DOI: 10.2507/34th.daaam.proceedings.xxx

# BENEFITS OF KNOWLEDGE MANAGEMENT IN CYBERSECURITY – INITIAL STUDY

Jan Albrecht, Petra Dostálová, Lukáš Králík & Gabriela Králíčková

**This Publication has to be referred as:** Albrecht, J[an]; Dostálová, P[etra]; Králík L[ukáš] & Králíčková, G[abriela] (2023). Benefits of Knowledge Management in Cybersecurity – Initial Study, Proceedings of the 34th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/34th.daaam.proceedings.xxx

**Abstract**

The work focuses on the aspects of knowledge management that could be beneficial in dealing with cybersecurity issues, specifically targeting common users with a basic knowledge in that area. To understand the connection, the paper briefly introduces knowledge management itself, capturing the essential information. The work explains how technological innovation changes the value of intangible assets that are closely related to cybersecurity, followed by the description of threats in the cybersecurity field, characterizing its categories, and giving current examples. The importance and potential benefits of knowledge management are often overlooked, making it much harder for many organizations to deal with various types of threats. The work presents how valuable knowledge management can be and how to use it to deal with the problem of avoiding and mitigating cybersecurity threats with their consequences, depicting the cycle of knowledge management, and describing its individual parts.

**Keywords:** Knowledge management; Cybersecurity; Technological innovation; ISMS; Continuous improvement.

## 1. Introduction

During the last decade, the world has been witnessing a major increase in technological innovation, which is exponentially rising. The improvement and exploration of new possibilities is not a problem on its own, on the contrary, there are plenty of useful outcomes that can help in many ways and be an enormous help in a lot of areas (healthcare, cybersecurity, predictions, etc.). New possibilities, often intentionally meant to be used mainly for beneficial outcomes, have a great potential of being misused by attackers. The rise of technological innovation has been there for some ages now and it is a natural way of evolution [1], [2], [3]. By acknowledging that fact, organizations and people should not only think about the possible benefits with positive outcomes, but also about the possibilities of misuses and what threat can they pose [3].

As Talet (2017) mentions, knowledge management (KM) alongside the potential risks requires to be taken very seriously in the matter of obtaining the actual and relevant information of possible threats [4]. By doing so, organizations can be prepared to respond to new threats, reducing the risk of them causing some crucial harm. One of the vulnerable parts of an organization and its cybersecurity measures is usually the human factor. When people within are not educated enough about the possible threats and consequences, they are not able to properly deal with the issues, even if the problem is only at the start and could be manageable with the right knowledge [5], [6].

In some areas it could be hard to use KM, however, cybersecurity on the level of the common user is one of the examples where the power of knowledge and its sharing can be a crucial factor for a fast and appropriate response to threats [4], [6]. The paper aims to introduce the benefits of using KM in cybersecurity on the level of the common user and suggests how should be the KM implemented into the organization's processes to be most effective.

## 2. The role of Knowledge management

In the previous ages, visible assets were the most important ones to be taken care of, today we live in an era, where non-material assets are becoming more and more valuable, hence their need for protection is also on the rise. Personal experience, relationships, talents, skills, subconscious, and many more were there even before, but their importance was overshadowed by the necessity to protect tangible assets such as material, human resources, premises, etc [4], [5]. Nowadays, when technology rises and with it, the amount of information, data, and knowledge, makes their value for dealing with threats (among other fields) greater than before. However, their value does not come only from their acknowledgment, but mainly from the way of their efficient gathering, storage, and sharing [5], [7], [8].

The Knowledge Management standard is ISO 30401:2018 and includes requirements, sets of best practices, processes, and many other topics related to KM [9]. As it functions as a great guidance tool for the implementation of KM principles, some organizations prefer to use frameworks such as the Information Technology Infrastructure Library (ITIL), Control Objectives for Information and Related Technologies (COBIT), AGILE, and many others. These tools mentioned are not primarily KM tools, but they do include the knowledge principles in their structure, making them suitable for that application, whilst the KM implementation on its own can be perceived as redundant for them [9], [10].

Knowledge management is working with more types of knowledge and the correct application should include the combination of them all. The main difference between them is in their expression, the possibility of their documentation, and the way people use and remember them. Their more thorough description follows [4], [5], [11], [12]:

- **Tacit knowledge –** This type can include the general knowledge of an individual, that one is usually not able to fully describe and document it. It can be sometimes characterized as personal knowledge, that people use naturally based on their subconscious, judgment, intuition, experiences, and understanding. The goal of KM is to try to add important information to the people's common knowledge and reactions.
- **Implicit knowledge –** Sometimes known as a subpart of tacit knowledge is the implicit one. They are better for description but are still considered as more personal data, gained by time and experience. Sharing and explaining are usually done by seeing the action in the process so others can see it, remember it, and apply it by themselves.
- **Explicit knowledge –** This type of knowledge is pretty normal for their easy description because they consist of known facts, standards, manuals, and clear explanations which should be understood the same by everyone. Their ease of expression makes them used for tangible documentation, manuals, and instructions.

## 3. Cybersecurity threats

The era of technological innovation and with it the related rise of cyber technologies used by a vast area of people brings certain advantages as well as threats and risks. With the contrast of many other kinds of securities and their threats, this type usually targets intangible assets, which can make it way more difficult to not only make the needed preparation for it but also to deal with them once they occur [13], [14], [15]. This area can divide the threats into two categories, intentional and unintentional, where both pose different risks and they are more thoroughly discussed in the sections below [13]. The major goal of that part is not to list all the potential threats, but to present the various types of threats associated with cybersecurity and to point out the necessity of its acknowledgment.

### *3.1 Intentional threats*

These are usually the outcomes of an attack executed by an attacker with the intention of causing harm of any kind. The harm in this area does not usually mean endangering the health of someone (but even these types can happen, e.g. targeting some functions of an automated vehicle, making it a potential tool to cause damage not only to the people inside, but also to others), but more often can be seen in the form of attacks that are intended to steal, modify, or delete some information, whether for the advantageous use (so the attackers can have some kind of leverage against them), or for destructive purpose. A few selected examples of these attacks are listed below [2], [3], [13], [14], [15]:

- Malicious actors;
- Social Engineering (Phishing, Vishing, Pharming, etc.);
- Ransomware;
- (Distributed) Denial of Service attacks;
- Cyber Espionage;
- Insider threats [16], [17];
- Zero-day attacks.

*3.2 Unintentional threats*

Technology innovation is much faster than before and that also raises the number of possibilities not only for attackers to execute their intended attack, but also for some issues from outside or within the system. These threats are hard to prepare for and they can be usually caused by [2], [6], [13], [15]:

- Human error;
- Risky behaviours due to a lack of knowledge about security;
- Software vulnerabilities, flaws (making opportunity for attacks, e. g. zero-day attacks);
- Wrong configurations of systems;
- Misuse of tools, software, hardware, etc.
- Failure to keep the software or hardware up-to-date;
- Threats caused by weaknesses and failures of third-party subjects.

Another category could describe threats caused by Natural threats such as floods, thunderstorms, earthquakes, etc. [14], but since they are the same for many security fields, their description in this paper would be only a piece of redundant information.

## 4. The benefits of the use of Knowledge Management in Cybersecurity

Information and knowledge are the most important tools in dealing with the security of intangible assets, which is one of the most targeted areas in cybersecurity. However, there can be a common misunderstanding between just having the information and being able to use it well [4], [5]. An organization can have plenty of data about cybersecurity and many other related areas, but with the lack of knowledge, right distribution, presentation, and application, the whole process of their collection could be wasted.

No matter the technological innovation phase, people are the most significant units in an organization to be well educated about all possibilities of the potential threats and risks included [4]. Cybersecurity deals with a lot of information and uses different types of SW and HW, but there is always someone who operates with, works with them, or just has access to them, making them a vulnerability, a weak point of the system itself. The common saying states that the system is only as strong as its weakest unit, then organizations have to always concentrate on the education and experience of their employees.

*4.1 The cycle of knowledge management*

As are the types of knowledge mentioned above, the process of their implementation is also an important aspect. The whole cycle described in this part is similar to the widely used Plan-Do-Check-Act matrix (known as PDCA or Deming matrix), which is used for continuous improvement (mainly in business process management) [13]. By understanding the continuous cycle and its benefits, the individual parts of KM were then incorporated into a continuous process which consists of 4 parts. The cycle captures what steps should be performed to set (and maintain) adequate knowledge of people about potential threats and how to respond to them. The individual parts are briefly described below [4], [5]:

- **Threat awareness –** The initial step should be to acknowledge all potential threats that can pose a risk to the subject, collect all the possible and relevant information, and create a well-constructed, and understandable document, that introduces all that is necessary to the involved group of individuals. Thorough threat awareness is a crucial part of all other steps.
- **Incident response –** Once good knowledge about the potential threats is established, everyone related to the area of interest should be able to know how to respond based on the threat they deal with. This mostly includes the documentation of the policies, best practices, and procedures, that should be done to achieve the best possible outcome of the occurred situations.
- **Knowledge sharing –** The communication between individuals in an organization is crucial for creating tacit/implicit knowledge. Even when the information about threats and responses should be already presented in the general threat awareness, sharing information between others can help to maintain that knowledge and understand it not only as something necessary to know but also as a custom that should be kept to establish better conditions at work.
- **Training/Education –** From the first step, there should be created documentation about the potential threats, and the suitable responses to them are well described for all interested individuals. However, periodical training and education should be involved to ensure that they know all the important information for sure, and mainly, that they understand them correctly.

To ensure that all the knowledge about the threats and the responses to them are all the time kept up to date, and by doing so is maintained the level of cybersecurity to the intended level, the whole process should be continuously updated and improved [4], [13]. That step should always check if there are any possible changes to improve the knowledge about the potential threats, and if so, it should be incorporated into the whole process. The whole cycle of knowledge management is pictured in Figure 1.

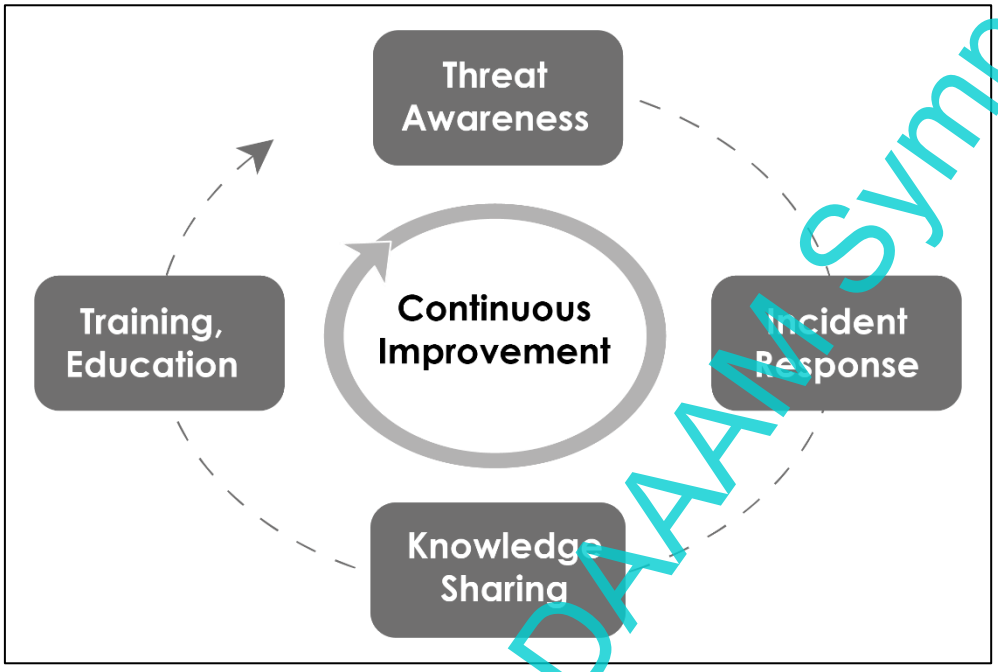


Fig. 1. Knowledge management cycle in the area of cybersecurity.

With the suggestions and steps described, organizations can improve their management of knowledge, and with it their overall cybersecurity measures and preparations. Since each organization has individual needs and capabilities, the way of implementation can vary. The first step should always be a thorough analysis of their current knowledge management, highlighting the main points that need to be changed. That part is highly recommended to consult with an expert from the field (internal/external) and with all the related and responsible people of the organization. If everything proceeds successfully, the expected outcome should make the organization better prepared to deal with many potential threats and change the behaviour of individuals within the organization, making them more responsible, since they are now well-informed about the potential consequences and how to prevent them. However, the preparation, well-executed analysis, and plan of implementation should not be underestimated. Poor or hasty implementation can result in no improvement in security, and may even lead to a negative response from employees.

## 5. Conclusion

The topic of knowledge management and its benefits, specifically in cybersecurity is sometimes a very overlooked point of view. Knowledge management serves as a universal tool, which can be slightly modified to be used in many different areas based on its needs. Cybersecurity is highly related to intangible assets, making them the prime target of cyber-attacks. To appropriately react to that fact, the necessity of their protection needs to have a high priority as well, in order to sufficiently protect the most valuable of them. For that, the knowledge of the potential threats, the measures, and responses to them are greatly important to mitigate not only their risks of occurrence but also to help with the potential consequences.

The article briefly describes knowledge management on its own, followed by the diversification of the knowledge types, where understanding and the right incorporation of Tacit, Implicit, and Explicit knowledge are the core parts of the successful application of knowledge management. The work suggests what four steps should be included in the cycle of knowledge management for cybersecurity, stressing the importance of continuous improvement, which is nowadays more important due to the rapid changes in the technological landscape. What one wants to achieve by the right implementation of KM within the organization is to elevate individuals' knowledge to a level where they are aware of potential threats and their consequences, enabling them to respond adequately to such threats. Additionally to that, the other focused area is, to change their behaviour to not only gather information and knowledge just because the regulations and policies say so but also because they know what damage it could eventually cause if they did not know how to respond to some threats.

The possibilities for further research can vary in multiple directions. The process of implementation of the KM cycle in organizations offers many opportunities to study, from the process on its own, methods of implementation, up to the outcomes it could bring. Another point of view about that study could explore the options of education about the knowledge among individuals and their different effectiveness.

## 6. Acknowledgments

This work was supported by the Internal Grant Agency of Tomas Bata University - Faculty of Applied Informatics under project No. IGA/FAI/2023/003.

## 7. References

[1] O. V. Syuntyurenko (2022), Predicting Potential Threats and Megarisks in Information Technology Development, *Scientific and Technical Information Processing*, Vol. 49, no. 1, 48–59, doi: https://doi.org/10.3103/S0147688222010130

[2] Prague Proposals on Cyber Security of EDTs (2021), https://www.nukib.cz/download/Prague_Proposals_on_Cyber_Security_of_EDTs.pdf

[3] D. F. Reding and J. Eaton, Science & Technology Trends 2020–2040 (2020), https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

[4] Talet, A. N. (2018), The Role of Knowledge Management with Risk Management for Information Technology Projects Risk Assessment. *International Journal of Environment and Sustainability* [online]. vol. 6, no. 2. ISSN 1927-9566.

[5] Milton, N. J. and Lambe P. (2020), *The knowledge manager's handbook: a step-by-step guide to embedding effective knowledge management in your organization*. Second edition. London, United Kingdom: Kogan Page Limited. ISBN 9780749484613. Accessed: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=2258716&authtype=ip,shib&custid=s3936755

[6] Rahim, A. S.; Widodo, P.; Reksoprodjo, A. H. & Alsodiq, A. (2023). Identify Cyber Intelligence Threats in Indonesia. *International Journal Of Humanities Education and Social Sciences*, *3*(1), doi: https://doi.org/10.55227/ijhess.v3i1.426

[7] Paulova, I.; Vanova, J.; Rusko, M.; Hekelova, E. & Kralikova, R. (2017). Knowledge Managements for Improvement the Competitiveness of Organization, Proceedings of the 28th DAAAM International Symposium, pp.1221-1226, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-11-2, ISSN 1726-9679, Vienna, Austria, DOI: 10.2507/28th.daaam.proceedings.170

[8] Mohapatra, S.; Agrawal, A. and Satpathy, A. (2016). Designing Knowledge Management Strategy. In: Designing Knowledge Management-Enabled Business Strategies. Management for Professionals. Springer, Cham. https://doi.org/10.1007/978-3-319-33804-1_5

[9] ISO 30401:2018 (2018) Knowledge Management Systems – Requirements, *International Organization for Standardization, Geneva, preview: https://www.iso.org/obp/ui/en/#iso:std:68683:en*

[10] Knoco Ltd (2021), *Global Survey of Knowledge Management 2020-2021*. Online. ©KNOCO LTD 2021. Knowledge management consultants. 2021. Accessed: https://www.knoco.com/knowledge-management-survey.htm.

[11] Rowley, J. (1999), "What is knowledge management?", *Library Management*, Vol. 20 No. 8, pp. 416-420. https://doi.org/10.1108/01435129910291175

[12] Davies, M. (2015), Knowledge–Explicit, implicit and tacit: Philosophical aspects. *International encyclopedia of the social & behavioral sciences*, v. 13: 74-90.

[13] IEC/ISO 27001:2022 (2022), Information security management systems - Requirements, *International Electrotechnical Commission, Geneva, preview: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en*

[14] Jerab, D. A. (2023), How to Deal With Risks and Threats, SSRN Electronic Journal, doi: http://dx.doi.org/10.2139/ssrn.4544513

[15] Sheth, A.; Bhosale, S.; Kurupka, F. (2021), Research Paper on Cyber Security. Contemporary Research in India (ISSN 2231-2137. Special Issue: April 2021.

[16] Probst, Christian & Hunker, Jeffrey & Gollmann, Dieter & Bishop, Matt. (2010), Insider Threats in Cyber Security, doi: dx.doi.org/10.1007/978-1-4419-7133-3

[17] Efijemue, O.; Ejimofor, I. and Owolabi, O. S. (2023), Insider Threat Prevention in the US Banking System. *International Journal on Soft Computing* [online]. 2023, vol. 14, no. 3, s. 17-28. ISSN 2229-7103, doi: 10.5121/ijsc.2023.14302