INFORMATION SECURITY - STRATEGY, CODIFICATION AND AWARENESS

Tamás Szádeczky

Abstract

Information security has an emerging importance, even in people's daily life, even in country-level policymaking, but these two are inseparable. National information security strategy, applied legal regulation and the actual awareness of citizen are interconnected. The article shows the legal regulation of the last decades in Hungary, the relevant laws and their impact on awareness. The interest of government, therefore the mass and deepness of law and so the awareness increased fairly these times.

1. Security implied by technology

During the last seven decades there was a huge advance in information technology. From the time Konrad Zuse made the first Turing complete computer in 1941 and the building of ENIAC, the first really universal computer in 1946, information security is still a part of information technology. [1][1] In the beginning they had a small common section, but it widened, though. Computers are processing sensitive data from the very beginning. For example ENIAC was used to do calculations regarding the atomic bomb. At that time physical security measures were enough prevent unauthorized access. The common usage of computers began with the implementation of multi-user mainframe computers mostly from the 1950s by IBM. While multiple users were accessing those systems, access control measures had to be implemented. The systems of universities were a real playground for hackers, who were testing the boundaries of those systems. The interconnecting of standalone systems became a usual solution to increase efficiency and collaboration quite early. The first point-to-point serial cable-based connections were inefficient, thus the Advanced Research Projects Agency (ARPA) started the 'Intergalactic Network' initiative to use the existing telex network for computer communication in 1962.[2] [2] Later ARPA started the ARPANET network in 1969 which connected University of California, Los Angeles (UCLA), Stanford Research Institute's Augmentation Research Center, University of California, Santa Barbara (UCSB), University of Utah's Computer Science Department in the beginning, but later it was broadened and in 1998 its name changed to Internet. Networking technologies implied the development of a new branch of information security: network security. It had to deal with phenomena like eavesdropping and man-in-the-middle attacks. Also the importance of cryptographic measures became more important then in the case of the defence of a standalone computer. With the usage of portable computers, notebooks, mobile phones, smartphones and tablets and especially with the bring your own device (BYOD) phenomenon the integration and secure connection to protected networks and security of the data on the move became new issues. Cloud computing technologies solved some problems of

[1] x

[2] Kita, 2003, p. 65.

reliability and business continuity, while generated new issues in outsourcing security, data portability and segregation.

A whole virtual world or cyberspace emerged on the ground of the above technologies shown above. Real world phenomena occur in this virtual world with more or less the same symptoms. Criminologists and lawyers can debate that the perpetration of certain crimes in the virtual world and real world differs or not, but the method of protection and security technology is unanimously differs from the real word's. Information security absorb elements from the traditional security areas such as military defense, burglar alarm or fire prevention, but it also have new attributes.

New technologies are appearing each year. Most of them cause new problems, opens new vulnerabilities. Those issues have to be solved by information security, but they are always tracking controls, because there is a delay between the implementation of the technology and the implementation of the effective adequate security control. This is because at the time of development the developers find out some security issues and implement some security controls against them, but more problems and vulnerabilities are visible afterwards, when hackers are challenging systems. At this point we have to implement newer and newer controls to protect our systems. This is a never-ending story which needs continuous awareness on security.
Intensive enhancement of the technology, possibilities and purchasing power did not involve the application development with the same rapidity. By the way the security of network-based activities did not reach the reassuring level. The enhancement and legal usability of public key cryptography and strong secret key algorithms gave the possibility to the computer users for secure communications, but it is still not enough. Security of a computer hardware element, computer system or network depends on the full picture, thus the weakest part's security determines the security level of the overall system.

In those decades the security profession fought for legitimacy of cyber security, and high level management more or less knows the importance of this area. The question at the beginning of the twenty-first century is not the *why* but the *how* and the *how much*. In the business sector, especially in times of economic crisis, costs can't be enough low and there is no compulsory expenditure from which they don't want to cut off a bit. The management's aim is to nominate the minimal security of IT elements, systems and networks in every aspect. The goal for citizens, shareholders, stakeholders and the government is the same: adequate information security level should be established and maintained. Every day we find that the decrease in IT budget implies much more decrease in security budgets. While in the case of a major telecom company it is hard to find serious deficiencies, the home computer users often don't install even free security tools. Obviously this can happen because of many reasons: for example lack of technical knowledge, experience, information, money, or interest. But the most important is that people don't draw enough attention to this area, despite of later they might be liable for that. By the legislator's point of view, everything can be improved and the goal is to reach perfection. Information security also deal with this issue in security awareness.

2. Early strategies and legislation 1989-2008

The above mentioned technical improvement made local system security improvements necessary. From the viewpoint of the government a higher layer of problem also exist: attack against multiple systems or a full infrastructure. This can take part of a conventional war as cyberwar or may be an unconventional event, as a cyberterrorist attack.

As a short bypass we should anatomize the word *cyberterrorism* for a while, but please notice that there is a huge debate regarding this topic and more scientific papers analyse this topic. According to Gorge [3] [3] the word cyberterrorism should be interpreted by its syllables. Cyberspace is the mass of computer communication networks. The term was created by William Gibson and was first used in science fiction novel Neuromancer, which was written in 1984. It meant collective hallucination by billions of people. Use of the term cyberspace emphasizes the close relationship between the networks, relationships between people and networks, and social networks, in contrast to the concept of network which has primarily a technical meaning. According to Benjamin Netanyahu[4] "Terrorism is the deliberate and systematic murder, maiming, and menacing of the innocent to inspire fear for political ends." [4] According to the U.S. Federal Bureau of Investigation,[5] cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." [5] But what kind of technical steps a cyber-terrorist do? The same, or very similar, as an online criminal does. The differences are the impact and the effort. This is why we have to defend all individual systems in order to protect the full infrastructure.

From the government's viewpoint we have to plan and prepare the national defence system against such actions. The first comprehensive security and defence policy system of Hungary after the political change in 1989 did not recognised cyber threats. Neither the National Assembly resolution no. 94/1998 (XII. 29.) on the security- and defence policy principles of Republic of Hungary, nor the Government resolution no. 2073/2004. (IV. 15.) on the National Security Strategy of Republic of Hungary, nor the Government resolution no. 1009/2009. (I. 30.) on the National Military Strategy of Republic of Hungary included cyber defence as an objective. According to these policies and strategies the defence against cyber attacks are treated individually, even in the legal regulation.

We may find an example of information security regulation in Hungary in the field of personal data protection (privacy or personally identifiable information protection in US law). [6][6]

As a general obligation all institutions managing and processing personal data, except private users has fallen under Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest or later Act CXII of 2011 on informational self-determination and freedom of information. The security requirements were almost the same.

Section 7 (2) about data security requirements says that "Data managers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing." [7][7] Relying on the analysis by András Jóri [8] in his handbook [8] it can be claimed that data security and so a slice of informational security falls under the scope of the statutory regulation pertaining to data protection. According to subsection (3) "Data must be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be

[3] Gorge, 2007, p. 9.

[4] Netanjahu, 1995. p. 20.

[5] FBI?

[6]

[7]

[8] Jóri, András: Adatvédelmi kézikönyv. Elmélet, történet, kommentár. [Handbook of data protection. Theory, practice and commentary.] Osiris, Budapest, 2005. p. 258.

corrupted and rendered inaccessible due to any changes in or modification of the applied technique." The legislator gives examples of threats which in general correspond to standards. It is recommended to make a risk analysis about risks threatening the system and process of handling and processing data and about their occurrence. It is not required by the act on data protection, but normally is required by all standards, so it is also a professional expectation.

This law is not detailed, nor explained, no controls are built to the law. Parliamentary Commissioner for Data Protection and Freedom of Information (later the Hungarian National Authority for Data Protection and Freedom of Information) supervised those data management and data processing, but have no coercive measures; despite of a part of data security is subject of personal data regulation. [8] The publicity is effective only in governmental cases. The Act IV of 1978 on the Criminal Code specified Misuse of Personal Data in Section 177/A. statement of facts:
(1) Any person who, in violation of the statutory provisions governing the protection and processing of personal data:
a) is engaged in the unauthorized and inappropriate processing of personal data;
b) fails to notify the data subject as required by law;
c) fails to take measures to ensure the security of data;
and thereby imposes significant injury to the interests of another person or persons is guilty of a misdemeanour punishable by imprisonment for up to one year, community service, or a fine.
(2) The acts described under Subsection (1) shall be upgraded to felonies and punishable by imprisonment for up to three years if they are committed by a public official in the course of discharging a public duty or in the pursuit of unlawful financial gain or advantage.
(3) Any misuse of special personal data shall be treated as a felony punishable by imprisonment for up to three years.

Another example for not detailed rules is electronic communication sector.
Due to Act C of 2003 on Electronic Communications Section 156:
(1) Service providers shall take appropriate technical and organizational measures - jointly with other service providers if necessary - in order to safeguard security of their services.
The focal point of this paragraph is intended cooperation between service providers for security reasons. This means mostly access control measures.
(2) The technical and organizational measures shall be sufficient - with regard to best practices and the costs of the proposed measures - to afford a level of security appropriate to the risk presented in connection with the services provided.
This requirement suggests risk assessment and appropriate security measures. Despite significance and sensitivity of ICT area, the regulation and detailed requirements are scanty, even in decree-level regulations.

There were also well detailed laws of information security in this period. In this case regular audit is done by authorities, like in the regulation of financial sector. Financial sector is regulated by Act CXII of 1996 on Credit Institutions and Financial Enterprises (Hpt.), Act LXXXII of 1997 on Private Pensions and Private Pension Funds (Mpt.), Act XCVI of 1993 on Voluntary Mutual Insurance Funds (Öpt.), Act CXX of 2001 on the Capital Market (Tpt.) and Act LX of 2003 on Insurance Companies and Insurance Activity (Bit.).
Before 2004 the regulation of this field was similar to data protection act. Hpt. section 13. About Personnel and Material Requirements was the only obligation of security: "Financial service activities may be only commenced or performed if the requirements pertaining to the technological, informatics, technical, and security background and the premises suitable for carrying out the

activities, information and control system for reducing operating risks, and a plan for handling extraordinary situations" [9] [9]

More details and a more precise requirement list were introduced by Act XXII of 2004 on Amendment of Acts Related to Increased Defence of Investors and Depositors and Act CI of 2004 on Amendment of Acts Related to Taxes, Contributions and Other Budget Payments. The acts embodied the similar requirements of Protection of Information Systems to Hpt. 13/B. §, Mpt. 77/A. §, Öpt. 40/C. § and Tpt. 101/A. §. In the case of Tpt. 101/A currently the requirements changed and moved to Government Decree No. 283/2001. (XII. 26.) of the Cabinet. Bit. was not amended, but same controls are recommended by the Hungarian Financial Supervisory Authority [10].[10] "*Financial institutions are required to set up a regulatory regime concerning the security of their information systems used for providing financial services and financial mediation, and to provide adequate protection for the information system consistent with existing security risks. The regulatory regime shall contain provisions concerning requirements of information technology, the assessment and handling of security risks in the fields of planning, purchasing, operations and control.*" The regulatory regime refers to the system of regulations like IT security policy, IT security laws, IT operational regulations. These regulations should be made and regularly (for example yearly) updated by the management. All users must know the relevant regulation.

"*Financial institutions shall review and update the security risk assessment profile of the information system whenever necessary, or at least every other year.*" The organisation must implement a risk assessment procedure and regular assessments. In case of usage of outsourced services the organisation must include the outsourced areas to the assessment, as well. "*The organizational and operating rules shall be drawn up in light of the security risks inherent in the use of information technology, as well as the rules governing responsibilities, records and the disclosure of information, and the control procedures and regulations integrated into the system.*" Roles, tasks and responsibilities have to be clearly defined without any incongruity. Scope of authority of workers has to be adequate to the role and responsibility. A Chief Information Officer (CIO) position should be formed as a responsible for IT. According to subsection 4, "*Financial institutions shall install an information technology control system to monitor the information system for security considerations, and shall keep this system operational at all times.*" This requirement does not refer to a computer system or application, but to a set of controls and effective internal audit system. This control system has to be regularly revised; activity and effectiveness should be measured. Keeping these controls up to date is a requirement in more standards. "*Based on the findings of the security risk analysis, the following utilities shall be implemented as consistent with the existing security risks*" Risk assessment in paragraph (2) is the starting point of the followings. "*Clear identification of major system constituents (tools, processes, persons) and keeping logs and records accordingly.*" The organisation has to make an inventory of configuration. The actual state and all previous states have to be accessible and all time up to date. "S*elf-protect function of the information technology security system, checks and procedures to ensure the closure and complexity of the protection of critical components.*" At this point the most important is the conformity of security measures with business and organisational requirements. This conformity conducts to proportionate defence. [11][11] According to bullet c, "*frequently monitored user administration system operating in a regulated, managed environment (access levels, special entitlements and authorizations, powers and responsibilities, entry log, extraordinary events)*" Identity- and access management procedures and rules have to be created,

[9] x

[10] x

[11] x

with rules responsible for databases. Changes in position or responsibility have to appear immediately in access levels. In d), "*a security platform designed to keep logs of processes which are deemed critical for the operation of the information system and that is capable to process and evaluate these log entries regularly (and automatically if possible), or is capable of managing irregular events."* Application of log analysers used widely in the industry should be used. If not, log saving, secure archiving and manual analysis is the minimum. *"Modules to ensure the confidentiality, integrity and authenticity of data transfer."* Secure channels or protocols have to be used for communication, like HTTPS, SSL, SSH, SFTP. [12][12] *"Modules for handling data carriers in a regulated and safe environment."* Data storage media, like DVDs, magnetic tapes have to be stored securely. It is necessary to protect them against disaster losses, incidents because of deficiency of technical requirements, electromagnetic disturbances, and technical reliability problems, protect against intentional damage and access management. Point g) requires *"virus protection consistent with the security risks inherent in the system."* Protection against malicious programs is necessary in servers, desktops and also in mobile devices. According to (6) *"Based on their security risk assessment profile financial institutions shall implement protection measures to best accommodate their activities and to keep their records safe and current, and shall have adopted the following."* Requirements declared in this point are minimum requirements, all of them are obligatory. *"Instructions and specifications for using their information system, and plans for future improvements"* means every systems and applications have to be documented. All services must have Service Level Agreement (SLA). *"All such documents which enable the users to operate the information system designed to support business operations, whether directly or indirectly, independent of the status of the supplier or developer of the system (whether existing or defunct)"*, so within the scope of availability plan, all of these acts are included. *"An information system that is necessary to provide services and equipment kept in reserve to ensure that services can be provided without any interruption, or in the absence of such equipment, solutions used in their stead to ensure the continuity of activities and/or services."* Disaster Management Plan and Business Continuity Plan are eligible for this requirement. *"An information system that allows running applications to be safely separated from the environment used for development and testing, as well as proper management and monitoring of upgrades and changes."* Separation of working and test environments is an industrial common necessity. [13][13] Also the personnel of these systems should be different. *"The software modules of the information system (applications, data, operating system and their environment) with backup and save features (type of backups, saving mode, reload and restore tests, procedure), to allow the system to be restored within the restoration time limit deemed critical in terms of the services provided. These backup files must be stored in a fireproof location separately according to risk factors, and the protection of access in the same levels as the source files must be provided for."* System backup operations also should be regularly tested. "A *data storage system capable of frequent retrieval of records specified by law to provide sufficient facilities to ensure that archived materials are stored for the period defined by legal regulation, or for at least five years, and that they can be retrieved and restored any time"*. Retrieving of data is necessary in lot of cases, for example tax revenue, anti-terrorism, data protection. A complex solution for them must be implemented, like a well-secured magnetic tape data storage system. *"An emergency response plan for extraordinary events which are capable of causing any interruption in services."* Disaster Management Plan and Business Continuity Plan mentioned at paragraph c) are eligible for this function. According to para 7 *"Financial institutions shall have available at all times: operating instructions and models for the inspection of the structure and operation of the*

[12] x

[13] x

information system they have developed themselves or that was developed by others on a contract basis." Available at all times means before authorisation of financial service and after that at 24/7. According to the above, all software documentations must be present and up to date. "*The syntactical rules and storage structure of data in the information system they have developed themselves or that was developed by others on a contract basis*" Software documentations, especially database documentations must contain data definition. "*The scheme of classification of information system components into categories defined by the financial institution.*" The computers, systems and networks have to be classified on its sensitivity. These rules have to be documented. They shall have available "*description of the order of access to data.*" Written rules of access control must be present. They shall have available "*the documents for the designation of the data manager and the system administrator.*" These documents have to be present in order to ascertain personal responsibilities. They shall have available "*proof of purchase of the software used.*" Also as a tax revenue requirement all software licenses and invoices must be present. A software inventory is also necessary. They shall have available "*complex and updated records of administration and business software tools comprising the information system.*" With a software inventory this requirement will be satisfied. "*All software shall comprise an integrated system, that is capable of keeping records of the data and information required for regular operations and as prescribed by law.*" This paragraph defines software minimum requirements. As it was mentioned above, long time preservation is required in more fields. The software also has to facilitate this. "*That is capable of keeping reliable records of moneys and securities*" Since money is nowadays mostly account money (has no physical form), reliable records of that is essential for trust in financial system. "*That has facilities to connect, directly or indirectly, to national information systems appropriate for the activities of the financial institution.*" Most administrational data is changed via computer systems, like tax revenue, statistical information. Implementation and maintaining interfaces to them is the responsibility of the organisation. "*That is designed for the use of checking stored data and information.*" Embedded controls for data self-correction and correction is imperative in such large databases. "*That has facilities for logic protection consistent with security risks and for preventing tampering.*" Value and sensitivity of stored data need endeavour on hardening logical security. According to para 7, "*the internal regulations of the financial institution shall contain provisions concerning the knowledge required in the field of information technology for filling certain positions.*" In other fields job descriptions contains required IT knowledge, but financial institutions have to determine them in regulations. As the mass of requirements shows, financial sector has much more regulations than sectors above. Reason of this is the importance and significance of this field. Most citizens keep savings in those organisations. A defect in the financial institution drastically decreases trust in the sector and the financial system inducing significant losses.

Before the Act on Electronic Public Service (before 29 June 2009) there was no acts dealing with information security in public- or governmental networks. [14] [14]

Only the following Government decrees regulated the field:

- 195/2005 (IX. 22) Government Decree on security, interoperability and uniform use of electronic administration systems
- 84/2007 (IV. 25) Government Decree on security requirements of the Central Electronic Service System and related systems
- 193/2005 (IX. 22) Government Decree on Detailed rules for the electronic filing

[14]

- 194/2005 (IX. 22) Government Decree on requirements for electronic signatures and the associated certificates used in the administrative proceedings, as well as requirements for certification service providers issuing the certificates
- 182/2007 (VII. 10) on the regulation of the central electronic service provider system

These gave rules sporadically to some systems, without any general framework.
As a result we may say that relatively low awareness of the legislator and the business is observable in usage of international IT security standards, despite its significance and high risk in some areas. No obligations found in acts of Hungarian Parliament for usage of standards in IT security. There are built-in self-control procedures in some acts, but in practice those procedures does work efficiently.

3. Interim strategy of 2009-2012

In 2009 a small change commenced with the adoption of Act LX of 2009 on electronic public services (abbreviated as Ekszt.). It has highlighted the requirement of security as a basic principle. Organizations providing electronic public services ensure the publicity of data of public interest (according to act on data protection and freedom of information) and protection of personal and any other data protected by during the provision of services. [15][15] During the provision of services particular attention must be paid to the realization of information rights, protection of classified information, business secrets and other protected data groups. Service providers ensure IT security, including the integrity of electronic records, and applicability of electronic signature technology. The legislator refers to the application of electronic signature technology and the importance of compliance with the relevant security requirements. The use of electronic signatures, according to Act on electronic signature (hereinafter Eat.) can greatly assist in maintaining the integrity of data. However, a huge discrepancy is observable between the principles and the practice. Despite of the above rules, electronic signatures are still not widely adopted and rarely usable in such systems.
The service providers shall ensure the continuity of the operation and enforcement of the requirements for the information systems collaboration. Interoperability, i.e. cooperation between the various systems has particular importance in the government information technology, as island-like systems have been developed, and over time the demand of integration increased fairly. Negative impact of island-like development is still being felt in the area of interoperation. The continuity of operation, as one of the main requirements for IT security, including disaster and business continuity planning, is an important feature for large government databases, where data loss can be catastrophic.
Data transmitted to the central system profiling (analysis of user habits, personal information and direct access to meaningful case data) is not allowed. Compliance will be ensured with the central system operator by means of technical solution. Profiling, one of the most challenging privacy issue in recent years is declared to be prohibited by a principle in Ekszt. The system must ensure this technically (e.g. through Privacy by Design technologies).
Use of remote services require a face-to-face pre-registration or an equivalent measure. Given that a significant number of electronic public services are administrative procedures, so they need proper identification. Personal appearance and identification means a registration in governemental offices or registration by electronic signature.

[15] Ekszt. 4. § (1) Az elektronikus közszolgáltatás alapelvei

Authenticity, quality, operational security and confidentiality of the data processed in electronic public services operate under the Central System must comply with defined rules. Here the act refers to Government decree no. 223/2009 (X. 14) about the security of electronic public services. In that the requirements and procedures were determined in sections from 11 to 32. Requirements set out in the Act are detailed in the following regulations:

- Government decree 223/2009 (X. 14) on the security of electronic public services
- Government decree 224/2009 (X. 14) on the central electronic system service's recipient identification and authentication services
- Government decree 225/2009 (X. 14) on electronic public services and their use
- Government decree 78/2010 (III. 25) on requirements of electronic signatures in administration and certain rules for electronic communication

There was a bill on information security in 2009, which never came to force, but had a remarkable impact on the area. [16][16] The proposal was a draft legislation framework, a so called lex specialis. The bill's scope was all IT systems and services in the Republic of Hungary, including private computers. It was applied to the operators and users, also.

The information systems are divided into 5 separate security level. One of the factors of the grouping was storage of personal data. The groups were as follows:

- Level 1: home computer networks and individual computers connected to the Internet
- Level 2: information systems used by every legal relationship between employer and employee, internal IT network, limited internal access non-public electronic communications services or internal network or individual computer capable to use public electronic services
- Level 3: any public electronic services that don't handle, store, process or transfer personal identifiable information, including anonymous registration services
- Level 4: organization providing public electronic services, application service provider and its public electronic services, regardless to personal data processing; any public electronic services that handle, store, process or transfer personal identifiable information
- Level 5: critical infrastructure sector's computer system, closed-circuit, and public electronic network or services and information technology

One of the most interesting questions is the mandatory audit required at level 4-5 as a means of control. By the intention it would have conducted by audit companies that are accredited by the National Accreditation Body for certification activity. Creator of the legislation could not tell that it belongs to management system or product certification. The social impact of the law would have been significant, at least because the scope is wide. Critics said there is lack of audit control in level 1 to 3, which make it a redundant regulation. In contrast, the legislation could have set the level of security requirements under other laws, because of its lex specialis character. For example, in Criminal Code Section 423 *adequate protection* is required in the case of hacking, but it was not defined before. The new law might give content to it, so increasing legal certainty.

4. Latest information strategy from 2012

[16] MeH: Előterjesztés a Kormánynak az informatikai biztonságról szóló törvényről. 2009.

Government Decision no. 1035/2012 (II.21.) on Hungary's National Security Strategy requires the strengthening of the security of electronic information systems to enhance the protection of critical national information infrastructure, and the development of adequate cyber defence. Detailing the above mentioned statement of the National Security Strategy, the Government adopted a National Cyber Security Strategy of Hungary as well. [17] [17] The legislator took the view that recently experienced cyber wars worldwide justify the coding of a modern Hungarian Information Security Act. 25th April 2013 was a huge milestone for the administrative control of information, when Act L of 2013was published on electronic security of state and local government bodies.

The scope of the act, despite of its title and scope definition in Section 2, is significantly wider as it seems to be. [18] [18]Because of the following scope (extension): data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements, as defined by law. These bodies can significantly extend the scope (even with private companies), so typically the public utility providers, electronic communications services, financial organizations can be included. An itemized list is not yet published. The law prescribes confidentiality, integrity and availability as information security requirements in electronic information systems and data, so the essential items known as CIA triad in information security field. [19][19]

The Act requires the integrity and the availability of information systems in a closed, complete, consistent way, proportionate to the risks for the electronic system and components. It is important to explicitly include the security control implementation’s proportionality to risks and usage of risk assessment in the state information security requirements, because security measures are typically implemented in an ad hoc manner, to minimize security budgets.

In order the protection of electronic information systems and data managed in them, proportionally to the risks, the Act states that the electronic information systems must be allocated to a security class. This classification is based on confidentiality, integrity and availability properties in a scale of 1 to 5 where 5 is the highest security level. From this section of the Act it seems that each part of CIA factors (confidentiality, integrity and availability) have to be evaluated separately, but from other parts of the Act we don’t find this separation.

Although the security classification depends primarily on the security classification of information, the law, in contrast to the earlier bill, does not specify what minimal security controls should be applied to data. In contrast, in Section 9 (2) it determines the minimum security level classification for a variety of organizations. This probably will mean that the security needs of data will not be evaluated, but the set the security levels according to the minimum-list, because public sector tries to invest as few as possible in security. According to the Act Section 7 para 5, in *exceptional circumstances*, the manager of the organization may set a lower security class may. Which also provides an easier way to avoid spending on security.

The only thing that can stop this expected downward bidding, the strictness of National Electronic Information Security Authority based on Section 9 Para 4. The authority is formed by Act Section 14 Para 1.

The minimum grades in the Act per organizations according to Section 9 Para 2:

- Level 1: no organizations (no requirements at this level)
- Level 2: Office of the President, Office of the National Assembly, the Constitutional Court 's Office, Office of the Commissioner for Fundamental Rights, local and national self-governmental bodies, the administrative authority associations

[17] 1139/2013. (III.21.) Korm. határozat

[18] muha

[19] ibtv

- Level 3: central state administration bodies, the National Judicial Office, courts, prosecutors' offices, the State Audit Office, National Bank of Hungary, the capital city and county government offices
- Level 4: Hungarian Defence Forces
- Level 5: data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements, as defined by law

The law does not define what these security levels are, how should the classification be conducted and what are the detailed rules for the levels.

According to Section 11 Para 1 (c), the head of the organization is obliged to appoint a person in charge of the electronic information system security, who is responsible for tasks related to the protection of electronic information systems. The list of tasks includes responsibilities of a conventional chief information security officer (CISO). Its name and definition suggesting that this person exempt the head of the organization and its employees from their security related task, but this mustn’t be the case.

The Act set up the National Electronic Information Security Authority under the Ministry of National Development. As a specialized authority, National Security Authority in involved in their activities with forensic log analysis and vulnerability testing. The Government Computer Emergency Response Team (CERT) responsibilities of the defunct Puskas Tivadar Public Foundation moved to disaster management, which is currently lack of information security skills. According to Section 23 the National University of Public Service develops training for those responsible for the security of electronic information systems and staff organizations. This development has finished and trainings are being held currently.

5. Consequences

Overall, the trend in recent years shows a more definite legal regulation, even with inception of technical standards in legal regulations. Due to the wide range of important legislation in the long-term wide social effects and improvement of information security awareness are expected. Probably the standard-based (e.g. ISO 27001 or COBIT) systems will multiply, given the fact that the organizations will already comply with the security rules. Certification of information security improves the trust in those systems, therefore it has also a public relations and marketing advantage. It worth to certify the organization’s management system against an international standard to use this advantage in the case of present legal compliance. The regulations will result in greater security and the national security risk in the area of information and communication technologies will decrease in the long term. The Act is a good step in the direction of the appropriate level of government information security, but it still provides loopholes from the application of the rules.

6. References

[1] KÖPECZI, B (ed.) et al., Az embergéptől a gépemberig, Minerva, Budapest, 1974, p. 206.

[2] KITA, C. I., J.C.R. Licklider’s Vision for the IPTO, IEEE Annals of the History of Computing, no. 3., 2003, p. 65.

[3] GORGE, M., Cyberterrorism: hype or reality?, Computer Fraud & Security, no. 2, 2007, p. 9.

[4] NETANJAHU, B., Harc a terrorizmus ellen, Alexandra, 1995. p. 20.

[5] TIEFENBRUN, S., A semiotic approach to a legal definition of terrorism, ILSA J. Int'l & Comp. L., 2002. p. 371.

[6] SZÁDECZKY, T., IT Security Regulation and Practice in Hungary, New challenges in the field of military sciences 2010 konferenciakiadványa, ZMNE, Budapest, 2010.

[7] Hungarian Act CXII of 2011 on informational self-determination and freedom of information

[8] JÓRI, A., Adatvédelmi kézikönyv. Elmélet, történet, kommentár. [Handbook of data protection. Theory, practice and commentary.], Osiris, Budapest, 2005. p. 258.

[9] Hungarian Act CXII of 1996 on Credit Institutions and Financial Enterprises

[10] A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről. [Hungarian Financial Supervisory Authority’s guide no. 1/2007] p. 3.

[11] ILLÉSI, Zs., Számítógép hálózatok krimináltechnikai vizsgálata, Hadmérnök, 2009. no. 4.

[12] VIRASZTÓ, T., Titkosítás, adatrejtés. [Cryptography, data hiding], NetAcademia, Budapest, 2004, p. 133.

[13] ISO/IEC 27002:2005 10.1.3. and 10.1.4. p. 60.

[14] DEDINSZKY, F., Informatikai biztonsági elvárások, MeH-EKK, Budapest, 2008, p. 4.

[15] Hungarian Act LX of 2009 on electronic public services

[16] MeH, Draft of act on information security, 2009.

[17] Hungarian Government decision no. 1139/2013. (III.21.)

[18] MUHA, L., KRASZNAY, Cs., Kibervédelem Magyarországon: áldás vagy átok?, HWSW ONLINE, 2013: Paper 5026. (2013)

[19] Hungarian Act L of 2013 on Electronic Security of State and Local Government Bodies