HUMAN RISK FACTORS TO MEASURE THE POTENTIAL OF DIGITAL INFORMATION LEAKAGE

EMBERI KOCKÁZATI TÉNYEZŐK DIGITÁLIS INFORMÁCIÓ SZIVÁRGÁS POTENCIÁLJÁNAK MÉRÉSÉRE

LAUFER Edit[1] – SZÁDECZKY Tamás[2] – VÁCZI Dániel[3]

Abstract

One of the most challenging risk factors of cybersecurity to measure is the human factor. Each individual working for a given organization has a different personality, environmental conditions, and everyone within the organization holds a different position. The various factors are often difficult to quantify, and furthermore, each is highly interdependent from the other. It is necessary to know this risk factor and then build stronger security based on it, as attacks in cyberspace often take advantage of the lack of user knowledge or the mistakes made by developers and operators. To establish a risk factor approaching reality, the authors aim to create a fuzzy system, as this mathematical method is best suited for modeling human logic in addition to handling uncertainties. In this study, the authors present the results of the survey they have conducted, exploring risk factors relevant to digital information leakage.

Keywords

Cybersecurity, Human factor, Risk factor

Absztrakt

A kiberbiztonság egyik legnehezebben számszerűsíthető kockázati faktora az emberi tényező. Ennek oka, hogy egy adott szervezetnél dolgozó egyén más személyiséggel, környezeti körülményekkel rendelkezik és a szervezeten belül is mindenki más pozíciót tölt be. A különböző tényezők sokszor nehezen számszerűsíthetők és ráadásul nagymértékben függenek egymástól. Ennek a kockázati tényezőnek a megismerése, majd ez alapján az erősebb védelem kialakítása szükséges, hiszen a kibertérben lévő támadások sokszor használják ki a felhasználók ismereteinek hiányát, vagy a fejlesztők, üzemeltetők hibáit. A valóságot megközelítő kockázati tényező megállapításához a szerzők célja egy fuzzy rendszer megalkotása, mivel ez a matematikai módszer alkalmas a leginkább a bizonytalanságok kezelése mellett az emberi logika modellezésére. Jelen tanulmányban a szerzők ismertetik annak a kérdőíves kutatásnak az eredményét, amely a digitális információ szivárgás szempontjából releváns kockázati tényezők feltárására irányult.

Kulcsszavak

Kiberbiztonság, Emberi faktor, Kockázati tényezők

[1] laufer.edit@bgk.uni-obuda.hu | ORCID: 0000-0001-8362-4334 | institute director, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Institute of Mechatronics and Vehicle Engineering | intézetigazgató, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mechatronikai és Autótechnikai Intézet

[2] szadeczky.tamas@kvk.uni-obuda.hu | ORCID: 0000-0001-7191-4924 | associate professor, Óbuda University Kandó Kálmán Faculty of Electrical Engineering Institute of Instrumentation and Automation | egyetemi docens, Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar Műszertechnikai és Automatizálási Intézet

[3] vaczi.daniel@uni-obuda.hu | ORCID: 0000-0001-6770-6954 | doctoral student, Óbuda University Doctoral School on Safety and Security Sciences | doktoravrományos, Óbudai Egyetem Biztonságtudományi Doktori Iskola

DIGITAL INFORMATION LEAKAGE AS A CYEBERSECURITY THREAT

Nowadays, people have easy access to various sorts of information. Previously in history, the flow of information has been a much slower process. Today, thanks to IT and network systems, we have many tools to acquire new knowledge. By the 2020s, we have come to the conclusion that digital transformation is not an option but an essential direction of development for companies. Because of the information-based operation processes, not only the companies can maximize their profits, but governmental and academic stakeholders can be more effective as well.

Besides our professional life, our private life becomes more and more information-centric. Our smartphones and wearable devices allow the development of cutting-edge technologies [1]. People intentionally or unconsciously share a lot of information about themselves, including their workplaces without thinking about what consequences their actions might cause. A reckless act can, unfortunately, easily lead to the economic disadvantage of an organization.

Even if professionals build state-of-the-art security solutions, they will never be completely effective against the human factor. That is why the cybersecurity sector needs to pay bigger attention to the people besides technology.

Targeted attacks are usually driven by a specific motive. It can be cybercrime, hacktivism, cyberterrorism, cyber espionage, or cyber warfare [2]. The goal can be gaining information, harming, blackmailing, holding back, making money, and many other reasons. The malicious party usually has enough time to gather the right amount and quality of information about security solutions, various IT solutions, and the workforce as well as at the target. Based on them the action is deliberately directed against an object or person.

If companies are surrounding themselves with dissatisfied, offended, underpaid employees, they can be a perfect next step of a targeted attack. In such cases, the attacker may offer an appropriate amount in exchange for inserting a flash drive into one of the company's computers. After that, the malicious program code executes. This is just an example. Attacks like this can make the attacker's job easier, because they do not need to crack complex systems, they just ask the user to do something. Of course, these have to be well prepared. They have to find the weakest link among the company and make any so-called social engineering (manipulation) attack [3].

Many people think they are too insignificant to be victims of a cyber attack, but in the case of a multinational company or a governmental organization, anyone can. Furthermore, the SME sector is not protected either. For example, if a ransomware virus purchased by a malicious competitor hits a small enterprise, all of its data can be lost without a proper data backup process. At the end of the day, it can easily lead to bankruptcy.

The social engineering attacks can be divided into two main types [4]. The first one, the human-based attacks do not require any technological tools. In these cases, the attackers usually steal someone's identity or use a fictional one to have access to different IT systems or gather classified (or at least sensitive) information.

The other group includes attacks where there is no real cracking of a system, but the attackers use some technology to pull the wool over the victim's eye. These are called IT-based social engineering attacks. For example, sending phishing emails, using keyloggers, or searching with Google Hacking Database or at different social media platforms are belong here [5].

CYBERSECURITY RISK MANAGEMENT WITH THE HELP OF FUZZY LOGIC

There are many risks in an organization's life, such as strategic, environmental, market, financial, operational, cybersecurity, or even compliance risks. In order to run a business properly nowadays, it is necessary to find the right optimum in the functionality, usability, and security of its information system. To optimize it, organizations use different risk assessment methods.

From the perspective of cybersecurity, the goal is to find the balance where preventive and reactive security controls are cost-effective. Firstly, it is necessary to identify potential security events with their mechanism and their effects. Then the impact on the organization should be estimated and quantified based on the recommendations and past experience [6]. This is typically done by the following calculation:

$$Risk = Probability * Loss$$

Based on the management's decision the company either takes the risks or onboard professionals to minimalize them. This decision depends on the risk exposure of the organization. One of the professionally accepted information security risk management methodologies is described in ISO/IEC 27005:2018 [7]. Cybersecurity risk management should be implemented along with a continuously developed business strategy [8]. This strategy should include the human risk as well, despite the fact that this is a risk that is very difficult to measure.

The reason behind the difficulty is the fact that each employee has various cybersecurity risks depending on their personality, personal background, and position in the organization. In addition, these factors are usually subjective and/or cannot be described by exact numbers. In addition, most cybersecurity professionals have a technological background, and human behavioral studies fall out of their focus.

Soft computing methods, and within that, fuzzy logic, is the most suitable to deal with these problems. A fuzzy model with a modular structure is suitable for handling the human factor in the field of cybersecurity [9], because this approach is able to deal with the uncertainty and subjectivity in the system and not just work with sharp boundaries.

HUMAN RISK FACTORS OF DIGITAL INFORMATION LEAKAGE

In order to develop an appropriate risk assessment model, it is necessary to identify risk factors. In order to identify cybersecurity risks, an extensive investigation is needed. It is necessary to know the individual's personality, private and professional environmental conditions.

In many cases, the factors explored in this chapter are only partially visible to the employer. Nevertheless, the authors have strived for a complete exploration, as the flexibility provided by fuzzy logic allows an organization to create its own model based on the information available.

In this article, the authors explicitly investigate the intentional or negligent leakage of digital information. Accordingly, when examining other cyber security threats, it may be necessary to review the composition and interaction of the factors described here.

Identification of risk factors

Digital information leakage can be interpreted as a planned behavior unless it is carelessly committed due to an individual's lack of competence or personality. It means that in order to find the risk factors we should examine how planned behavior works and what are the modifiers which can most likely eventuate by negligence rather than intent.

Ajzen's Theory of Planned Behavior (TPB) [10] guides us to understand how a person acts in a planned situation. It shows how *attitude*, *subjective norms*, *perceived behavioral controls* affect each other and the *intention*. Based on this theory Hunyady and Münnich conducted further research. Their goal was to find additional factors besides the primal ones which also have an impact on a much more specific course of action: corruption. Their model (Solid Moral Index) [11] insert *organizational norm*, *personality traits*, *self-assessment*, *social norm*, *moral perception*, *profit*, *loss valuation*, and *experience* as important factors.

Previous studies [12] [13] show that if we would like to examine a specific behavior prediction (in our case the digital information leakage) the merged enquires are not usable. Therefore, in order to explore as many factors as possible, it is necessary to synthesize the results of existing and relevant researches [14] [15] [16] and conduct further ones.

It is important to emphasize, the authors do not intend to create an extended version of the TPB model or any more specific version of it. The focus is on examining various factors that may be suitable as inputs for a risk assessment fuzzy model.

In addition to examining the models in the previous subsection, it was necessary to explore additional factors to find as many possible inputs of the fuzzy model as possible. For this reason, the authors examined the national security questionnaire [17] and also made in-depth interviews with professionals familiar with various aspects of information leakage.

Demographical data of the questionnaire

Incorporating the processing of the listed sources a questionnaire was created to examine whether the cybersecurity profession can validate the hypothetical risk factors. A total of 174 surveys were completed, which, although not a representative sample, but can be used due to the specific selection of the focus group. The completion consisted of the following stages:

- First version created in Alchemer[4].
- Seventeen professionals working in different cybersecurity areas has been selected to fill the questioner and give feedbacks of it.
- Based on their completion, minimal stylistic and content changes were made. As no substantive changes have been made, their completion can also be considered during the evaluation.
- The questionnaire was published on the mailing lists of various professional organizations (ISACA Budapest Chapter and Hétpecsét Információbiztonsági Egyesület[5]) and in specific social media groups.

Although a total of 341 people started to complete the questionnaire, more than half of the respondents did not finish it. Due to the unrealistically short time of a number of

[4] In the beggining of the research it was named as SurveyGizmo.
[5] In mirror translation: „Seven Seal Information Security Association"

respondents have spent with filling the questionnaire, several ones can be considered invalid during the evaluation. The professional composition of the valid responders (several options could be selected) is described in the following table:

Role	**Number of fillers**
Security auditor	47
Security analyst	14
Security engineer	7
Security system administrator	4
Security strategist	7
Security consultant	36
Security tester/ethical hacker	2
CSO/CISO/CIAO/ISO	21
Deputy CSO/CISO/CIAO/ISO	3
Network administrator	3
Forensics specialist	3
Incident manager (organizational)	4
Information security manager	17
Project manager	17
SOC (monitoring, incident analyst)	2
Technical consultant	10
Operation manager	6
Other security	12
Other	44

1. Table: Rolls of the responders (own comparative analysis, edited based on own research)

The respondents were evaluated in two ways for issues related to the determination of risk factors. First, everyone's response was taken into account, and secondly, only the emphasized security professionals. In this second group the *Project managers*, *Technical consultants*, *Operation managers*, and those who clearly not security profession from *Other* roll was not included. People who answered *None* at the question *How many years of experience do you have in IT/cyber/information security?* were also not included in the second category, despite the fact that their position was relevant.

Timeframe	Number of fillers
None	28
I am an intern	18
3 years or less	20
4 -6 years	31
7-10 years	28
11-15 years	32
16-25 years	15
More than 25 years	2

2. Table: Rolls of the responders (own comparative analysis, edited based on own research)

The responders have experiences in many cybersecurity areas as the following table shows (several options could be selected):

Security area	Number of fillers
Safety awareness of end-users	103
Data protection	105
Application security	54
Auditing	93
Security administration	58
Security architecture and models	37
Planning cybersecurity exercises	37
Security management	74
Security regulations (not data protection)	49
Security planning	42
BYOD	26
Security of cloud-based services	32
Threat modeling	31
Incident response	63
Access management	89
Risk management	83
Forensics	16

Security area	Number of fillers
Mobile device protection	32
Education	72
Personal security risks management	34
Telecommunications and network security	42
Operational safety	57
Business continuity and disaster recovery planning	70
None of them	34

3. Table: Cybersecurity areas of the responders (own comparative analysis, edited based on own research)

Most of the responders work at relevant sectors, such as telecommunication, financial, governmental and IT. Hence the main focus was the human factor, the questionnaire contained also the question *How much do you consider yourself a good judge of character?* From the 5 possibilities a total of eighty percent responded *Average*, *Better than average*, or *Very good* and the rest fifteen percent selected only from the *Not at all* or the *Little* answers. It means that the result is evaluable.

Exploring additional factors using a questionnaire

The first not sociodemographic part of the questioner focused on the risk of the different roles in a company. The assumption is that individuals working in different jobs represent different levels of risk with respect to digital leakage. The goal was not to define all kinds of jobs at a multinational company but to find the most typical ones. Additional uncertainty is further specifications could be used within a role. A member of the cleaning staff who also has access to the server room may pose a higher risk than an accountant with few privileges. Although a more specific result would be closer to reality, the answers show that the assumption is correct, as there is a clear difference between the risks of each job based on the answers' median (*Table 4*). In this sense, it is an important risk factor in the fuzzy model.

Job	Median in a 1-10 scale
Assistant (non-managerial)	4
Security guard at the reception	4
Controller	4
Trainee	4
Hostess	3
HR officer	4
Education	6

Job	Median in a 1-10 scale
Computer scientist	5
IT security officer	4
Lawyer	4
Branch manager	4
Accountant (finance and accounting)	4
Marketing	3
Cleaning / maintenance staff	4
Customer Service Representative	3
Management Assistant	5

4. Table: Median of the job risk (own comparative analysis, edited based on own research)

One of the most important parts of the questionnaire was character analysis. Sixteen character descriptions were given to the responders. In each, specifics were placed indirectly that emerged as a risk factor during literature research, in-depth interviews, and real social engineering audits. In addition to the characteristics of the workplace, there were also elements related to lifestyle, marital status, or even personality traits. Each description looked like the following one (without underscores and numbers):

An agile college student (7;5), who has a partner (6;0), but often flirts with others within the company (45;35). She has a weak financial background (64;42), coming from a poor family (6;4). Due to her age, she is more receptive to technology (11;8). She is an average active user (9;7) who also uses social media a lot (53;41). She does a monotonous job with precision (13;10), which is underestimated (77;53). She could do a lot more work (7;5). She failed to fully integrate with full-time employees (26;14), who treat her as "just a trainee" (24;16). Her moral values have not yet fully been developed (87;69). She smokes (6;5) and goes to parties a lot (11;8).

The responders had to select a minimum of one, maximum of three words or short phrases in each characteristic, which they consider to be risky for leaking sensitive information upon external request, voluntarily or negligently. All the given answers were analyzed. The separate underlined sections in the previous paragraph are considered as an element. The first number in parentheses shows how many of the one hundred and seventy-four respondents marked out of them in total as risky. The second value shows how many of these have relevant cyber security experience. If more than twenty percent of all respondents or professionals indicated the element as risky, it was highlighted as a relevant risk factor (input) in the fuzzy model.

To explore other factors, items in the list below also needed to be evaluated. The consideration was to what extent it increased the risk of a person becoming blackmailed so they could leak sensitive information. The list, sorted by results (starting with less risky) is as follows:

- The relationship status of a given person, in which case s/he is also responsible for her/his partner.
- Having extensive work experience in the given location and position.
- The fact that the given person is an external staff member.
- Inadequate health condition.
- Insufficient life experience.
- Lack of a proper, attentive leader.
- The ability to bear psychological load (stress and frustration tolerance).
- Marginalization from the workplace community.
- Lack of self-knowledge.
- Low level of EQ.
- Social environment voicing negative opinion towards the given person.
- Inattentiveness.
- Low level of IQ.
- The person must support several children.
- The person has already committed minor offenses.
- Large-scale access to sensitive data.
- Hidden deviation from social norms (religious, sexual, political, etc.).
- Poor financial background (perceived or real existential problems).
- Lack of loyalty to the organization.
- Infringement (salary increase, lack of promotion).
- Poor value judgment / value system.
- Addiction.
- Weak morals.

SUMMARY

Reducing cybersecurity risks is essential for an organization in order to preserve proper functioning from a business perspective. The treatment of human factors is crucial, however, it is a challenging process, hence human beings are very complex, and the threats they pose are often subjective and difficult to quantify.

Understanding human risk factors as a specific threat, digital information leakage has been selected and examined with the help of literature research, in-depth interview, and questionnaire research. During the exploration, many risk factors have been found.

Knowing the right factors, a complex model can help to identify the riskiest employees from the perspective of digital data leakage. Each explored element can be an input of a complex fuzzy model that help the managing board and the cybersecurity professionals of an organization to identify employees who pose a potential risk. The model can also help to examine other weaknesses after performing appropriate changes.

LITERATURE

[1] Gottdank T., *Szolgáltatásalapú világ*. Bicske: SZAK Kiadó, 2013.

[2] C. Krasznay, „A polgárok védelme egy kiberkonfliktusban”, *HADMÉRNÖK*, köt. VII, o. 142–151, 2012. [Online] Available: http://hadmernok.hu/2012_4_krasznay.pdf [Accessed 19 08 2021]

[3] D. Váczi, „Célzott támadások módszertana”, in *Célzott kibertámadások*, 2018, o. 52–75. [Online] Available: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7237/C%E9lzott%20ki-bert%E1mad%E1sok%203_jav.pdf;jsessio-nid=073EEE9139D87BF87C010387DBB0E054?sequence=1 [Accessed 19 08 2021]

[4] K. D. Mitnick és W. L. Simon, *A legendás hacker - A megtévesztés művészete*. Budapest: Perfact-Pro Kft., 2003.

[5] H. Cristopher, *Social Engineering - The scinece of Human Hacking*. Indianapolis: John Wiley & Sons, Inc., 2018.

[6] J. Beinschróth, *A kockázatok kezelése, védelmi intézkedések*. 2018.

[7] „ISO/IEC 27005:2018”, *ISO*. [Online] Available: https://www.iso.org/cms/ren-der/live/en/sites/isoorg/contents/data/standard/07/52/75281.html [Accessed 19 08 2021]

[8] L. Kovács, *Kiberbiztonság és -stratégia*. Dialóg Campus Kiadó - Nordex Kft, 2018.

[9] D. Vaczi, E. Toth-Laufer, és T. Szadeczky, „Fuzzy-based Cybersecurity Risk Analysis of the Human Factor from the Perspective of Classified Information Leakage”, in *2020 IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY)*, szept. 2020, [Online] Available: https://ieeexplore.ieee.org/document/9217053 [Accessed 19 08 2021]

[10] I. Ajzen, „The theory of planned behavior”, *Organizational Behavior and Human Decision Processes*, köt. 50, sz. 2, o. 179–211, 0 1991, doi: 10.1016/0749-5978(91)90020-T. [Online] Available: https://www.sciencedirect.com/science/article/abs/pii/074959789190020T [Accessed 19 08 2021]

[11] Hunyady G. és Münnich Á., „A szilárd erkölcsiség elvárása a rendvédelemben: egy lehetséges pszichológiai modell”, *Belügyi Szemle*, köt. 64, sz. 6, Art. sz. 6, jún. 2016, doi: 10.38146/BSZ.2016.6.2. [Online] Available: https://belugyi-szemle.hu/hu/node/1415 [Accessed 19 08 2021]

[12] A. W. Wicker, „Attitudes versus Actions: The Relationship of Verbal and Overt Behavioral Responses to Attitude Objects”, *Journal of Social Issues*, köt. 25, sz. 4, o. 41–78, 1969, [Online] Available: https://spssi.onlinelib-rary.wiley.com/doi/10.1111/j.1540-4560.1969.tb00619.x [Accessed 19 08 2021]

[13] M. Walter, *Personality and Assessment*. Wiley, 1968.

[14] C.-H. S. Lin és C.-F. Chen, „Application of Theory of Planned Behavior on the Study of Workplace Dishonesty”, előadás 2010 International Conference on Economics, Business and Management, Manila, Philippines, 2010. [Online]. Available: http://www.ipedr.com/vol2/14-P00029.pdf [Accessed 19 08 2021]

[15] Hunyadi G., Malét-Szabó E., és Münnich Á., „A rendvédelmi szervek szervezeti normáinak és kultúrájának, mint a szilárd erkölcsiség egyik alapvető háttértényezőjének

empirikus próbavizsgálata", 2016, [Online]. Available: http://www.bm-tt.hu/assets/letolt/kutat/2016/SZEM.kulktura.tanulmany.pdf [Accessed 19 08 2021]

[16] P. Csató, G. Hunyadi, E. Malét-Szabó, és Á. Münnich, *Az erkölcsi értékrend és a személyiség közötti kapcsolat vizsgálati szempontjai*. Budapest: Crew Kft, 2015. Elérés: márc. 07, 2021. [Online]. Available: https://bmprojektek.kormany.hu/download/5/0a/51000/Az%20erk%C3%B6lcsi%20%C3%A9rt%C3%A9krend%20%C3%A9s%20a%20szem%C3%A9lyis%C3%A9g%20k%C3%B6z%C3%B6tti%20kapcsolat.pdf?fbclid=IwAR1HlU1A5XVJ3ufU1toGW1tM3sJPM-tD4z8KN__c5T8BoceAgVP7E4wnlPQ [Accessed 19 08 2021]

[17] „Nemzetbiztonsági ellenőrzés - NBF" [Online] Available: https://www.nbf.hu/hasznos-informaciok/nemzetbiztonsagi-ellenorzes/. [Accessed 19 08 2021]