ISSUES OF LEGAL REGULATION OF HUNGARIAN HIGHER EDUCATION IT SYSTEMS

Ferenc Koczka[1]

DOI: 10.24989/ocg.v341.22

Abstract
The operation of IT systems of Hungarian higher education institutions is governed only by general law. These institutions have a large amount of personal, economic and research data. The management of these organizations is defined by internal regulations which are not controlled in terms of form or substance. As a consequence, the security of Hungarian higher education IT systems currently varies from institution to institution. Internationally, the first step in the legislative regulation of higher education systems was published in the United States in 2004, followed by only general rules from European legislators. In recent years, however, this situation has changed, and in several countries, including Hungary, the extension of the legislation on state institutions to higher education systems has begun. At present this has manifested in placing of research institutes under national security protection. In the light of international trends and Hungarian development, it is expected that this process will continue.

One possible way to raise the IT security level is to place higher education institutions under Act L. of 2013. This, in addition to not being a simple process, would create a serious financial burden for the maintainer and would have a noticeable impact on institutional autonomy, teaching and research freedom. There is currently no public source of information on IT incidents or their success and management in higher education IT systems in Hungary. In my presentation, I review the IT data assets of Hungarian higher education and based on my personal experience, I give an overview of IT attacks on the sector and a what can be expected based on changes in the L. Law of 2013.

1. Informatics in Higher Education

The world economy has changed at an unprecedented rate with the emergence of the internet. With few exceptions to economic competition, those who introduced and applied IT developments were allowed to remain viable, while other organisations, especially public organisations, had to adapt. Each country has developed its registration systems and electronic administration processes according to their level of development. Over the past decade, the number of cases that can be dealt with electronically has increased for both institutions and citizens. As a result, today's IT systems in developed countries handle large amounts of data, the protection of which has become critical.

Hungarian National Security Strategy [4] highlights the importance of protecting information systems and cyberspace on a number of points and draws attention to the potential for operational disruptions to affect the country as a whole. To this end, these countries have developed their own cybersecurity frameworks that define their legal environment and defense organisations. Their

[1] Eszterházy Károly University, Eger, Eszterházy square 1., Hungary, koczka.ferenc@uni-eszterhazy.hu, https://www.uni-eszterhazy.hu

primary objective is to maintain the functioning of the economy, to protect the economic system and the public sector. The operation of areas outside them is little regulated, even if they are maintained by the government. This is why, with a few exceptions, institutions in the academic sphere are subject only to general legislation.

However, the role of universities and research institutes has grown significantly in these areas in recent years. Research on COVID-19 was also carried out by higher education research teams, while their IT systems only operate according to their internal rules. Although the research unit of some universities in Hungary has been placed under national security supervision, there are already visible signs in some countries that in the future the IT systems they operate will be able to function under much stricter legal regulations.

The central issue of this article is the examination of the legal regulation of Hungarian higher education IT systems and the fact that the existing rules are no longer sufficient.

2. Legal Environment, Services

The Hungarian cybersecurity framework is relatively well defined and covers the legal and organisational areas necessary for the performance of cyber defense. The strategic context is based on the National Security Strategy and the National Cybersecurity Strategy [6]. This Government Decree of 2013 needs to be updated from time to time due to the rapid development of information technology and in order to be in line with the EU Directive on the Security of Network and Information Systems.

Hungary's National Security Strategy focuses on the protection of Hungarian cyberspace, attacks from cyberspace, and the avoidance of their negative effects. Its military approach is in line with international practice, which defines cyberspace as the fifth area of operations, defining cyber assets capable of causing significant material damage as weapons. It sets the task of developing the cyber capabilities of the Hungarian forces and emphasizes the importance of international cooperation. It identifies e-government as a priority sector, as well as utilities, strategic companies, and vital components. The strategy identifies organized crime, international terrorist organizations, cybercrime groups, extremist religious communities, private security companies and international networks as the most common perpetrators of cyber-attacks. It highlights the growing intensity of cyber-attacks, the importance of research into this, and the importance of user information security.
The main goal of Hungary's National Cyber Defense Strategy is to draw the attention of political and professional decision-makers to the existence and management of cyber security problems. The strategy is in line with the recommendations of the “Cyber Security and Defense” 2012/2096 (INI), NATO's Strategic Concept for 2010, the Cyber Defense Policy for 2011 and the Alliance's cyber defense principles and objectives.

Neither the National Security Strategy nor the National Cyber Defense Strategy mentions higher education institutions.

At the top of the organisational hierarchy of Hungarian cyber defense is the Ministry of The Interior (BM), which is different from general international practice. State and local government organisations are supervised by the National Cyber Defense Institute (NKI) within the framework of the National Security Service (NBSZ), which covers three professional areas. The Government Event Management Center (GovCERT) is an organisation specialized in threats or attacks from cyberspace. The National Electronic Information Security Authority is responsible for enforcing the

law and verifying their compliance. The Security Management and Vulnerability Investigation Department supports the operation of organizations covered by the Information Security Act [5], including the development of their security capabilities. NISZ Zrt. provides centralised infrastructure and related services to the entities covered by the law. The NAIH is an independent authority under the Constitution.

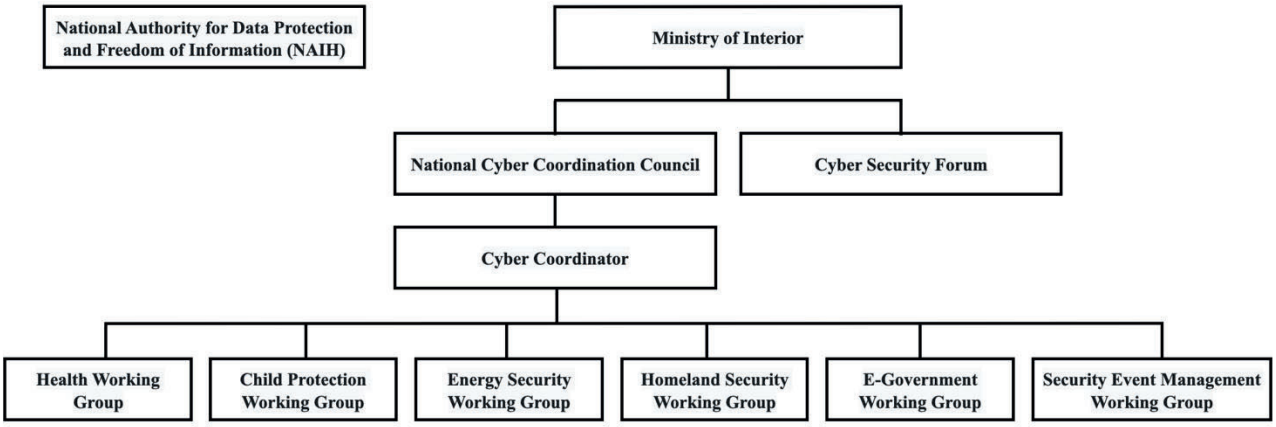

Figure 1: Strategic level of Hungarian cyber defence. It was created by the author.

These organisations do not provide IT security services to the academic sphere. GovCert's activities in higher education appear only secondarily, and HM CERT, which operates within the Military National Security Service of the Ministry of Defense, specializes exclusively in military organisations. Systems of municipalities and hospitals are regularly inspected, sometimes carrying out vulnerability checks and indicating the vulnerabilities discovered. Higher education is not within the scope of any of them, so with a few exceptions, they only report spam activities. CSIRTs are not responsible for handling damage which has occured, they are not investigative officials and therefore do not have such authority. For higher education, in theory, these tasks are performed by two organizations, Hun-CERT and KIFÜ CSIRT. The stated aim of the former is to provide professional and network security advice to the entire Hungarian Internet community. The Government Information Technology Development Agency (KIFÜ) is an organisation managed by ITM, which supports, among other things, Hungarian public education, public collections, higher education and research institutions. Its aim is to develop the IT infrastructure of the institutions and to provide the services based on it, as well as to operate the KIFÜ CSIRT. Its main services, which can be used free of charge, are the improvement of cyber security, the forecasting and prevention of incidents, and the provision of regular information. Unfortunately, it is not the priority of the CSIRT's to protect higher education. There are a number of incidents in middle education institutions, thus the KIFÜ CSIRT's services are mainly targeted at those.

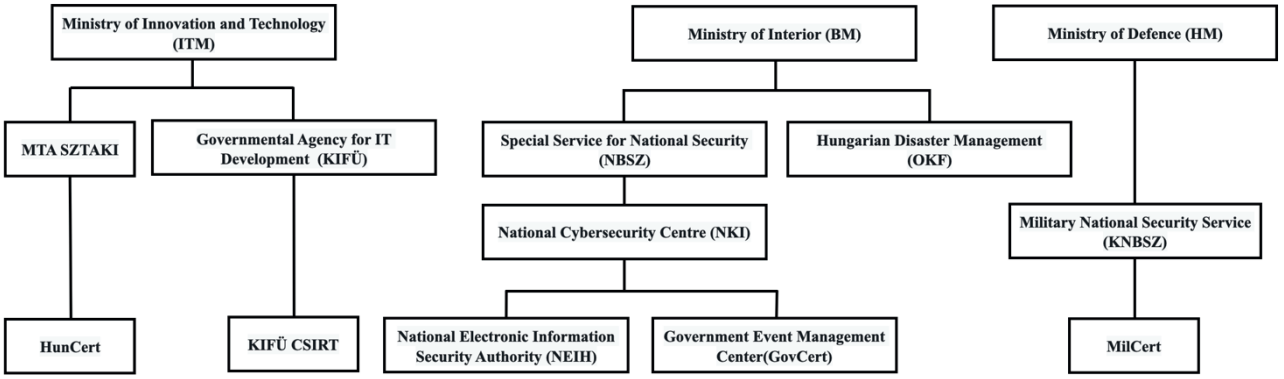

Figure 2: Operational level of Hungarian cyber defence. It was created by the author.

The protection of research institutes and research results is not based on legislation of general application. The 2009/2015 Government Decision[2] placed the research teams and research institutes of the Budapest University of Technology and Economics, the University of Debrecen, the University of Dunaújváros, the University of Pécs and the University of Szeged under national security supervision, but they do not cover the entire Hungarian research sphere. In the case of protected institutions, the National Security Service shall provide security protection against threats from cyberspace in its information security functions and shall require the relevant departments to comply with stricter data protection procedures.

Strict regulations are not common in foreign practice either, but as of 2004 the need to protect higher education IT systems and the creation of legislation can be traced back. Since 2004, the State of California in the United States has been required to report data breaches. Due to the rising number of incidents and the alarming amount of data leaked, a similar law has been put in place in other states of the country within a number of years, which has highlighted the numerous incidents in education systems. Since 2011, such cases have also been reported in Australia, Canada, India, Italy, Pakistan, the United Kingdom, Norway, New Zealand, Belgium, Mexico and Morocco. These cases have predicted the general spread of the notification obligation and made clear the need for regulation.

Australia has recently put its universities squarely in the critical infrastructure category, making it the first to assume its maintenance burden [1].

3. Higher Education's Data Assets, Motivations for Attack and Incidents

Defining cost-effective protection, based on risk analysis, is a fundamental task in the design and development of the protection of any IT system. In doing so, the impact of the damage caused to the operation of the organisation in the event of partial or complete loss or leakage of data content must be recorded in each of the IT systems, as well as the probability of its occurrence. In determining the latter, we can rely on previous incidents, predictions and possible attack motivations.

Intel's cyberattack motivations document lists the motives for IT incidents in 10 groups [7]. These include damage caused by unprofessional treatment, obtaining business and organisational benefits, religious and ideological causes, dissatisfaction, revenge, personal satisfaction, notoriety and dominance.

[2] https://net.jogtar.hu/jogszabaly?docid=A15H2009.KOR&txtreferer=00000003.TXT

Higher education information systems cover three main areas. Their risk analysis should be examined taking into account data assets, motivations and previous incidents.

3.1. Administration

The systems in the administrative area shall support the functioning of the institution. The most important elements are personnel systems (HR, payroll and related systems) and general economic systems (management, finance, procurement, material management and related systems). They are complemented by a number of other information systems, from tendering systems to the target software of technical units providing technical maintenance of buildings to vehicle use accounting. It also includes management information systems or software to assist with various risk analysis.
The economic systems of higher education have been centralised in recent years, and an SAP-based economic system has been developed on the server park of Eötvös Loránd University (ELTE). Central protection of this is not the responsibility of client universities, but local infrastructure and access regulations are. In contrast to centralized systems, most institutions are distrustful. In that case, the full customizability of the professional system, the definition of its scope of functionality and the foundation of other functions on the existing professional system will disappear. In many cases, centralized systems do not allow direct access to the data stored in them, so application programming interfaces (APIs) cannot be created, often as a result of double administration. On the other hand, the development of centralised software relieves the institution of the development and operation of the infrastructure and distributes responsibility between the external operator and the data host. In current practice, the costs of these schemes are a significant financial burden for universities. A software that is mandatory for all universities is supposed to be a well-designed system, including security planning for its entire life cycle. Unfortunately, this is often not the case for isolated, proprietary software designed to solve a task quickly.

Centralisation does not mean data protection. The stored passwords of the computers providing access, the exported data, statements, and possible data backups from them are easily attacked points that are not affected by a strong central protection.

The main motivation for attacks on the administrative areas of the sector is to obtain direct and indirect benefits. Although other motivations are worth considering on a theoretical level, I did not find any Hungarian public practical examples of these. In the USA, however, the perpetrator of the first attack on a higher education institution was motivated by obtaining social security numbers and credit card information.

In most cases, social engineering or phishing techniques are used to obtain economic benefits, in which targeted attacks and whaling techniques against managers have also appeared. Eszterházy Károly University (EKE) was also involved in a series of scams in which attackers used internal information to force employees of the financial office to change the bank account number of one of the recipients of a large amount of regular monthly payments by an administrator in the accounting system. Payments were made to the fraudsters' account from then on.

In 2020, the salaries of staff at several Swiss universities were stolen and transferred to foreign bank accounts with access data cheated by phishing letters [11].

3.2. Education Systems

The most important element of education systems is the administrative study system[3], on which many additional services are built in most institutions. The study system contains not only the personal data of current students, but also the personal data of former students. Hungarian higher education institutions have recently undergone a number of organisational changes in which university faculty have been reallocated to other universities. When migrating data from study systems, redundant data necessarily appears, thus this redundant personal data is fully accessible in multiple systems. Study systems include not only the personal data of students but also of teachers, which, since HR and payroll systems are present in every institution, this information is therefore redundant.

Although the sensitivity of data in a study system is not comparable to that in a hospital system, special data is also included. The scope of data to be stored is defined in the CCIV of 2011 on National Higher Education Act (Nftv.) and related legal regulations, therefore the health data influencing the student's studies and the method of examination have also been recorded (visual or hearing impairment, dyslexia, etc.).

The loss of study systems would be fatal for a higher education institution. In addition to the current educational tasks, it would be impossible to certify previous studies and diplomas, and in the case of some institutions, to show the number of state-supported semesters.

In order to identify the risks related to the study system, it is also worth considering the data of the Higher Education Information System (FIR), which contains the data of the students of 74 Hungarian higher education institutions graduated since 2006. This is regularly updated on the basis of the data provided by the universities, so we can get an idea of the number of students and lecturers involved. The national data announced in January 2021 in the FIR are summarised in the table below:

Total number of students in Hungarian higher education:	1,832,965
Number of students on 14 January 2021:	608,301
Total number of people working in higher education:	69,602
Number of people currently working in higher education:	51,020

Table 1: Number of personal data stored in the FIR. It was created by the author.

The aggregate data of the FIR include those students who have participated in several higher education courses more than once, so it should be interpreted in terms of the amount of personal data and not the number of students. Therefore, at the time of writing this, the EKE study system contains much more personal data than the statement of the FIR, 108,417 students and 5,649 employees.

Among the professional systems supporting education, it is worth highlighting the library, not only because of the personal data stored there, but also because the dissertations and doctoral dissertations prepared in the institution can be found in the university repositories. They are not necessarily public and members of the public may want to obtain them for the purpose of cybercrime.

[3] As of 2017, the study system of all higher education institutions in Hungary is Neptun developed by the SDA.

The main internal motivations for challenging the study system are hacktivism from students, changes in study results or possibly tuition fees [12]. Among the external motivations, the acquisition of a large number of personal data is most likely, although there is also a Hungarian example of an internal attack.

A staff member managing the study system of a Hungarian university committed fraud of approximately EUR 225,000 by manipulating the data of the study system. In some cases, the offender transferred it to her own account after paying the tuition fees and temporarily cancelled the payment obligation for that semester. The offense lasted for nearly eight years, which could have been prevented by requiring the four-eye principle and checking the processes of the system. Her activity was revealed when the financial system was replaced, and the data was migrated. As logs of IT systems were not available for such a long period of time, the evidentiary process encountered serious difficulties.

In 2009, access to the University of Pannonia's study system was distributed by an attacker to some of the Hungarian press. During the investigation of the incident, it was established that the access codes and passwords came from the university's own system. [2].

In July 2020, a new type of operational incident was found at the University of Utah, whose IT system was infected with a ransomware. Unlike in the past, the data was not only simply encrypted, but also stolen by attackers. The blackmail of the university did not end with the purchase of the key needed for the restoration, as they were threatened with the disclosure of the stolen data if the ransom was refused. The university eventually paid the attackers nearly $457,000 to preserve its reputation. This type of extortion appeared in 2020 and has been used by attackers ever since [8].

3.3. Research Data

The volume and quality of so-called intellectual property vary greatly between universities. Research institutes at universities conduct a wide range of research, in many cases in international cooperation. Some of the research results are less useful scientific results in economic life, which can only be obtained by smaller groups. Others are related to economic or national interest. In Hungary, the results of technical and medical research are typical, but last year's COVID-19 research also plays a key role. The already mentioned Government Resolution 2009/2015. ensures the protection of some research groups and research institutes, which strengthens the security of the research results produced there.

Attacks aimed at obtaining research data are therefore in most cases of economic connection, seek to obtain scientific results and the personal data of researchers which can be sold to economic organizations.

In 2012, an error in the IT system of the University of Pécs caused a loss of patient care and the service of students. The case also deserves attention because there was a partial data loss as well [3].

There have been four successful ransomware attacks at EKE since 2013, but just one of those resulted in a loss of research data. The simplest and most effective technical step to protect against extortion was to restrict the transmission of zip attachments in e-mail.

The three areas are not sharply separated, in many cases they operate as data connection paths as a result of local developments. EduRoam, which also operates in the international relations of higher education institutions and public collections and provides unified WiFi access, usually operates on the basis of the institutional directory and, in the case of students, on the basis of the study system. In order to avoid the administration of guest users, 43 Hungarian institutions have joined the EduID[4] federation, which also identifies its users on the basis of the institutions' internal systems. Due to possible name identities, EduID requires additional registration of logged out users, which forces the retention of additional personal data. However, the registration of personal data is not always centralised, in most cases this is not how it works in library systems.

4. IT Incidents in Higher Education

An IT incident is usually defined as a complete or partial loss of an unplanned service in an IT system, or a deterioration in the quality of the service. Their effects are different, in most cases minimal[5]. Incidents that require intervention are usually not the result of a cyber-attack, but of user or operational failure. Therefore, defense design should focus not only on cyber-attacks but also on operational and administrative protection.

The easiest way to determine the extent of a threat is to establish the number of previous incidents and to analyze trends. Data on this is not available in all countries, and for reasons of defense, it is far from certain that the publications are complete. In the US, only three university data breaches were registered in 2004, but the number of data records stolen was 2 million. By 2017, the number of known incidents in higher education had increased significantly, with 187 cases reported in 43 states. However, due to the lack of a reporting obligation in non-US countries, no data was published until 2011. Since then, however, incidents at universities in at least 45 countries have become known [10].

Details of U.S. attacks are also available. EduCAUSE database contains a brief description of 9,015 U.S. incidents between 2005 and 2019. Educational institutions were affected in 848 cases, most of which were from higher education. The cases are divided into eight categories, with numerical summations shown in the table below [9].

[4] https://eduid.hu/en

[5] The basic condition for the safe operation of an SMTP server is that only authorized users can send mail. In the case of a public server, attempts are made almost every few minutes to find out passwords. This increases the load on mail servers, resulting in slower response times, effectively depleting the definition of incident.

#	Type of breach	Incidents
1.	Fraud Involving Debit and Credit Cards not via Hacking (skimming devices at point-of-service terminals, etc.).	1
2.	Hacked by an Outside Party or Infected by Malware.	290
3.	Insider (employee, contractor or customer).	26
4.	Physical (paper documents that are lost, discarded or stolen).	61
5.	Portable Device (lost, discarded or stolen laptop, PDA, smartphone, memory stick, CDs, hard drive, data tape, etc.).	138
6.	Stationary Computer Loss (lost, inappropriately accessed, discarded or stolen computer or server not designed for mobility).	48
7.	Unintended Disclosure Not Involving Hacking, Intentional Breach or Physical Loss.	239
8.	Unknown.	45

Table 2: IT incidents affecting educational institutions in the US, 2005-2019. Based on [9] it was created by the author.

Attacks from cyberspace are the most difficult to defend against. This and other data leaks for unknown reasons, account for 40% of all cases. Thus, more than half of the cases could presumably have been reduced by administrative measures.

So far, I have not been able to find a complete numerical summary of the IT incidents in educational institutions in Hungary, the main reason for which is the lack of reported notifications despite the obligation. Statistics published by the Ministry of the Interior can provide data for the numerical investigation of attacks against IT systems [6.] It contains data on a total of 407,067 crimes between 2018 and 2020. Only 2% of this, 8,892 cases, were connected to information systems[7], but it is not known how many of these were directed against higher education institutions. Therefore, the analysis of international data rather warns that higher education institutions should also pay special attention to the protection of their IT systems.

5. Current State of Higher Education

In the IT field of higher education, there has not been the same development as in the economic sector. The infrastructure of the institutions are very different, IT devices used are selected on the basis of the existing knowledge and skills of the IT staff. The modernisation of higher value assets is possible only in the framework of grants as the budget cannot cover their costs. As a result, many institutions have outdated IT tools, and long-term end-of-life network equipment and servers are not uncommon and cannot be replaced by institutions. The grant funds can be used only for the development of one sub-area, not for the central elements of outstanding importance for the whole institution. The poor financial situation is further aggravated by the public procurement obligation, which makes it difficult to select and procure the necessary assets on a number of points. The range of products available there is limited, it is not always possible to procure elements that fit into an existing system, which is why it is common for solutions to be found along trade-offs.

The IT organisations of Hungarian higher education institutions are mostly independent islands as there is hardly any organised professional relationship between them and they do not form a formal

[6] https://bsr.bm.hu/Document

[7] Types of offenses: fraud using an information system, breach of an information system or data, and circumvention of a technical measure to ensure the protection of an information system.

organisation. The HBONE Workshop, organized by KIFÜ and its predecessors, is perhaps the only event organized for the IT staff of higher education institutions and provides an opportunity to exchange information and share experiences. As a consequence, there is no forum through which the flow of information can be solved, in which the unification of defense experiences, good practices and IT tools can be shared.

There is no database known about sector incidents that would provide co-institutions with information on individual cases and trends.

Universities carry out their IT security tasks under their own authority, which is usually designed and developed by the head of operations. In day-to-day operations, availability is the most visible task and maintaining confidentiality and integrity requires less operational work. The large amount of data managed, the many different systems, the conversion and conversion constraints required by frequent reorganizations, and software limited to public procurement make it very difficult to manage them securely. Highly skilled professionals are paid much more at economic organizations, so they prefer to work there. Therefore, it is difficult to employ a good specialist in higher education and as a result the IT departments are small, their staff is overburdened and their replacement is problematic. It is not uncommon that one would have no applicants for a job post.

The protection of personal data is the responsibility not only of IT teams but also of data handlers. A significant proportion of incidents are the result of improper data management, lost media, lack of knowledge of rules, or e-mails sent to the wrong location. Data owners do not always understand the internal operation of their own system, the scope of access rights, nor is it common for all outgoing worker's access to be deleted immediately from all systems.

As a result of COVID-19, in spring 2020 higher education institutions had a week to develop a methodology and tools for virtual education and conditions for working from home. In such a short time, only those institutions that had already started this preparation, and during this period had organizational and minimal technical tasks, were able to meet this deadline. During this period, information security and data protection considerations became secondary because the focus was placed by all operators on completing the task on time. During this time, security aspects have temporarily become secondary. Immediate start-up of the home office has caused serious information security problems. Completely unknown, in many cases non-university-owned, and thus uncontrolled home IT devices accessed internal systems behind firewalls via vpn connections or ssh tunnels. Inadequate security settings for clients used by the whole family, illegal software running on them, torrented applications, and infection hotspots created by cracks caused difficult moments for administrators.

Policies relating to IT systems are also prepared on their own authority. Some universities have developed them in the spirit of Act L of 2013, but there are no legal requirements in this regard either. Leaders of the largest universities, on the other hand, know and apply this when designing their own regulations. The person responsible for information security (if any) is often the IT manager, which would be incompatible in the public sector. There are no precise rules for the protection of systems, no official controls are in place, and although the GDPR requires the reporting of incidents involving IT systems to the NAIH, in my view this is only partially the case in practice. Overall, it can be said that the IT systems and processes of Hungarian higher education institutions are not limited by any legal regulations, apart from some general regulations, each institution develops them according to their own ability.

6. Conclusions

Lost data in a system, albeit at a high cost, can usually be replaced. However, damage caused by data leakage cannot be fixed. Some personal and health data cannot be pulled back and will remain public forever. The events of data theft no longer a surprise to anyone as there are a number of such cases almost every day.

However, if we compare the amount and sensitivity of the data processed in Hungarian higher education institutions with the local government of a small settlement, the difference between them is obvious. It is inconsistent that a small municipality is still subject to Act L of 2013, while this is not the case for universities.

Although the freedom of higher education is an important aspect, stricter regulation of the operation of IT systems is inevitable. The already mentioned international tendencies seem to confirm this assumption and it is expected that the Hungarian legal system must follow them as well.

However, change requires significant financial resources. Compliance with the law can only be ensured with the right professionals and the right equipment.

Both the EU and the US cyber defense systems are based on cooperation between member states. Following this example, the establishment of a common IT strategy would greatly improve the operation of the higher education sector, which covers almost a tenth of Hungary's population. This could unify the IT units of the institutions, implement uniform regulations and bring the currently highly heterogeneous systems closer together. The problem of isolation could be solved and standards could be set that could be developed in all institutions.

A clear management structure should be established for this, along with real responsibilities, and the professional support that had been available to Hungarian universities in previous years should be restored. A formal organization should be put in place to ensure a rapid exchange of information and response between operators in the event of incidents involving partner institutions. A Hungarian university CSIRT service could operate on the Dutch model[8].

Professional training, factsheets, forecasts and analyses are essential. Operators need to know actual cybercriminal motivations and hacking tools. The IT systems of the institutions should be designed to support the long-term conduct of forensic investigations and measures should be put in place to prevent attacks.

A system for educating and informing users on a regular basis needs to be set up. Recovery and penetration tests of critical systems should be performed at regular intervals.

These changes would greatly help institution leaders to operate well-regulated, incident-ready IT units at higher levels of protection and service in institutions.

Act L of 2013 and the related implementing regulation provide a framework that puts the operation of IT systems at a higher level of security. It provides help on specific points in a number of ways and clarifies the minimum level of tasks to be performed. International processes are already predicting the need for protection, which has led to an increase in the number of known incidents. A

[8] The Dutch university CSIRT provider, SURFnet-CERT, is available at http://cert.surfnet.nl/.

well-functioning legal background is available, it just waits to be applied. Thus, I consider it necessary that 2013 / L. extend the scope of the law to Hungarian universities and research institutes, regardless of whether they are funded by state, foundation or church.

7. References

[1] Australian Government, Department of Home Affairs. 11.2020. [Online]. Available: https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf. [Downloaded: 01.2021].

[2] DAJKÓ, P., Hacker járta be a Pannon Egyetem informatikai rendszerét. IT Café 2009. [Online]. Available: https://itcafe.hu/hir/pannon_egyetem_veszprem_hacker.html. [Downloaded: 01.2021].

[3] FÜLÖP, Z., Adatvesztés volt, de működik az egyetemi rendszer. Dunántúli Napló 31.01.2012. [Online]. Available: https://www.bama.hu/kozelet/adatvesztes-volt-de-mukodik-az-egyetemi-rendszer-425458/. [Downloaded: 01.2021].

[4] Government of Hungary, 1163/2020 (IV. 21) Government decision Hungary National Security Strategy. 2020. [Online]. Available: http://njt.hu/cgi_bin/njt_doc.cgi?docid=219153.382110. [Downloaded: 01.2021].

[5] Government of Hungary, Act L of 2013 on the electronic information security of public and municipal bodies. 2013. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv. [Downloaded: 01.2021].

[6] Government of Hungary, Government Decision 1139/2013. 2013. [Online]. Available: https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf. [Downloaded: 01.2021].

[7] Intel Corporation, Understanding Cyberthreat Motivations to Improve Defense. 2015. [Online]. Available: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf. [Downloaded: 01.2021].

[8] O'DONNELL, L., University of Utah Pays $457K After Ransomware Attack, Threatpost. 08.2020. [Online]. Available: https://threatpost.com/university-of-utah-pays-457k-after-ransomware-attack/158564/. [Downloaded: 01.2021].

[9] Privacy Right Clearinghouse, Data Breaches. 12.2018. [Online]. Available: https://privacyrights.org/data-breaches. [Downloaded: 01.2021].

[10] SANDHU, K., How is cybersecurity impacting digital transformation within Higher Education. Keyrus Official Blog 12.10.2017. [Online]. Available: http://blog.keyrus.co.uk/how_is_cybersecurity_impacting_digital_transformation_within_higher_education.html. [Downloaded: 01.2021].

[11] Swissinfo.ch, Hackers steal wages from Swiss universities. 04.10.2020. [Online]. Available: https://www.swissinfo.ch/eng/hackers-steal-wages-from-swiss-universities/46075528. [Downloaded: 01.2021].

[12] VmWare Inc., University Challange: Cyber Attacks in Higher Education. VmWare Inc. 2016. [Online]. Available: https://www.nextgensecurityforeducation.com/wp-content/uploads/VMWare-UK-University-Challenge-Cyber-Security.pdf . [Downloaded: 01.2021].