieved by use of cryptographic algorithms, applied to IP packets. IPSec presents a common security environment to all applications, which is backward compatible with IP v4. Its basic building blocks are authentication header (AH) and encapsulation security payload (ESP). AH provides support for authentication and data integrity by using keyed message authentication codes (MACs). Keyed MACs are outputs of one-way hash functions, applied to headers and shared secret keys. To provide confidentiality of a payload, ESP is involved with symmetric encryption. IPSec uses a principle that has been already described for establishment of secure session — public keys are used to authenticate involved parties and to exchange session keys, which later serve for symmetric encryption of bulk data.

Secure Sockets Layer/Transport Layer Security
SSL protocol was developed by Netscape as a common security layer for a variety of application protocols, with emphasis on Web services. It is positioned just below the application level. It provides authentication, confidentiality and integrity with a possibility to negotiate crypto primitives and encryption keys. Authentication includes server authentication by default and, optionally, client authentication. The session is initiated by a client and in a response a server sends its certificate and cryptographic preferences. The client then generates the master key, which is encrypted with the server’s public key and returned to the server. Using its private key, the server recovers the master key and returns to the client the message encrypted with this master key. This is the basic phase, which can optionally be extended with authentication of a client, which is analogous to the basic phase with roles of client and server exchanged. At this stage, entities are authenticated and subsequent messages are encrypted with a symmetric algorithm that uses session keys derived from a master key and this provides confidentiality. A successor of SSL is TLS [Dierks, 1999] but although they are close relatives, TLS is not compatible with SSL.

Secure/Multipurpose Internet Mail Extensions
Secure/Multipurpose Internet Mail Extensions or S/MIME [Ramsdell, 1999] are security enhancements for email. Ordinary email is designed to transfer only printable characters (so called 7 bit ASCII code). In order to send graphics, sound and programs, these data have to be re-coded into a format that is understood by the majority of mailing systems --- the RFC 822 format [Crocker, 1982]. The transformation is defined by MIME standards, e.g. RFC 2045 [Freed, 1996]. S/MIME, as a security enhancement of MIME, uses X.509 v3 certificates and offers authentication, confidentiality, integrity and non-repudiation. S/MIME is important for electronic data interchange (EDI). EDI standards, be it ANSI ASC X.12 [ANSI, 2001] or EDIFact [UN, 1993]
do not address security issues and leave them to the transport system. EDI business documents can thus be securely transferred with S/MIME. Unresolved S/MIME problems have a common denominator with IPSec — these are open PKI issues.

Extensible Mark-up Language
Extensible Mark-up Language or XML is becoming the de facto standard for the definition and processing of electronic business documents (including EDI). It is a meta-language that consists of three parts. The first part covers basic XML documents with user-defined tags in a human readable form, used by subsequent programs as processing instructions. The second covers structuring of XML documents, where data definition documents (DTDs) are used, which define the syntax of a document. The third is intended for presentation of a document, where so called cascading style sheets and extensible style sheets are defined.

Encrypting XML documents as a whole in a classical manner, along with tags, disables a search for relevant data. Syntax definitions included in DTDs remain inaccessible. However, business needs solutions to encrypt and/or sign certain parts of the whole document. Moreover, already encrypted and/or signed data may be further processed as part of a different data set etc. This results in new threats, e.g. if procedures enable insight into plain tags together with encrypted tags, plaintext attacks are enabled. To date, the necessary standards have been accepted by the main standardizing body for XML, the W3C consortium. These standards address the above issues under two groups: XML signatures and XML encryption [Mactaggart, 2001]. The main motivation behind them is to preserve flexibility when applying security services to XML documents.

Virtual Private Networks
Virtual Private Networks (VPNs) provide a cost effective solution for building secure private networks using public networks. With security services, based on PKI, physical links of an arbitrary provider can be used to transfer the protected organization’s data, thus logically implementing a private network. Devices, users and applications are authenticated by use of certificates and appropriate cryptographic protocols. Similarly, cryptographic protocols are used for secure session key exchange, so confidentiality and integrity can be assured. IPSec technology actually enables a straightforward implementation of a VPN in an organization.

Mobile computing, mobile code and intelligent agents
Mobile computing is gaining strong support and importance in the business environment, and we are reaching the point where the number of wireless devices will exceed that of fixed nodes. This poses new requirements for security. Handheld mobile devices have limited processing power and memory capacities. It is
not a problem to provide strong cryptographic mechanisms for these devices since the invention of elliptic curve cryptography. However, PKI is a problem for the wireless world. It requires extensive computation for certificates and CRLs and it further narrows the available throughput [Miller, 2001]. Appropriate standards that would enable a wide-scale secure deployment are yet to come, but the principles of secure operations are similar to those for fixed devices.

Mobile code and mobile agents present a fundamentally new approach. They pass from one processing environment to another and they use the computing resources of the host. Agents are supposed to act on behalf of their users, e.g. finding the best offers, bidding at auctions, etc. Therefore, their security is very important. Typical threats include uncontrolled read and write access to core agent services and information (e.g. agent directory services), privacy and integrity of messages and message transport services, and denial of services. Moreover, such code operates in partly predictable environments and has to be protected from malicious hosts. This introduces two new generic threats, which are code peeping and code modification through false computation (a promising method for their prevention is mobile cryptography [Sander, 1998], but it is at a research phase). Speaking generally, security issues in this area have yet to be resolved [FIPA, 2001].

Smart cards
Smart cards are plastic cards of standard dimensions with an embedded microprocessor, and serve as a personal electronic device [ISO, 1994]. Their importance in establishing security infrastructure is growing, because they present one of the best possibilities for storage of keys and digital signature processing. However, once they are used as secret key storage devices, their tamper-resistance is of utmost importance and various design tricks are used to achieve this [Hendry, 1997]:

- Sensitive elements of micro controllers, e.g. ROM, EPROM, E2PROM, are buried in lower layers of a substrate to prevent analysis of stored data.
- Buses are scrambled and not laid out in a sequential order to prevent analysis of processed data (similar holds true for addresses of memory locations).
- Dummy components are inserted in the chip, as well as low/high frequency and temperature detectors to prevent attempts for analysis.

Despite this, smart cards may still be vulnerable to various kinds of attack [Anderson, 1996]. One of the latest attempts is based on power analysis [Kocher et al., 2000] by sampling power consumption during crypto-operations. Nevertheless, they are an effective and mature technology. They can serve as a link between the digital domain, when using cryptographic primitives for IS services, and the physical world when implementing security policy (access control).

Firewalls
Firewalls are specialized computer systems, which are used primarily for access control [Cheswick and Bellovin, 1994]. They operate on the border between the corporate’s network and the Internet, where all traffic must pass through the firewall. Only authorized traffic is allowed to pass, which is defined by the security policy. This makes security management much easier, as the firewall presents one central point for auditing and alarms for outside attacks. It blocks potentially vulnerable services and provides additional useful features like local network hiding through address translation. All local addresses are mapped in the outgoing packets, thus making it harder for attackers to obtain appropriate data for successful attacks. Besides, firewalls can provide proxy software that receives and pre-processes requests before passing them on. Firewalls can even host exposed server software like HTTP daemons.
The main limitation of classical firewalls is their inability to prevent tunneling attacks, e.g. virus attacks and Trojan horses. Of course, firewalls cannot protect against bypassing attacks, e.g. internal modem pools [Stallings, 1999].

There are three types of firewall: packet filtering router, application level gateway and circuit level gateway. Each packet is routed through the network, based on source and destination IP addresses, while the application for which the payload is intended is identified through ports. This is the basis for firewall operations. Thus, a packet filtering router applies rules to each incoming IP packet and forwards or discards it. This simplicity of operation is the main advantage of packet filtering, while the disadvantage is lack of more sophisticated operations. The opposite design uses special purpose code with application level gateway, also called a proxy server. Proxy relays the traffic between the original application and the user. Only applications with a proxy are available to a wider community. Proxy can use enhanced authentication procedures and application code scanning, but it has a drawback of large processing power requirements. It can also provide application hiding, where various internal machine names can be stripped to a unique, publicly available name. Finally, circuit-level gateways can be used to prevent end-to-end connections. In contrast to proxy, circuit-level gateways maintain connections on different ports. They are the preferred method for securing outgoing connections.

Intrusion detection systems
Real-time intrusion detection systems (IDS) were developed in the 90s and have been significantly improved since then [Kemmerer and Vigna, 2002]. Their operation requires reliable and complete data about the system activity. The first important step is to determine what information to log and, where to get it (distributed systems log information at different places and analyzing only a particular host’s logs could not reveal the real picture). Afterwards, two basic approaches are possible: anomaly detection and misuse detection. Anomaly detection uses models of normal behavior and detects acts that differ from normal patterns. The advantage of these systems is that they can detect previously unknown attacks, but they produce high false-positive alarms. On the other hand, misuse detection systems are based on definitions of wrong behavior, also called signatures (this is similar to functioning of anti-virus software, which is actually a kind of IDS). Audited data are compared with these signatures, and if matched, alarm is generated. The main advantage of these systems is the low rate of false positive alarms, but they can detect only known attacks. Therefore, the majority of intrusion detection systems are based on misuse approach. To compensate the weaknesses of each approach, hybrid techniques are used.

Technological compliance – Common Criteria
When buying commercial off the shelf (COTS) products, it is necessary to pay attention to independent evaluation of their security properties. A few years ago, the main approach in Europe in this field was Information Technology Security Evaluation Criteria or ITSEC, while in the US this was Trusted Computer System Evaluation Criteria or TCSEC. Joint harmonization efforts are now underway within ISO, called Common Criteria for Information Technology Security Evaluation - CC [ISO, 1999]. CC defines requirements that products have to fulfill from the security point of view and they present a base for comparing various security evaluations. Consumers can determine if a certain product is secure enough for the intended use, developers can determine desired security properties and declare them in a standardized way, and evaluators can verify them.

CC consists of four parts: the first part presents a general model for evaluation, the second provides the catalog of security functional requirements, the third contains assurance...
requirements, and the fourth one contains examples of protection profiles. There is a part in preparation that contains functional and assurance security requirements for cryptographic support in distributed systems and networks.

Functional requirements consist of functional classes, where each of them contains various families. Similarly, assurance requirements consist of assurance classes, where each contains various families. An important notion, introduced by CC, is that of evaluation assurance levels (EALs). These predefined assurance packages present the baseline set of assurance requirements for evaluation. They form an ordered set, which defines the assurance scale of the CC:

- **EAL 1** refers to functionally tested products as the lowest assurance level for which evaluation is meaningful and economically justified. It is intended to detect obvious errors and is applicable in circumstances where risks to security are not serious.

- **EAL 2** refers to structurally tested products and can still be used without imposing additional tasks on the developer. If the developer applies reasonable standards, this level may be feasible without developer involvement, other than support for security functional testing. EAL2 is applicable to a low or moderate level of security without the need for the complete development record.

- **EAL 3** refers to methodically tested and checked products. This level can be assured by using positive security engineering at the design stage (there is no need for substantial alteration of existing sound development practices). Therefore, EAL3 provides a moderate level of assured security without substantial reengineering costs.

- **EAL 4** refers to methodically designed, tested, and reviewed products. It provides maximum assurance based on good commercial development practices. These practices still do not require substantial specialist knowledge and skills. This level is likely to be economically feasible for implementations within an existing product line. It provides moderate to high level security for conventional products, incurring minimal additional engineering costs.

- **EAL 5** refers to semi-formally designed and tested products. It requires security engineering based on rigorous commercial development practices supported by moderate specialist security engineering techniques. Although EAL 5 additional costs should not be excessive, it provides a high level of security.

- **EAL 6** refers to semi-formally verified design and testing of products. It provides high assurance by using a rigorous development environment and techniques. EAL 6 products are for protecting high value assets against significant risks.

- **EAL 7** refers to formally verified design and testing of products and constitutes the upper bound for practically useful products. It is aimed at security products for application in extremely high-risk situations and/or where the high value of the assets justifies these costs.

**Systems analysis and design**

Although many ready-to-run applications are available on the market, there is a permanent need for customized solutions, which is especially the case with new business models, where designing E-business systems brings new challenges to managers and engineers. Because of the increased importance of IT solutions for core business processes on the one hand, and increased complexity on the other, bugs have to be eliminated carefully. Exploiting vulnerabilities of poorly verified code is the main reason for denial of service attacks and their prevention is becoming critical. This is achieved with a use of formal techniques,
which have to be taken into account at the process of analysis and design. A variety of formal techniques can be used to support these processes and three of the most frequently used ones are discussed here.

**Unified Modelling Language**

At the level of managerial specifications, and consequently level of information engineering, Unified Modeling Language (UML) [OMG, 2001] is becoming a definite standard. UML is a graphical and object oriented language for capturing knowledge (semantics) and expressing knowledge (syntax) regarding the subject [Alhir, 1998]. It is intended primarily for modeling systems that have to be implemented in software. It is based on best industry practices and used for specifying, visualizing, constructing and documenting systems. UML covers static and dynamic properties of systems through extensive views that include:

- use case diagrams for describing the functionality of a system and users of a system
- class diagrams that describe the static structure of a system
- object diagrams that describe the static structure of a system at a particular time
- sequence diagrams that describe interactions among classes
- collaboration diagrams that describe interactions among classes and associations
- state diagrams that describe the states and responses of a class
- activity diagrams that describe activities of a class
- component diagrams that describe the organization and dependence of SW components
- deployment diagrams that describe configuration of processing elements

The main objective of UML is to provide effective, structured means for communications at the highest managerial and conceptual levels. However, UML specifications have to be further elaborated before they can be fully transformed into a program code. These steps, especially the most critical parts, are suggested to be specified and analyzed with tools that have a sound mathematical basis.

**Language Z**

Language Z was developed at Oxford University in the late 80s [Spivey, 1989]. It is based on set theory and first order logic, i.e. it has mathematical semantics, while its syntax also is being standardized. Z is a typed language. Using schemas, models are constructed that cover static and dynamic views of the system. Once the system is formalized, errors can be discovered, the system can be rigorously analyzed, and its critical properties can be proven. Put another way, it is possible to derive proofs about properties of these models, which significantly reduces the possibility of false or buggy implementations and contributes to the strength of proper transformations into executable code. However, formalization is not an easy task. It requires highly skilled professionals and significant time investment. Therefore, it is usually used for the most critical parts of the designed system. Z is currently in a standardization process at ISO [ISO, 2002].

**BAN Logic**

Secure E-business solutions in networked information systems depend strongly on protocols that use cryptographic primitives, i.e. cryptographic protocols. To provide assurance that a particular security service is fulfilled once the protocol runs from its initial state to the final state, appropriate formal techniques are used. One such formalism is BAN logic [Burrows et al., 1990], which is focused on proving authentication properties of cryptographic protocols. It relies on cryptographically transformed messages, where proper use of cryptography assures integrity.
and freshness of exchanged messages, thus achieving authentication. The proof process starts with conversion of a protocol into idealized form. Then assumptions at the initial state are given. Logical formulas are attached to these statements. In line with transformation rules and the run of a protocol, formulas are obtained which state beliefs of involved parties at the end of a protocol. BAN logic has a strict syntax and proof derivation rules. However, it lacks formal semantics with respect to which the logic would be sound. Nevertheless, it is one of the most successful techniques in this field. Other useful formal techniques regarding cryptographic properties are [Gong et al., 1990] and [Syverson, 1994].

Users are strongly advised to use protocols that have a sound reputation in the literature. However, there is always a chance of being forced to tailor existing solutions to particular needs, to deal with slightly different roles or assumptions, or to invent or design a completely new protocol. In this case, formal verification of a cryptographic protocol is necessary, although passing a formal verification does not provide watertight evidence that a protocol is bug-free. Finally, formal verification of ordinary protocol properties (dead-locks etc.) is increasingly important to prevent denial-of-service attacks [Holzmann, 1991].

**Security policy**

Even technologically superior solutions will be in vain without complementary organizational aspects, because many successful attacks have nothing to do with sophisticated kinds of technological attack [Anderson, 1994]. Thus, risk management should address human resource management through organizational and legislative issues.

Security policy is defined by procedures that set out an organization’s approach to managing security. It is vital that this policy is based on management commitment. The policy document should include the definition of information security, basic terms, its objectives and scope, brief explanations of principles, standards and compliance requirements, a definition of responsibilities for information security management and references to documentation that supports the policy. The basic standard in this area is BS 7799 [BSI, 1999], which has recently been accepted as an international standard [ISO, 2000]. It is recommended that organizations follow closely this standard as the main methodology for establishing security policy.

**BS 7799-related issues**

BS 7799 consists of two parts. The first part describes the code of practice for information security management, while the second gives a specification for information security management systems. We will concentrate on code of practice, which explicitly states the main areas that have to be addressed in order to produce a sound security policy [BSI, 1999] (Figure 6):

- **Security organization:** information security infrastructure, security of third party access, outsourcing.
- **Asset classification and control:** accountability for assets, information classification.
- **Personnel security:** security in job definition and resourcing, user training, responding to security incidents and malfunctions.
- **Physical and environmental security:** secure areas, equipment security, general controls.
- **Communications and operations management:** operational procedures and responsibilities, system planning and acceptance, protection against malicious software, housekeeping, network management, media handling and security, exchange of information and software.
- **Access control:** business requirement for access control, user access management,
user responsibilities, network access control, operating system access control, application access control, monitoring systems access and use, mobile computing and teleworking.

- Systems development and maintenance: security requirements of systems, security in application systems, cryptographic controls, security of system files, security in development and support processes.

- Business continuity management: aspects of business continuity management.

- Compliance: compliance with legal requirements, reviews of security and technical compliance, system audit and considerations.

The main tasks behind the above-mentioned areas are briefly given in the following subsections with emphasis on activities that may be easily overlooked or underestimated.

Security organization
The code of practice gives recommendations on information security management to those responsible for initiating, implementing or maintaining an organization’s security. Initially, there has to be a person (information security manager) or a body (information security group) that is responsible for establishment, maintenance and review of security policy. Security policy has to be reviewed independently, whether internally or preferably, by an external specialized organization.

Asset classification and control
The responsible entity identifies all assets and allocates further responsibilities to members of the organization through the definition of clear and documented processes, taking into account authorization procedures for use of information processing facilities. Inventory access should include:

- information assets, which means databases, other files, system documentation, manuals, training material, operational procedures, continuity plans, archived information

- software assets, which means applications, operating systems, development tools
physical assets, which means servers, clients, mainframes, terminals, notebooks, modems, routers, faxes, data media, power supplies, air conditioning, furniture and accommodation.

Each asset has to be classified and labeled accordingly. These labels should reflect how critical information is in terms of its confidentiality, integrity and availability; however, overly complex schemes should be avoided. For each classification, handling procedures should be defined (in the case of data this includes copying, storage, transmission in electronic format or by spoken word, and destruction). Of course, all procedures are defined in line with threats analysis, so that the costs incurred do not exceed the value of resource being protected.

Physical, environmental and personal security

Cryptographic mechanisms only reduce the need for physical protection, but they cannot eliminate it. Thus, physical and environmental security has to be addressed carefully. This kind of protection should include issues about clear-desk policy, locking of sensitive information, logging off the system, prevention of unauthorized photocopying, immediate clearance of sensitive information from printer, appropriate use of passwords etc. In order to prevent unauthorized access, secure areas have to be defined. Physical entry controls should include supervision of visitors, recording of their entry and departure, and providing visitors with instructions. They should wear some form of visible identification. Securing offices, rooms and facilities should consider possibilities of theft, dust, excessive vibration, electrical interference, electromagnetic radiation, proper cabling and maintenance, fire, flood, smoke, explosions and other forms of natural and man-made disasters. Facilities should be located in a way that prevents public access, buildings should give minimum indication of their purpose, and support equipment (faxes, photocopiers) should be sited properly. Further, protected windows and slam shut doors should be considered, suitable intrusion detection systems and alarms should be in place, as well as smart card-based control throughout the building. Hazardous materials, fallback equipment and back-up media should be stored at a safe distance. Working in secure areas has to be properly related to working in delivery and loading areas.

The basis of security in every organization is informed, educated, and loyal employee. This is the most important factor for minimization of human error, misuse, fraud and theft.

Communications and operations security

Special attention has to be paid to internal communications and operations; operating procedures should be documented and every change formally approved. Segregation of duties is one of the main principles to reduce the risk of system misuse. Certain groups of procedures that might be easily overlooked, but may present a significant threat, are:

- Sufficient attention is not paid to event logs, especially their integrity and regular analysis, which are essential for detecting suspicious behavior and for cases of legal dispute.
- Media management is considered sufficiently (transport of media, its exchange and disposal), e.g. high security measures are conducted within an organization, but neglected when transporting back-up copies to a remote location.
- Minor operations are overlooked: clocks are not synchronized, equipment is left unattended, automatic time-out procedures are not implemented, software is not upgraded on time, mobile phones are used for sensitive communication in public places, passwords are poorly managed, faxes are sent to wrong numbers, etc.
- Equipment that is used off-premises; management should authorize every
such use and this equipment should not be unattended, and additional adequate insurance cover for such equipment should be considered.

Access control
The introduction of networked and Web-centric information systems requires a security policy that clearly defines the use of network services, necessary user and node authentication, physical segregation of networks, enforced paths for services, and filtering and limitation of connection time for high-risk applications. Regarding data access within an organization, it is advisable to manage information propagation using the Bell-La Padulla model [Bell, 1973] with its ‘no write down’ and ‘no read up’ principle. This principle assures that sensitive information can only propagate horizontally and upwards, so there is no leakage of confidential information; it is especially suitable for hierarchical organizations. Regarding an important technological threat to access controls, steganography should be mentioned [Katzenbeisser, 1999].

So far, we have concentrated on issues related to internal members of an organization, but external, third party access should not be overlooked. This access is defined based on identified risks and includes hardware and software maintenance staff, cleaning, catering, security guards, students, short-term appointments, consultants and outsourced partners. Following this, types of access are identified (physical access, logical access). For each type, reasons of access are given and appropriate measures are defined. Third party access should be based on formal contracts that include general security policy, description of services to be made available with physical and logical access control. Further, acceptable levels of services, the definition of performance criteria, liabilities and responsibilities with respect to legal matters (e.g., intellectual property rights), the right to audit contractual responsibilities, reporting and investigation of security incidents have to be defined.

Development and maintenance
Operational and development systems have to be separated, which is often not the case. Development environments are typically less protected and access to their data can be used for breach into the operational system. For example, testing is often performed on extracted operational data, which can easily be exposed in this way. Data input checks have to be put in place, together with control of internal processing to prevent abnormal behavior of applications. Output data validation is also needed. Even planning for appropriate capacity should be considered to prevent insufficient support of business requirements.

Compliance
Security policy has to address cryptographic controls. A decision whether to use cryptographic solutions or other kinds of controls is based on risk estimate. Once cryptographic controls are selected, the policy about their use has to be set and it should cover user roles, responsibilities and the determination of the appropriate level of protection, in line with information classification (algorithms, keys lengths, protocols). Further, it should address standards and take into account: key generation, distribution and activation, changing and updating of keys, recovery of lost keys, certificate management, archiving keys for business and legislative needs, logging and auditing of key management. Finally, appropriate procedures have to be defined for other legislative reasons: accounting purposes or potential disputes, where cryptographically processed documents are used as evidence. Procedures should cover the problems of re-encrypting and re-signing documents, when older technologies become vulnerable, or when key lengths become insufficient.

It is important to include aspects of operational software in security policy: operating systems,
applications, system files, and libraries. The modifications program (new installations, updates) should be put in place and each change approved and carefully planned. Back-up copies of previous versions should be maintained and programs listings should be stored in a safe place. Software patches have to be applied when necessary, which is most important for open source code products. An attacker can analyze a patch to obtain unauthorized access to resources that are not updated. It is also necessary to consider licensing, support agreements, assurance and quality agreements.

To ensure appropriate quality of systems and services, it is advised that security policy addresses ISO standards for quality assurance [ISO, 1995b]. These standards cover the problem of ensuring quality by defining models for design, development, production, final inspection, installation, testing and servicing. For the specific subgroup that applies to IS, see [ISO, 1997].

Continuity planning

Business continuity planning (BCP) is a very important issue and it has to be covered carefully [Devargas, 1999]. After a serious disaster many businesses recover with difficulty, e.g. in the case of major fire in the UK, over 80% of businesses never recover, despite insurance arrangements, which effectively cover 30-50% of losses. Thus, continuity planning should be an integral part of security policy. BCP starts with threats identification, asset valuation and determination of likelihood of incidence. Afterwards, business impact analysis has to be done to identify critical business functions. This analysis should identify effects of disaster and requirements for a recovery, including all resources. Afterwards, critical business functions need to be prioritised, depending on their impact. This impact forms the basis for financial justification of related investments for equipment, procedures and training to enable recovery in the necessary time frame. BCP requires inclusion of internal and external effects, which includes business interruptions of partners’ processes, loss of credibility and image.

Auditing

As information security management in E-business systems becomes common practice, standards for auditing are becoming increasingly important. It is vital for management to consult proactively and to advise on IT security. There are two mainstream auditing methodologies for IS. The first is based on BS 7799 standards. Information Systems Audit and Control Foundation (ISACF) has defined a complementary approach and this group of auditing standards is called Control Objectives for Information and Related Technology or COBIT [COBIT SC, 1998]. COBIT is more of a general nature. It is oriented towards understanding and managing business risks that are associated with implementation of new technologies. Put in another way, it bridges gaps between business risks, control needs and technical issues, by providing good practices to structure and manage activities. These activities are related to business objectives and they are structured into four domains: planning/organization, acquisition/implementation, delivery/support, and monitoring. Each of these domains consists of processes that have to be performed and there are 34 such processes, e.g. from definition of a strategic IT plan to independent monitoring. Using these processes, two additional views are covered: information criteria (quality, fiduciary, security) and resources (people, applications, technology, facilities, data).

Legal issues

Unifying legislation, to the extent that is comparable to standardization of technology, is very hard if not impossible. The reasons are political and historical, and are related to fundamental issues like territorial principles. Besides, many legal issues in the area of IS
security management are yet to be resolved. Last but not least, concentrating on particular state regulations would exceed the scope of this paper. Therefore, this subsection concentrates on international, EU and US regulations, which present a basis for national (state) legislations. This subsection provides general guidelines and a checklist of explained legal issues that have to be addressed by organizations within a particular legislation. In every case, final decisions should be discussed with a lawyer.

The subsection is structured as follows: cryptography regulations, digital signatures issues, privacy rights, intellectual property rights, and responsibilities of service providers.

Cryptography regulations
Cryptography has become a common practice in the business environment, as governments have recognized the importance of securing online business. At the international level, the basis for use of cryptography is presented in OECD Cryptography Guidelines [OECD, 1997]. They are strongly in favor of privacy — the fundamental right of individuals to privacy (including secrecy of communications and protection of personal data) should be respected. This rejects key escrow approaches, although cryptography policies may allow lawful access to plaintext, or cryptographic keys. These guidelines also state that cryptographic methods should be trustworthy in order to generate confidence. They should be developed in response to the needs, demands and responsibilities of users and governments, where users should have a right to choose any cryptographic method, subject to applicable law. Further, the liability of individuals and entities that offer cryptographic services, or hold or access cryptographic keys, should be clearly stated.

In recent years, relevant national regulations are becoming increasingly liberal to stimulate E-business processes. However, it is always important to check the cryptography usage situation on a case-by-case basis. There might be restrictions on import and export of crypto products as well as their use. An extensive survey on regulation of cryptography can be found in [Koops, 2001].

Digital signatures
The United Nations Commission on International Trade Law (UNCITRAL) defines an international framework for a derivation of national implementations. It has adopted model laws for electronic commerce and electronic signatures [UNCITRAL, 1996 and 2001]. In the EU, the legal basis forms Electronic Signature Directive [EU, 1999]. This directive facilitates electronic commerce through resolving infrastructure-related issues. It covers details about qualified certificates, certification service providers, signature-creation devices and signature verification procedures. The main goal of this directive is to enable electronic signatures to be admissible in court in member states. It should be pointed out that electronic signature is a very broad term, meaning data in electronic form that are attached or logically associated with other data and serve as a method of authentication, which does not require use of digital signatures and certificates. Of course, the most efficient authentication is enabled only through digital signatures and certificates. Therefore, the directive concentrates on this matter, starting with certification services. These services should be, conditionally said, market driven, i.e. without a need for prior accreditation. However, this does not mean that providers should not be subject to national supervision. On the contrary, there should exist certain national requirements, i.e. schemes for qualified providers. If such requirements are met, member state may not restrict the provision of certification services originating in another member state. Further, certification service providers should be liable for their operations up to a certain limit. Additionally, certification service providers should comply with Data Protection Directive [EU, 1995] with regards to processing of
personal data and their free movement: these data may be collected only directly from the subject or after explicit consent of the subject, and may not be used for any other purpose.

Many countries have already defined their national legislations and their implementations are frequently based on the above-mentioned models. A comprehensive reference to relevant legislation can be found in [Baker and McKenzie, 2002]. It includes international directives, enacted and pending regulation with summaries and related resources.

Intellectual property rights

Intellectual property rights (IPR) cover copyrights, patents, design rights and trademarks (for introduction see [WIPO, 2000]). Copyright infringement can result in serious consequences, even criminal prosecution. Traditional legal systems for intellectual property protection are based on sovereignty and territoriality. The global network challenges these issues significantly. From the security point of view and for the majority of businesses, copyright issues apply mainly to software. Thus, organizations should have a published copyright compliance statements, defined procedures for acquisition, installation and use of new software products, registers of copyrighted assets with proof and evidence of ownership and procedures to control compliance with licensing agreements [BSI, 1999]. Regarding patents, for the majority of users they may apply only to algorithms, e.g. in the US. From a wider security perspective, design rights and trademarks have to be considered in relation with Web services. Page designers should avoid using elements of proprietary literary and artistic works, while administrators should take care to prevent meta-tags that may violate trademarks. Trademark issues have also to be considered when registering domain names. Finally, an organization has to consider even such IPR issues like agreements with developers and designers of their website to prevent claims that they own the rights of that work.

Privacy rights

On the international level, the base for privacy rights is the OECD Privacy Guidelines [OECD, 1998]. These recommendations put forward the following principles: transparency regarding the collection of personal data, transparency regarding the use of personal data, and control of personal data and access to it by the individual. Privacy rights have can be addressed from two perspectives: internal and external entities.

With regards to external entities, websites should have a privacy statement, explicitly expressing the organization’s online privacy policy. US Federal Trade Commission recommends four practice principles that should be addressed: notice, choice, access, and security [Dreben and Werbach, 1999]. Similarly, the EU Data Protection Directive [EU, 1995], discussed below, requires processing of personal data only upon an individual’s specific, informed, and unambiguous consent. With regards to privacy issues for employees, workplace monitoring, retrieving and storing of employees’ communications has to be addressed. Organizations must decide what policies they wish to adopt concerning use and disclosure of electronic mail sent and received by their employees [Dichter and Burkhardt, 2001]. Web surfing policies should be put in place as well. Although these policies will vary among companies and jurisdictions, the following issues should be considered: employee privacy rights, the disclosure of confidential information, the rights of third parties to obtain access to company records, the company’s need to manage resources, the right of unions to access company employees via email.

Generally, workers in the US have few privacy protections in law. As a minimum standard, employee can expect a reasonable expectation of privacy. It is quite a different situation in the EU, where employees in public and private sector are secured by Data Protection Directive. This directive requires clearly defined purpose
for collecting personal data, including all data that enable to identify a person indirectly. The processing of these data is allowed only within the specified purpose, where processing includes collection, recording, storage, organization, adaptation, alteration, retrieval, consultation use and dissemination. Additional important limitations are:

- data may be processed only to the adequate extent
- data must be kept complete and up to date
- data can be stored only for the period, necessary for the stated use
- the consent of data subject should be obtained
- sensitive data, e.g. racial or ethnic origin, political opinions, religious beliefs, health and sex life must not be processed.

Finally, an entity that is processing personal data is responsible for their protection against destruction, alteration, disclosure or unlawful forms of processing. Of course, the above-mentioned measures do not apply in case of state security, criminal prosecution and alike.

Providers rights and responsibilities

Additional problems are related to service provisioning [Dreben, 1999]. The possibility for clients to post content on an organization's website has to be seriously analyzed, as the organization may be responsible for infringements and offensive or harassment messages stored on its site. In general, two main acts, [EU, 2000] in the EU and [US Congress, 1998] in the US, do not state a responsibility of a provider for content, if the provider is not aware of it or if the provider does not remove illegal content after being informed about it. As a countermeasure, companies should make clear that they are not original publishers of third party content. In the US, organizations can consider registering with the Copyright Office as service providers. This is likely to reduce a website operator's liability for copyright infringement that may occur without its knowledge. As a widely accepted business practice, a click-wrap approach is used. Before accessing services, a user is given terms and conditions. By clicking the appropriate button, the user is enabled to access site resources. Terms and conditions should include proprietary rights notices, disclaimers of liability and warranty for the site, linking disclaimers, framing prohibitions, a prohibition on using the site to transmit infringing material, dispute resolution clauses requiring arbitration, governing law and jurisdiction.

EU service providers should follow closely the Directive on Privacy and Electronic Communications [EU, 2002], which supplements Data Protection Directive. It covers relations between subscribers and service providers. The principle of subject's consent is preserved, while needs of service providers to process data that are necessary for their service provisioning are explicitly addressed. These data include naming, numbering, addressing, traffic related data (routing, beginning and end of communication, volume), location information, data, needed for charging etc. Further, service providers should safeguard the security of their services and inform subscribers of special risks, including those that lay outside the scope of their possible corrective actions. Informing users of particular security risks does not discharge providers from obligation to take necessary and immediate measures to remedy unknown security risks. Providers should prevent unauthorized disclosure of not only communications, but also operational data that are needed for communications. This does not prohibit processing of data that are needed to support or to improve operations. Such data may be further stored and even accessible to public if data referring to the individual subscribers or users requesting such information are erased. Further, when necessary and legally authorized, communications can be recorded to provide evidence of a commercial
transaction. However, the scope and purpose of Data Protection Directive should be taken into account. This means that parties should be informed about the recording prior to recording, and recorded communication should be erased as soon as the transaction cannot be lawfully challenged.

Spyware, cookies and similar technologies can be used, but only for legitimate purposes, with the knowledge of users concerned. Therefore, users have to be informed about such use, and have to have a possibility to refuse these techniques. It is generally advised to obtain users consent by any appropriate method, e.g. by ticking a box on a website.

**Inter-organizational issues**

Coordination of security activities

Successful management of E-business security requires coordination between organizations with reporting of incidents and coordination of countermeasures. These activities started at the end of 80s with establishment of so called computer emergency response teams. Many national governmental, industrial and educational emergency response teams now exist. In the US the main one is CERT Coordination Center, located at Carnegie Mellon University. These teams provide technical assistance and coordinate responses to security compromises through coordination, technical documents and training courses. They further coordinate their work at the international level within the Forum of Incident Response and Security Teams (FIRST). Following their activities is necessary, especially for on-time upgrades of compromised software components. Contacts should be maintained with response teams, and also with law enforcement authorities, regulatory bodies and service providers to ensure responsiveness in case of a security incident.

General interdependency

Security policy according to BS 7799 is mainly organization-centric. However, it is becoming increasingly important to think also in wide inter-organizational terms. There are growing trends to consider global dimensions. According to [Hunker, 2002], there are five critical dimensions, which are mainly yet to be resolved: measuring system risk and resiliency, managing and understanding interdependencies, overcoming barriers to technological change, selecting appropriate forms of infrastructure governance, developing efficient incentive structures, and adopting an integrated systems perspective.

Although Hunker is addressing all critical infrastructures and not only Internet, the paper is relevant since it has a lot to do with Internet security. Regarding system risk, there is no definitive and quantifiable risk measurement to underpin risk mitigation strategies. Regarding interdependencies, each organization is linked to billions of users in the Internet, which is a highly complex, non-linear system, especially as it inherently includes human factor. Modeling this point of view is a very difficult task, and research in this area is very much in its early stages. Hunker also stresses the importance of barriers to technological change, as advances in technology can often prevent threats, but the inertia of existing systems is mainly based on required investment and it is an open question how and whom to force to perform such transitions, and who should pay for them. The basis is certainly some kind of societal consensus in laws and public policy. This is linked to the problem of governance of the Internet infrastructure, which is currently governed loosely only by IETF that decides acceptable technological solutions in an open manner. To establish efficient incentive structures, the following is suggested: market forces, regulations, liability and contracts, voluntary standards, best practices, insurance, public disclosure, reputation and procurement.

---

1 Legal, and security issues in general, are especially important in marketing IS [Devetak, 1995], but they have been paid no attention until very recently.
Trust issues
Rapidly growing trends in collaborative and cooperative business relationships expose trust. Fundamental questions are [DeMaio, 2002]: can I trust entities and infrastructures on which I depend? Can involved organizations trust me? Together, can we trust our common infrastructure and processes? In order to achieve trust, an e-Trust initiative has been started, where each participant willingly continuously demonstrates that he/she is acting openly, honestly, following the rules and being controlled appropriately [DeMaio, 2002]. This demonstration comes in various forms and it is managed by Information Systems Security Certification Consortium, which is a non-profit consortium for training and certification of information security professionals.

Conclusions
Managing security in information systems has reached the point where sufficient, but dispersed, knowledge exists in various domains. Approaches related to security of IS are to be linked within appropriate methodology to achieve optimal and balanced solutions for an enterprise. This is the main motivation behind the paper, which should provide security practitioners with concrete steps and sufficient background on related issues. It is based on experience gained with a nation-wide project of establishing IP and smart card-based health care information system infrastructure [Trček, 2001].

When using the methodology presented in this paper, one should not forget the following: security of an E-business system is not a state, but a process that has to be incorporated into the system from scratch, and not treated as an afterthought. Moreover, it is not something that can be accomplished by technology alone — human resources play a central role. Thus, security should become an integral part of corporate cultures.

References
An Integral Framework for Information Systems Security Management

Denis Trček
