AARMS Vol. 19, No. 2 (2020) 79–91.

10.32565/aarms.2020.2.6

Leadership Responsibilities in Information Security Awareness Development

Balázs KÁRÁSZ[1] – Csaba KOLLÁR[2]

This paper aims to introduce the main aspects arising in the organisational context related to leadership roles when information security awareness is being engineered and developed according to purposes set within. Achieving these development purposes is connected to the commanding function of leadership, while being influenced by key human risk factors such as: leadership commitment and example setting, leadership quality, the state of being motivated and above all, the ability of responsible decision-making on a professional basis. In order to improve the effectiveness of putting the implementation into practice, a methodological toolset needs to be elaborated for the disposal of the leader, thanks to which, besides taking on a transactional leadership style and a cyclic program management, the continuous monitoring and tailoring to the organisation of the development purposes all become facilitated.

Keywords: *information security, security awareness, manager communication, leadership commitment, leadership skillset*

Introduction and research details

Due to current threats on information society, as well as the growing need of dynamical development in safety culture, it became pronouncedly important for organisations to protect information as an intangible asset of high value, as well as the information systems and information infrastructures affected. Despite applying all sorts of countermeasures that have a technical approach, human risk factors highly influence their effectiveness in practice. Therefore, the psychological side also needs to be assessed, which, in the organisational context, can be intervened by employees in key positions, including leadership and management level, but also non-leadership levels of technical departments.

[1] PhD student, University of Public Service, Faculty of Military Sciences and Officer Training, Doctoral School of Military Engineering, e-mail: karaszb@gmail.com; ORCID: https://orcid.org/0000-0003-2065-4928

[2] PhD, Lecturer, University of Public Service, Faculty of Military Sciences and Officer Training, Doctoral School of Military Engineering, e-mail: kollar.csaba@uni-nke.hu; ORCID: https://orcid.org/0000-0002-0981-2385

Scientific research problem

Based on the above-mentioned issues, the following question arises: how can organisational information security awareness be, and how could leaders effectively manage human risks when reacting to cyber threats at leadership level by applying civil methods of HR and risk management, as well as security awareness development?

Research objective

The objective of this research is to determine the roles of leadership within the concept on how organisational information security awareness can be outlined and defined, through analysing the available literature on the functions of leadership. As a second step, the research aims to emphasise major responsibilities of leaders, which can be effectuated as reactions to the expected effects of human risk factors. The expected results are targeted to further researches in military context.

Research methods

The authors used theoretical and empirical research techniques, partly with the method of synthesis. Related scientific literature from Hungary, as well as abroad, from professionals of both technical and management background are widely mapped and elaborated, in terms of review papers, monographs, conference publications, laws and internet sources.

Literature review

In this section, the authors enlist concepts on the role and functions of leadership in general, besides introducing how the awareness on leadership level influences the information security awareness within organisational processes. The authors found that literature from the past decades can still be considered the fundaments of the theoretic review of the topic. Concerning the professional proposals discussed in the *Conclusion and outlook* section, more up-to-date publications are cited, which support the necessity of forward-pointing in the practical implementation of the theory.

Organisational information security awareness

The conceptual foundation for organisational information security awareness has been established already 20 years ago, in order to emphasise the role of motivation within security awareness education programs.[3] In his widely cited paper, Siponen claims that

[3] Mikko T Siponen, 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security* 8, no 1 (2000), 31–41.

the creation of an information security awareness program requires a systematic approach, dividing awareness into framework and content parts, where the framework should be developed in a systematic and structural manner, with the help of appropriate standards (reference in section *Standardisation of security management*). If end-user internalisation of the security guidelines is the objective, the content part of the awareness program must also come under serious consideration. It is argued that all approaches affecting the behaviour of the user (increasing awareness and so on) should satisfy the requirements of behavioural theories and provide answers for employees acting as end-users in the organisation, letting them observe the reasons for following security guidelines. In this respect, a wide variety of persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions have been established so far. The use of a persuasion strategy is a necessary condition for giving any strategy for increasing awareness a solid basis and for achieving user commitment.

Functions of leadership

Up to current times, data has evolved as the biggest asset of any organisation, since each one of them has to deal with data. A substantial part of data is also personal, belonging therefore to the affected person at the same time. It is crucial to mention the importance of the responsibility of the organisation managing personal data to elaborate the suitable data protection measures and security regulatory system, as well as the sustainable compliance to the related regulations. In favour of full data privacy and information security, it is not enough to introduce internal rules, technological controls, follow-up logs and do back testing, all these measures must be supported by corporate culture itself, enabling the company to continue and apply practices of data management based on awareness.

This aspect originates from an effective setup and continuous improvement of the personnel development system. Such systems assign a declared role to training and career guidance, and when discussing both knowledge management and career planning, functions of leadership play the most significant role.[4] It includes various methods, forms of learning, amongst others lecturing, negotiation, printed material, digital solutions, behaviour challenging methods and techniques of practice and feedback.

A personnel development system, including training of experts and specialists in addition to the training of leaders, can also act as an answer to the recent requirements of the personality of the leader and how they fill their part, such as empathy, encouragement, recognition and inspiration. According to the classic school of Henri Fayol, the functions of leadership can be summarised as follows: planning, organising, commanding, coordinating and controlling.[5] Moreover, organisational communication has got similar functions[6] such

[4] Mártonné Karoliny and József Poór (eds), *Emberi erőforrás menedzsment kézikönyv – Rendszerek és alkalmazások* (Budapest: Wolters Kluwer, 2015), 365–383.

[5] József Roóz and Balázs Heidrich (eds), *Vállalati gazdaságtan és menedzsment alapjai* (Budapest: Budapesti Gazdasági Főiskola, 2013); Henri Fayol, *General and Industrial Management* (Martino Publishing, 2013), 142.

[6] Károly Balaton, Gyula Bakacsi, Miklós Dobák and Antal Máriás, *Vezetés-Szervezés II.* (Budapest: Aula, 1991), 106.

as emotional (social needs), motivational (mediated by communication), informative (in favour of integrity and accuracy) and controlling (based on the organisation structure).

Leadership awareness

When performing the enhancement of the information security awareness, the strengthening of engagement should be brought through first at leadership level and only secondly at employee level. This can also be facilitated conceptually by being embedded into a complex development strategy. According to the basic risk management methodology of investigating precedents and detection of patterns and trends, if translated to operational context, this would mean that targeted courses should focus on case studies and the analysis of artificial cyberattacks and social engineering attacks organised in realistic environment. This is also the fundamental research result of Wilson and Hash[7] in whose paper, concepts of awareness, training and education are defined in order to outline principles to build up a security awareness training program. According to the direction they show, when designing related education material, the most important factor to consider is the utilisation rate of the program and material from the point of view of implementation possibilities and the significant role of follow-up.

In the context of security, knowing the most possible ways of carrying out attacks of either physical or cyber nature can substantially reduce information leakage and unauthorised use, while in parallel, it can increase the stability of State institutions and the safety of actors in society and economy.[8] After a thoroughly structured introduction to security risks found in the thesis of Chestnut,[9] the emphasis is put on the real impact of the mistakes happened or made. According to various methodologies browsed and analysed to discover administrative and management responsibilities with direct impact on human risk factors influencing the information security level, economically grounded proposals are formulated to mitigate risks. These proposals have one common inference to be drawn, which is an emphasised importance of back testing and controlled supervision.

Information security engineering

In this section, the authors collect technical aspects of security management including related standardised concepts, physical/human and information security risks and countermeasures, underlining the role of leadership commitment.

---

7 Mark Wilson and Joan Hash, *Building an Information Technology Security Awareness and Training Program* (Washington, D.C.: National Institute of Standards and Technology, U.S. Government Printing Office, 2003).

8 Veronika Deák, 'Biztonságtudatosság az információs környezetben', *Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle* 15, no 3 (2017), 59–76.

9 Jacqueline Annette Chestnut, *Assessing the Impact of Human Error in Information Security Incidents* (Mississippi, MI: Bell & Howell Information and Learning Company, 2000).

Standardisation of security management

In favour of establishing a general framework for ways of information security engineering, a possible solution is to implement an information security management system (further referred to as ISMS) within the organisation based on a certified standard. ISO 27000 is a collection of internationally acknowledged and applied standards, which introduces basic directions, according to which, operating an ISMS ensures the manageable safety and security.

Information security (not to be mistaken for IT security – being a subcategory of information security in the context used by this paper) must be interpreted only in the way of the effectuation of *confidentiality, integrity, and availability* (further referred to as C.I.A. triad) together and under all circumstances according to the following reasoning:

1. Confidentiality: no one without authorisation can access any part of data or information (often regulated by extensive access management), contrary to *availability*.
2. Integrity: the data or information is genuinely authentic and undeniable, while also no changes are performed on its original state (also proven by *confidentiality*).
3. Availability: in case of properly functioning information security, the (*intact*) data and information can be accessed by those disposing of authorisation at any time.

According to recent summary data, Hungary is no 17 out of 170 countries in having obtained the most ISO IEC 27 001 certifications in number as of 31 December 2018.[10]

The PDCA model is used wide-spread and applied in ISO standard-families, including the group ISO 27000 dedicated to information security. Furthermore, the model can be used in the development of information security awareness of leaders and even executives, although not in its original form. It serves, however, as a suitable fundament to be completed by further elements – especially envisaging purposes – and this way becoming an effective consultancy and coaching method at the disposal of business coaches working on executive areas.[11]

Security risk management

ISMSs need to be established in the organisation including a comprehensive mapping, identification, assessment, analysis, management, monitoring and review of risks, in harmony with the PDCA cycle used widely in all management system related standards. Physical security issues and risks deriving from information technology background should not be handled separately. Some examples are collected here to show the importance of the risk integrity when discussing about cyber protection at workplace:

- Welcoming external persons: guests are often left alone or without surveillance in office areas or are entering meeting rooms when confidential documents from previous meetings are not yet put away. Also combined with either the interruption of the

[10] Certification & Conformity, 'The ISO Survey 2018'.

[11] Csaba Kollár, 'Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében coaching és tanácsadás módszerével', *Magyar Coachszemle* 5, no 3 (2016).

entrance security system, losing the access card or lending them to guests (that is, unauthorised access is made possible to even protected areas).
- Leak of information: informal discussions in the canteen, in the elevator or not adapting adequately to the clean desk and clean display policy can lead to unauthorised persons overhearing confidential information. Suspicious calls via telephone can also be categorised here in some cases.
- Unauthorised access: originating from either social engineering (psychological manipulation) or inherent and unintentionally present human risk factors such as inadvertence, authentication data is leaked and used by unauthorised persons to access the information system for personal use.
- Protection against malicious software: both sources (for example emails, websites, downloaded programs) and file names can be suspicious, but without regularly updating antivirus programs or by attaching data media of unknown origin unawareness can mean a serious threat to confidential information.
- Data breach: when considering the worst scenarios, the stored data can be destroyed, seriously damaged, or locked down by blackmail viruses. Without a successful external attack, data breach can be suffered by the company if an information device is lost, upon which corporate data can be accessed.

Seeing the above-mentioned examples, it can be clearly understood that the common origin of these can be found in the human behaviour,[12] out of which, sanctioning can only cover intentional or unintentional but eliminable actions or happenings according to the following overview of several exemplary cases:
- Loss or damage caused to physical device (such as mobile phone): beyond the book value of the device, damages should be estimated according to the C.I.A. triad of the stored or accessed dataset – especially when information is compromised.
- Default in reporting an incident: either technically, connected to the systems, devices used to access corporate information (for instance noticed failure message or unusual operation method), or connected to physical and human security – damages caused by the late or defaulted report should be estimated.
- Not intended (that is, not work-related) use of information infrastructure: unsubstantiated personal use (music, movie, game download), use of illegal software, changing centrally controlled settings can all be continuously monitored by log, email check and so on. Damages are to be assessed according to the Criminal Code, too.
- Ignoration of information security regulation measures: damages should be assessed by taking into consideration material, reputation, operation expenses, as well as legal consequences, client dissatisfaction and business continuity issues.

Furthermore, the enforcement of various sanctions also plays a significant role in key leadership responsibilities managing information security issues, which is placed into organisational context in section *Using specific leadership skills*.

[12] Balázs Kárász, 'Az információbiztonság felhasználói oldali humán kockázati tényezőinek hálózata', *Biztonságtudományi Szemle* 2, no 2 (2020).

Leadership commitment

In harmony with Clause 5 of ISO 27001 standard (and appearing in the High-Level Structure of ISO standards): 'Top management and line managers with relevant roles in the organization must demonstrate genuine effort to engage people in the support of the ISMS.' (ISO, 2013) Concerning all security management professional areas, the crucial question is – beyond its transparency – how leadership commitment can be demonstrated. Security therefore should be engineered at top-level within an organisation, just as we see that sanctioning and regulation measures can also be implemented by management.[13] A possible step forward is the subordination of the responsible department(s) unto the managing director/chief executive officer, as it can be seen at organisational structures of, for example, several large enterprises operating critical infrastructures.

When discussing about lower employee levels, awareness here originates and is principally based on the awareness level of the management. Development programs such as training, personal coaching and consulting that aim the improvement of security awareness should therefore include all hierarchic levels.[14] Commitment can be grounded by turning the focus of top management development to risks expressed in quantified ways as well as client relationships (in terms of the commitment towards handling personal data of customers), while the shareholder value should also be emphasised. If the leader makes decisions observing accurately collected and processed information, besides being highly committed to security measures, even responsibility related to the moment of decision can be decreased significantly.

Leadership responsibilities in information security

Key leadership skills in shaping security management include both technical (including business and professional) competences and interpersonal skills (mostly communication-related). In this section, the authors also put emphasis on competences influencing the enhancement of organisational security awareness, which are related principally to leaders.

Using technical and business skills

Visibility is the first attribute that must be ensured in an organisation in the sense that if an attack surface or its part is not visible, no measures will be able to maintain security. Therefore, all assets and all attack vectors must be mapped and accurately understood in order to mitigate breach risk. Also, the exact timing of a cyberattack is hardly known, which is the reason for applying methods, suitable tools, processes and models predicting risks according to breach scenarios. This will create a modern risk approach to cybersecurity, which has three main characteristics in being *predictive, proactive, and preventive.* Not

[13] Balázs Kárász and Imre Négyesi, 'Information Security Responsibilities of Critical Infrastructures in the Aspect of Human Risk Factors', *Hadtudományi Szemle* 13, no 3 (2020).

[14] Kárász, 'Az információbiztonság'.

to forget the third aspect, that is, recognising all kinds of threats (including password issues, misconfigurations, phishing, ransomware, encryption issues, and so on) against which protection should be established. Proven that visibility, prediction and full-scope recognition of threats are in function, appropriate response can be carried out overall.

Regarding a full functioning alert system, prioritisation of vulnerabilities becomes a must, based on the extent of business criticalness of all elements affected, such as assets, threats, controls and exposure, in order to be able to focus on tasks of high priority. When facing problems, it is response time that will influence the impact of the threat; therefore, among possible ways of finding the solution, natural language search across the personal network is at hand.

All in all, strong cyber hygiene should be built and practiced by the leader of technical responsibility. For example, multifactor authentication is an efficient way to reinforce security posture, which mitigates cyberattacks connected to compromised user credentials.[15] Investing in technologies that enable strong password creation is highly recommended, since systems can be easily defended against brute force attack techniques with the help of them. Also, the elaboration of a continuously controlled and efficiently functioning access management is inevitable. When determining the regulations for each user within the organisation, the 'principle of least-privileged access' should prevail, for instance a project engineer does not need access to an organisation's financial data and a finance manager does not need to access the organisation's production code repository. Building a strong identity and access management system begins with having a single trustworthy reference of all users and their roles within an organisation.[16] These are considered the fundaments of human security management.

Using interpersonal and communication skills

Leadership can be defined as the process to influence (that is, motivate) others to follow rules and procedures (including compliance to standards) to achieve objectives, whereas leadership style refers to the characteristics of the leader to monitor and control their followers.[17] Here it can be seen that interpersonal skills are key to efficient communication and reaching well-defined objectives within the organisations.

Taking a closer look on cyber risks, in order to manage them, not exclusively the leaders of security-related departments but all leaders in the organisation must also leverage colleagues. The best way to encourage employees to participate in security programs is to use gamification and make them win incentives, rewards and awards for completing security related tasks. Gamification is a process where game mechanisms are integrated into platforms and programs, which traditionally would not consist of such elements,[18] or it can be defined from the perspective of motivation, where gamification utilises game elements in order to encourage users and communities by commitment to do activities that they are not necessarily willing to take up under different circumstances. From our point

[15] Kárász and Négyesi, 'Information Security Responsibilities'.
[16] World Economic Forum, *The Cybersecurity Guide for Leaders in Today's Digital World* (Geneva, 2019), 22.
[17] James MacGregor Burns, *Leadership* (New York: Harper and Row, 1978), 530.
[18] Christopher Swan, 'Gamification: A New Way to Shape Behavior', *Communication World* 29, no 3 (2012).

of view, gamification therefore is a useful tool to build commitment to security measures at all levels of the organisation.

The other aspect to be mentioned among communication skills is reporting to the board as a security/IT professional leader. Here lies a crucial point to break through when communicating business-level risks in a quantified way, in terms of metrics, indicators and everything translated to cash. When convincing them of a necessary cyber protection investment, leaders must quantify the security posture of the organisation to the board or top management to get their buy-in for the initiatives and focus on the trade-off. Leaders should possess and develop for themselves a strong business acumen to translate the technical risks into business strategy risks, so that a non-technical audience can understand the potential threats to business operations.

Using specific leadership skills

When discussing skills that belong exclusively to leaders either by personality or by responsibility, the problems should be divided into two aspects, just as we did above, the first being the category of leaders being responsible for a security department. In this case, as we already agreed, the leader should avoid technical approach and language and start thinking like a business leader by ensuring transparent communication and building trust in the organisation. With the help of the leader paying attention and making efforts to develop critical thinking, creativity and problem-solving skills within the organisation, not only the cybersecurity team but the entire personnel can benefit from it thanks to their mindset being challenged and finally changed. Beyond all technical (hard) and interpersonal (soft) qualities – even with the lack of them which can be easily completed by learning – every leader in the organisation has to make efforts in aligning to and complying with security regulations. One side of this coin is already mentioned as the concept of leadership commitment. It is an attribute which can be visible and easily demonstrated, for example, in legal and regulatory context.

The other side of possessing an affinity in example setting as a leader cannot be put away, since as a non-technical leader, it supports the authenticity of commitment, while as a technical leader, a culture of cybersecurity can be created on this basis. Either perceived in the aspect of interpersonal relations, that is, drawing the attention of employees to the importance of complying with security regulations, or manifested connected to technical knowledge, for instance knowing the most modern way of protecting information infrastructure, authentication credentials and so on, the leader has to achieve the goal that the employees will follow these habits by their own understanding. Especially when discussing about the access to domains handling sensitive data, leaders are exposed from the point of view of their example setting, in order to make themselves able to align with security guidelines. Moreover, the leader exclusively disposes of the power to enforce the compliance with regulations of the employees with sanctions. Not to be forgot, we have to mention the special characteristic of example setting, being especially important in security areas, where, on the contrary, it is not the exclusive responsibility of the leader, but equally of all colleagues throughout the department.

To have a more global outlook on the above-mentioned questions, fostering both internal and external partnership (from the view of the organisation) is an important recommendation, since threats and information security innovations share a dynamic nature, and therefore a better global systematic architecture should be built on cyber protection.[19] The network behind all similar kinds of potential initiatives is based on the cooperation and acquaintances that leaders can support. This way, more effective platforms can be created to facilitate information and knowledge sharing within and across industrial segments.

Transactional and transformational leadership

According to the study of Humaidi and Balakrishnan,[20] which focuses on the following two styles of leadership described partly by Burns[21] and Bass:[22] transformational and transactional leadership, we can suppose that these two well-described styles differ fundamentally and can therefore have significant impact on shaping both information security engineering culture and awareness within an organisation. Leaders who are engaged with their team members and motivate them are said to have the characteristics of a transformational leader, while on the other hand, a transactional leader is somebody who as a leader operates within the existing system or culture and strictly controls how policies are implemented in the organisation.

Many leadership studies already have pointed out that both of the leadership styles influence work performance overall significantly. The three constructs of awareness that serve as a second dimension of the study are threat severity (as an externally determined factor), susceptibility (which can be considered an interior human risk factor) and security-countermeasure awareness (a retaining factor affecting human behaviour). Although the above and following statements are focused on security/IT professional or department leaders, we must take into consideration – as stated before – that all measures to the benefit of operating an effective information security should be expanded to circles beyond security and IT leaders and include every leader of the organisation, plus, through them, all employees.

Synthesising the two key skills of section *Using specific leadership skills*, example setting and commitment, with the above described leadership styles, this paper intends to add that example setting on leadership level makes up an inseparable part of transactional leadership, while commitment, regarding its basic characteristics, is an attribute mainly of the transformational leadership style. This becomes even more meaningful if we take into consideration the quantitative research results published in the cited paper,[23] which show that transactional leadership has significant direct and indirect impact on the user's policy compliance behaviour through threat severity awareness and in parallel, security-

---

19 World Economic Forum, *The Cybersecurity Guide*, 22.

20 Norshima Humaidi and Vimala Balakrishnan, 'Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness', *International Journal of Information and Education Technology* 5, no 4 (2015), 311–318.

21 Burns, *Leadership*.

22 Bernard M Bass, *Leadership and Performance beyond Expectation* (New York: The Free Press, 1985), 256.

23 Humaidi and Balakrishnan, 'Leadership Styles and Information Security'.

countermeasure awareness, while transformational leadership turned out to have no indirect effect on the user's behaviour.

The reason behind the transactional leadership being more resultful compared to transformational leadership, especially when related to information security compliance behaviour, may be found in higher transparency in terms of clearly showing rewards and punishments. When transactional leadership is exercised strongly by applying rewards depending on following regulations properly and punishment of not complying employees, situations can come across, with the help of which, higher awareness level is formed, and therefore, information security compliance behaviour may also be ameliorated.

Conclusion and outlook

We attempt to find the shared section of all above-mentioned aspects of leadership functions and styles, security awareness, commitment and example setting, key skills – in order to locate leadership example setting within the concept of organisational information security awareness.

Organising security awareness programs alone does not result in realising security awareness itself, since it is inevitable to entirely process the information needed for design, achieve full leadership commitment and example setting, as well as undertaking corrections after the realisation of the program according to the related feedbacks, in order to implement an effective and successful personnel development system. The development of information security awareness of leaders and executives is one of the most crucially important fields of consultancy and coaching services of the beginning of the 21st century, especially taking into consideration that the leadership attitude towards security is not an autotelic responsibility, but has a significant impact on the financial situation and safety of the organisation. The improvement of the company nowadays cannot be separated from the information security awareness of the employees, including executives as well, which also has to involve the recognition and successful defence against social engineering attacks.[24]

Example setting cannot be interpreted as a leadership attribute or skill standing alone, since it can be accomplished in the field of responsibly taking main leadership tasks and communication. In leadership positions within any organisation, the following qualities have to be in balance to effectuate example setting: goal setting, decision-making, change management, delegation, assessment, control, feedback, problem management in terms of correction application, conflict handling, negotiation techniques, hierarchy acumen and creativity.[25] Out of all these aspects, control is necessary to be considered the only function that cannot be delegated, since it originates from the responsibility and position of the leader. In the context of the network of human risk factors in information security, specific leadership skills play a substantial role in shaping relations, that is, reactions of employees to human and IT-based social engineering attacks.[26] Most likely of all, example setting represents the outlined role of the control function of leadership in the effectuation of high

[24] Kollár, 'Az információbiztonság-tudatosság fejlesztése'.
[25] Daniel Eppling and Laurent Magnien, *Leadership in Action – What Great Managers Really Do*, 222.
[26] Kárász, 'Az információbiztonság'.

level information security awareness, since its 'target audience' cannot be limited to direct subordinates, but extended to indirect subordinates, colleagues on same or lower hierarchic level, as well as a higher level leader, thus potentially, the entire organisation.

In order to make it possible to realise an effective control function in leadership, independence of security departments needs to be assured, since when operating as a local department, it did not dispose of enough power to enforce the necessary guidelines or steps.[27] This is the reason for our proposal towards organisations that security departments should be centralised – even as a service provider within large organisations – and assigned under direct control of top management. This organisational structure can effectively function based on leadership commitment at top levels, which will escalate then to all hierarchic levels in the organisation.

Summary

This research collected the most recent international literature concepts as well as standards concerning the role and responsibilities of leadership in the field of information security awareness development. Beyond the technical capabilities, personality and a wide scope of skills of the leader have a significant impact on shaping human behaviour, that is, the awareness throughout the entire organisation. The research also successfully defined the concept of organisational security awareness, and all results build up a useful basis for continuing research in the topic of measuring effectiveness of development steps and processes, also suggested to be considered in military engineering context. The results will be used to widen the network of human risk factors in information security by the aspect of specific leadership skills and responsibilities.

References

Balaton, Károly, Gyula Bakacsi, Miklós Dobák and Antal Máriás (eds), *Vezetés-Szervezés II*. Budapest: Aula, 1991.

Bass, Bernard M, *Leadership and Performance beyond Expectation*. New York: The Free Press, 1985.

Burns, James MacGregor, *Leadership*. New York: Harper and Row, 1978.

Certification & Conformity, 'The ISO Survey 2018'. Online: www.iso.org/the-iso-survey.html

Chestnut, Jacqueline Annette, *Assessing the Impact of Human Error in Information Security Incidents*. Mississippi, MI: Bell & Howell Information and Learning Company, 2000.

Deák, Veronika, 'Biztonságtudatosság az információs környezetben'. *Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle* 15, no 3 (2017), 59–76.

Eppling, Daniel and Laurent Magnien, *Leadership in Action – What Great Managers Really Do*.

Fayol, Henri, *General and Industrial Management*. Martino Publishing, 2013.

[27] Viktor Spilák and Zsolt Tibor Kosztyán, 'Szervezeti kultúra, vezetői szerepek, az információbiztonság és a felhőalapú megoldások kapcsolata', *Vezetéstudomány* 50, no 7–8 (2019), 70–87.

Humaidi, Norshima and Vimala Balakrishnan, 'Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness'. *International Journal of Information and Education Technology* 5, no 4 (2015), 311–318. DOI: https://doi.org/10.7763/IJIET.2015.V5.522

Kárász, Balázs, 'Az információbiztonság felhasználói oldali humán kockázati tényezőinek hálózata'. *Biztonságtudományi Szemle* 2, no 2 (2020), 57–68.

Kárász, Balázs and Imre Négyesi, 'Information Security Responsibilities of Critical (Information) Infrastructures in the Aspect of Human Risk Factors'. *Hadtudományi Szemle* 13, no 3 (2020). DOI: https://doi.org/10.32563/hsz.2020.3.6

Karoliny Mártonné and József Poór (eds.), *Emberi erőforrás menedzsment kézikönyv – Rendszerek és alkalmazások*. Budapest: Wolters Kluwer, 2015, 365–383.

Kollár, Csaba, 'Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében coaching és tanácsadás módszerével'. *Magyar Coachszemle* 5, no 3 (2016).

Roóz, József and Balázs Heidrich (eds), *Vállalati gazdaságtan és menedzsment alapjai*. Budapest: Budapesti Gazdasági Főiskola, 2013.

Siponen, Mikko T, 'A conceptual foundation for organizational information security awareness'. *Information Management & Computer Security* 8, no 1 (2000), 31–41. DOI: https://doi.org/10.1108/09685220010371394

Spilák, Viktor and Zsolt Tibor Kosztyán, 'Szervezeti kultúra, vezetői szerepek, az információbiztonság és a felhőalapú megoldások kapcsolata'. *Vezetéstudomány* 50, no 7–8 (2019), 70–87. DOI: https://doi.org/10.14267/VEZTUD.2019.07.07

Swan, Christopher, 'Gamification: A New Way to Shape Behavior'. *Communication World* 29, no 3 (2012).

Wilson, Mark and Joan Hash, *Building an Information Technology Security Awareness and Training Program*. Washington, D.C.: National Institute of Standards and Technology, U.S. Government Printing Office, 2003. DOI: https://doi.org/10.6028/NIST.SP.800-50

World Economic Forum, *The Cybersecurity Guide for Leaders in Today's Digital World*. Geneva, 2019. Online: www3.weforum.org/docs/WEF_Cybersecurity_Guide_for_Leaders.pdf