The concept of improving the security of IT systems supporting the storage of knowledge in organizations

Paweł Moszczyński¹, Maciej Moszczyński²,³, Patrycja Bryczeł-Wróbel⁴, Michał Kapalka⁵,⁶, Tomasz Drozdowski⁷ and Jarosław Wrobel⁸

¹Faculty of Cybernetics, Military University of Technology, Warsaw, Poland; ²TakeCtrl.eu, Warsaw, Poland; ³Institute of Security and Defence, Faculty of Security, Logistics and Management, Military University of Technology, Warsaw, Poland; ⁴Cyber Command, Warsaw, Poland; ⁵Institute of Applied Physics, Faculty of New Technologies and Chemistry, Military University of Technology, Warsaw, Poland

ABSTRACT
This article presents the concept of improving the security of information systems intended for storing knowledge in organizations. It is designed to protect knowledge from leakage, theft or destruction, but without denying access to its resources to employees. It is possible thanks to the introduction of the so-called security and sharing groups (S&S groups) that have two attributes at the same time – the level of knowledge security and the level of knowledge sharing. The proposed concept also assumes assigning knowledge categories to data and enabling the organization to manage the allocation of operations on data from individual knowledge categories to S&S groups. As a result, the system enables the protection of the most valuable knowledge resources, without restricting access to its other categories. The developed concept makes it easier to find a compromise between the strength of security and the free flow of knowledge at the time of system implementation. In addition, the dynamic ability to choose the level of security and the level of access to knowledge in the system allows adaptation to changes taking place in the environment of the organization and increases its resilience.

ARTICLE HISTORY
Received 1 December 2021
Accepted 13 July 2022

KEYWORDS
Knowledge management; knowledge sharing; organization resilience; security

Introduction
The end of the industrial era and the transition to the announced, among others by A. Toffler and P. Drucker (Drucker, 1994; Kundera, 2016), economy is based on information and knowledge forced organizations to transform the model of operation based on labour, raw materials and capital into modern knowledge organizations. Unlike their ‘industrial’ predecessors, knowledge organizations were forced to compete in the conditions of dynamic changes, globalization and fiercely competitive markets. For this reason, it is knowledge, and not, for example, raw materials, that has become a key element of their struggle for survival which allowed them to build a potential and competitive advantage over the environment (Asrar-ul-Haq & Anwar, 2016; Sveiby, 1997).

The knowledge perspective as a key strategic resource of an organization is widely described in the literature on strategic management (Alavi & Leidner, 2001; Cole, 1998; Nonaka & Takeuchi, 1995; Spender, 1996a, 1996b). It is an extension of the enterprise resource theory introduced by Penrose (Penrose, 1958) and developed by other researchers (Barney, 1991; Conner, 1991; Wernerfelt, 1984).

According to this theory, knowledge management should be as important as managing other resources. And based on later studies, it can even be said that, currently, knowledge and its derivative – innovation has become the most important foundation in building the success of an organization (Asrar-ul-Haq & Anwar, 2016; Drucker, 1999; Kogut & Zander, 1992; Nonaka & Takeuchi, 1995). Moreover, since knowledge-based resources are difficult to imitate and contain complex social relations, they can be a source of a long-term competitive advantage for an organization (Alavi & Leidner, 2001).

To manage knowledge organizations use knowledge management systems (KMS) created to support the transfer and processing of knowledge using information technology (IT), in particular information systems and applications such as intranets, systems for knowledge management, document management systems or instant messaging (Gallupe, 2001).

In the literature (Alavi & Leidner, 2001; Cerchione et al., 2015; Corso et al., 2005), we can find the division of KMS into two categories:
(1) Knowledge Management Practices (KMP) defined as a set of methods and techniques supporting the process of creating, storing and transferring knowledge.

(2) Knowledge Management Tools (KMT) describing specific IT-based systems supporting KMP.

On the one hand, the use of KMS undoubtedly accelerates the flow of knowledge and enables its use to create a new knowledge, as well as to take actions that constitute the basis for gaining a competitive advantage (Alavi & Leidner, 2001; Bartol & Srivastava, 2002; Nonaka, 1994). On the other hand, it is important to know which specific tools (KMT) will be used to achieve it.

Since the use of poorly secured IT tools may expose the organization’s knowledge to cyber threats, related to violation of its integrity, confidentiality, availability and non-repudiation. These threats involve the risk of cutting off the organization’s access to knowledge or knowledge leakage, as well as losing its attribute of exclusivity, which is crucial to building a competitive advantage (Jordan & Lowe, 2004).

Thus it is necessary to use KMT that will allow organization’s members for free (but tailored to their needs) access to knowledge, while securing this knowledge against leakage, destruction, deletion or unauthorized modification, and, in such a way that the key knowledge resources stored in the organization remain safe and confidential.

To meet this challenge, this paper proposes a methodology for classifying and securing knowledge stored in KMT. Its essence comes down to creating special security and sharing groups (S&S groups) for individual knowledge operations. Each group (S&S group) simultaneously has a certain level of IT security and a different sharing status (e.g. knowledge available to everyone, only to those who need it, or to selected users). Thanks to this, it is possible to classify the knowledge processed in the organization and assign different security levels to different resources.

Threats to KMT supporting knowledge storage

To better present the idea of security and sharing groups, the authors focused in their work on the description of KMT for processes supporting knowledge storage. They are especially important because organizations constantly create new knowledge, as well as learn and forget just like any human being. At the same time, like with humans, organizations also store and restore knowledge. The kind of knowledge that is preserved has been called organizational memory (Stein & Zwass, 1995; Walsh & Ungson, 1991). It is equivalent to the set of neural connections in the brain on which knowledge management operations – in this case, the knowledge of the organization – are docked. This memory comes in many forms. It includes knowledge in various forms, e.g. written documentation, information in electronic databases, codified knowledge contained in expert systems, documented procedures and organizational processes, and, most interestingly, also tacit knowledge belonging to individual members or groups of people in the organization (Alavi & Leidner, 2001; Tan et al., 1998).

As an extension of the organizational memory possibilities, advanced data storage technologies and techniques of searching for information in external memory databases are used. KMT are effective tools for increasing the efficiency of using organizational memory. They can increase the speed of access to both memory and product memory. They can also enable organizations to create intra-organizational memory in the form of both structured and unstructured information and share this memory over time (Alavi & Leidner, 2001; Vandenbosch & Ginzberg, 1996). Moreover, the use of KMT for document management allows simultaneously for the storage of knowledge and its effective sharing, even in the variant of distributed storage locations and different moments of time (Alavi & Leidner, 2001).

The benefits of implementing KMT supporting knowledge storage seem unquestionable. Unfortunately, organizations are still sceptical about their implementation. The problem is primarily the cost of purchasing these systems, their complicated operation (Branscomb & Thomas, 1984; Davis, 1989; King, 1999) and the risk of loss or leakage of the knowledge stored and processed in KMT (Rot & Sobińska, 2017). While money for the system can be set aside and systems can be simplified, the fear of losing confidential data and leakage of organizational knowledge is fully justified.

How serious is this threat is demonstrated by numerous cybersecurity studies, for example, the 2018 Cyber Security Breaches Survey2 shows that 43% of companies experienced a breach of their systems in the 12 months preceding the survey and suffered from cyberattacks. On the other hand, the Global Information Security Survey (GISS) conducted by Ernst Young3 shows that the average cost of losses due to hacking into the organization’s database is $3.62 million.

Therefore, it is not surprising that managing the risk related to cybersecurity, in the era of widely used information and communication technologies, is one of the greatest challenges of organizations on which depends not only economic but also social development.4

Referring to the concepts related to information security, we can mention three main threats to the knowledge processed in the IT system: threats to confidentiality, integrity and availability. These threats are associated
with elements of the so-called CIA triad (Dhillon & Backhouse, 2001; Samonas & Coss, 2014), which is one of the commonly used information security models in which are distinguished three basic threats to the organization’s KMT which may cause potentially unfavourable processes and, consequently, widely understood losses. Threat to confidentiality is connected with an unauthorized access to knowledge in the system. Knowledge confidentiality loss may occur, for example, in the case of sending it via ICT network without the use of encryption or in a situation where, using phishing methods, an adversary obtained the login details of an authorized user and used them to gain access to the data.

Threat to integrity is related to the introduction of unauthorized changes to the organization’s knowledge. For example, the organization deals with the knowledge integrity loss in a situation where a disloyal accountant modifies the provisions of the organization’s accounting system, thanks to which he hides the fact of illegal operations on the company’s accounts or in a situation when the invoice data, in the course of sending it to the accounting department, will be modified as a result of which the accounting will pay the invoice to the wrong account.

Threat to availability is related to temporary or permanent unavailability of some or all organization’s knowledge stored and processed in the system. Such a phenomenon may occur due to natural causes, e.g. a fire in the server room or a power loss, as well as it may be the result of adversaries deliberate actions, e.g. as a result of a distributed denial of service (DDOS) attack.

Apart from the canonical three types of threats to the organization’s knowledge, the literature also includes extensions of the CIA model. From the KMT point of view, the following threats also seem important:

Threat to authenticity is related to entering data into the system on behalf of another entity, unaware of a given activity. Again, the example with an invoice may be used here. The adversary sends an invoice to the accounting department for payment, claiming to be the head of the procurement department. Another example is an IT specialist pretending to be his colleague and modifying the knowledge in the system on his behalf.

Threat to non-repudiation is related to an attempt by an entity operating in the system to deny the fact of performing a specific operation on knowledge. An example of such a phenomenon may be a supervisor who gives an order to a subordinate through the system, and then, due to unfavourable development of events, denies the fact that he gave such an order. We deal with a similar situation when a message is sent from one system user to another, and then, the first of them denies the fact that this act was done.

At this point it is worth adding that the attributes of authenticity and non-repudiation were not the only attempts to extend the CIA triad, researchers from 1980 to today have repeatedly attempted to update and supplement this list (Anderson, 2001; Dhillon & Backhouse, 2001; Dhillon & Torkzadeh, 2006; Harris, 2002). These attempts resulted in the introduction of additional criteria related to information security, such as correctness of specification, responsibility, integrity of people, trust, ethicality and identity management.

However, even based on a simplified image, one can be convinced that failure to ensure any of the five basic criteria may lead not only to the loss of access to knowledge (e.g. due to failure of servers or IT systems) but also to its corruption or leakage, which as mentioned above, may result in a loss of the knowledge exclusivity. And this exclusivity allows to build a knowledge-based competitive advantage of modern organizations.

Therefore, it is necessary to take into account in KMT not only their ability to store and search through the organization’s knowledge but also to secure it effectively and guarantee the required level of all five security attributes. The threats mentioned above are counteracted by KMT by using the number of mechanisms, such as encryption, digital signature, strong, multi-factor authentication, intranets and hash functions.

**KMT securing methods overview**

Organizations use the basic security mechanism of access control to ensure controlled processing and knowledge sharing. Traditionally, the definition of ‘access control’ is a decision to authorize access for a user who wants to use specific resources (Park & Sandhu, 2004). In terms of computer security, access control is classically carried out in three main stages – **identification, authentication and authorization** (Kim & Solomon, 2010, p. 147; Subhani & Amjad, 2020 Chapter 9; Todorov, 2007).

The first stage task, which is **identification**, is to determine the identity of a given person. In a digital world, this means providing a unique login stored in the system of a given e-service (Sonnenbichler, 2013, Chapter 1). Identification allows to tell ‘who it is’ but does not confirm that the user of a given service is actually the person who has been declared and identified. User identification is the basis of the so-called AAA (authentication, authorization, accounting) (Andress, 2011, Chapter 1).

The second stage, which is **authentication**, is the process of verifying whether we are who we say we are (Andress, 2011, Chapter 2). In the era of cybercriminals and e-entity theft, it is a key process for maintaining data confidentiality. Currently, three main methods of authentication are used, based on:
• something you know – the user must provide information known only to him, e.g. pin, password, date of birth;
• something you have – the user must provide that he has an object assigned to him, e.g. an access card, a mobile phone on which he will receive a message with an access code, e-mail account;
• who you are – the user must prove to the system that he has appropriate biometric features, such as fingerprint, eye retinal pattern, blood vessel distribution (Manikupri 2017).

Nowadays, it is a common practice to use more than one factor at a time for authentication, e.g. the user, when logging in to the system, must enter the password and additionally rewrite the code from the text message received on the phone. The more the data in the system require more protection, the greater the number of factors needed to be presented to the system in the authentication process.

However, it should be remembered that the intrusiveness of this element of the access control process should not be too complex and time-consuming which could lead to attempts to circumvent this problem, e.g. by lowering the value of knowledge placed in KMT, so that it would not require as strong protection as it should.

The third stage is authorization, i.e. verifying whether the person who has successfully passed the identification and authentication has the right to access specific content. The scope of the rights granted results mainly from the role of this person and the procedures used in the organization (Andress, 2011, Chapter 3).

There are four basic methods of resource access control in the literature: MAC (Mandatory Access Control), DAC (Discretionary Access Control), RBAC (Role Based Access Control) and ABAC (Attribute Based Access Control).

**Mandatory access control** MAC is a method of controlling access to the system in which we distinguish a set of entities capable of performing actions and objects on which actions can be performed. In the case of MAC, objects are given certain security attributes, e.g. document security classification level (e.g. secret, top secret data). The system is equipped with several policies based on which it decides whether the entity can perform specific actions on the site, e.g. an employee of the organization wants to read data in the system marked as sensitive data and the policy says that such data can only be accessed by a person from the Management Board. Therefore, depending on whether the employee is a member of the Management Board or not, access to the data may be granted.

Another look at the access control issue is **discretionary access control** DAC – where the data owner decides who and to what extent will have access to it. The data creator is usually considered the data owner. In this model, the owner can delegate his rights to any entity in the system. This access control model is much less restrictive compared to MAC. Its weak point is the fact that it depends on the system users how the data is protected, so it is quite easy to lose control over the level of access control to data in the system.

Yet another look can be at **access control based on RBAC roles** – where data access permissions are not assigned directly to entities, but indirectly through roles. For example, access to the preview of accounting data in the system may be granted to all accounting employees (for whom the role of the accounting employee was created in the system), while the possibility of saving data is granted only to selected employees (for whom the role of the accounting data administrator was created in the system). Any number of roles may be assigned to individual entities appearing in the system. Most often, user roles result from the position held by the employee in the organization (Zhang et al., 2007).

Development of access control methods and development of KMT-related practices led to the creation of **access control based on ABAC attributes** – where entities, objects, as well as individual actions and contexts can be assigned attributes based on which the system equipped with policies (similar to the MAC) decides to grant access to data. Such policies can be, for example: blocking access to the file to people who connect to the system from foreign IP addresses or allowing people working in the sales department to access a tab on the website who have authenticated themselves to the system using a strong authentication mechanism. This model enables more diversified and flexible protection of the organization’s knowledge.

Since most of the modern KMT operate in an open network environment, apart from access control, it is also important to secure the processed data with encryption. This encryption should apply to both the encryption of the so-called data at rest, i.e. data stored on data carriers, and the encryption of data in motion, i.e. data sent via ICT.

**Availability-security dilemma**

The introduction of encryption and access control to IT systems supporting knowledge storage allows to significantly reduce the risk of leakage, destruction, deletion or unauthorized modification of the organization’s digital memory. Unfortunately, the more stringent safeguards are applied to the KMT system, the more difficult it will be to share knowledge and obtain an environment for
its growth due to the effort required to use these systems (Davis, 1989). Which means that a rigorously secured knowledge storage support system can be so complicated and difficult to use as to be impractical. Because it will take too much effort to use the resources stored in it. Therefore, for the KMT system to support the organization’s activities in real terms, it is necessary to find a compromise (C) between the strength of security and the free flow of knowledge (see figure below).

This compromise will change, among others, depending on the organization’s management style and its structure. For example, according to the typology introduced by Frederic Laloux, the so-called red organizations dominated by the management authoritarian style, strict division of labour and power exercised by sovereignty (Laloux, 2014, p. 51) will value more knowledge confidentiality and its security. Because knowledge will be available only to a narrow group of management (e.g. management board or directors).

Whereas the so-called turquoise organizations, that have moved away from industrial operation patterns and abandoned the hierarchical pyramid of roles and positions in the direction of decentralization and teams’ self-management, will need KMT allowing for effective knowledge sharing. Because in turquoise organizations, the impulses to act no longer come only from the management, but from each employee, just like in a living organism, in which impulses to act come from every cell and every part of the organism without the need for central management and command-giving control (Laloux, 2014, p. 72).

The summary of these ‘organizational poles’ shows a variety of needs and requirements for KMT and explains why it is necessary to design such a system that will allow the organization to independently determine a compromise between the strength of security and freedom of knowledge flow. To enable this, in the next chapter, the authors proposed the introduction of a system access control mechanism to KMT that has two parameters at the same time:

- the required level of security, which determines what access control methods are used to authenticate a given operation based on knowledge (in line with the company’s policy and its risk appetite),
- and the level of sharing, which determines which users or group of users should have access to a given operation on knowledge.

Together, these parameters create a new entity which is the security and sharing group, thanks to which organizations can work out a compromise consistent with their policy (C) and resolve the security-accessibility dilemma for individual types of knowledge processed in KMT.

**Security and sharing groups concept**

The goal of S&S groups is to simultaneously protect and share the knowledge processed in KMT, therefore, before groups are introduced, the organization must determine the value of its knowledge resources and their sensitivity to leakage and cyber threats. This means the need to classify all the organization’s knowledge and, then, divide it into categories so that each resource of knowledge (e.g. project documentation, reports, personal data, medical data, patents, etc.) is assigned to one of the knowledge categories.

Then, it is necessary to determine which operations on a given category of knowledge can be performed within the framework of the KMT used, e.g. it may be: knowledge reading, knowledge reading and recording, reading, writing and deleting knowledge, etc. This is important because, from the perspective of the IT system, some other risk to knowledge is related to its reading, e.g. from a computer, as well as another risk is related with the possibility of simultaneous editing or deleting. Just like a different thing would be to show the test results report at a meeting with the customer and another thing would be to send the report to their private mailbox.

It should be mentioned here that the number of available operations on knowledge can vary for each category of knowledge – O1, O2, O3, ... OK. For example, with regard to the set of operation O1 for a knowledge category that is publicly available, an organization might allow employees to read, edit or even delete that knowledge because there are no valuable resources in that category. While only a knowledge-reading operation will be allowed in the operation set O3, as this collection refers to a category containing confidential or sensitive data (e.g. medical data or customer contracts).

After designing the knowledge categories in the system (1, 2, 3, ..., K) and the number of operations on knowledge from each category (O1, O2, O3, ... OK), we can proceed to assign individual operations on kth category of knowledge (1, ..., Ok) to security and sharing groups. Which means that there will be assigned two parameters to them:

- the required level of security specifying the methods of controlling the access to a given operation that will take values from 1 to X,
- the level of sharing determining which users or groups of users have access to a given operation on knowledge and taking values from 1 to Y.
The exact scope of safeguards included in each level of safety and determining who should have access to knowledge within the sharing levels is not strictly defined in this work, as the number of categories of knowledge K and parameters X and Y will be determined for each KMT differently, taking into account organization’s risk management policy of technical capabilities of the KMT system itself.

As shown in the ideological diagram in Figure 2, a single S&S group can contain operations on different categories of knowledge. In addition, different operations in the same category of knowledge can go to different S&S groups. This is symbolically represented as different coloured columns on the plane (x, y). The possibility of such allocation allows for comprehensive management of the level of dissemination and security to ensure confidentiality, integrity and availability. The possibility of such allocation allows for a comprehensive management of the level of sharing and security to ensure confidentiality, integrity and availability. For example, any user who logs in to KMT will have access to a document with knowledge, but only selected persons who pass the additional authorization will be able to delete the document (what will simultaneously ensure the maximum sharing and protection of the knowledge resource integrity).

The introduction of S&S groups allows for the implementation of different security procedures for different knowledge operations within a single system. In addition, it introduces an additional mechanism that supports sharing knowledge processes and knowledge dissemination to the organization’s members. This allows the KMT administrator to manage both the level of knowledge security and the level of knowledge sharing that users add to the system.

For example, a turquoise organization building its competitive advantage on knowledge can create an open system that allows each user to access most of the knowledge as soon as they log in to the system. And an orange organization (e.g. government administration) will create a closed system that will guard most of the knowledge very rigorously (e.g. via VPN connection, encryption and multi-step user authentication, etc.)

**Method of assigning operations to groups**

The authors in the presented S&S groups concept did not define one single method for assigning operations to security and sharing groups which is due to several reasons. The first is the lack of a common risk management policy for the processing of KMT knowledge for all types of organizations. This means that each organization determines its risk appetite itself, meaning the amount of risk it can accept in connection with conducting a particular activity by setting a point of compromise between the benefits of introducing KMT available to all employees (see Figure 1) and the risks associated with the lack of confidentiality and integrity of the knowledge processed in the system.

Therefore, on the one hand, we will find organizations putting the safety of knowledge stored in KMT first, and the purpose of their policy is to protect knowledge, e.g. red and orange organizations (with a strongly drawn division of labour and power). On the other hand are those who are primarily interested in sharing knowledge with employees, because the purpose of their policy will be to use knowledge to improve the efficiency of organization’s work and development, as is the case in green and turquoise organizations. The divergence of strategic objectives between different organizations shows that two opposing poles cannot be assigned an identical method of assigning operations to security and sharing groups.

Another limitation is due to the multifaceted nature of knowledge. Knowledge is defined as ‘a legitimate belief that increases an individual’s ability to act effectively’ (Huber, 1991; Nonaka, 1994). Knowledge can be viewed from several perspectives: (1) state of mind, (2) state of object, (3) state of process, (4) state of condition of access to information or (5) state of ability (Alavi & Leidner, 2001). These different views on knowledge lead to different perceptions of knowledge management (Carlsson et al., 1996) which is reflected in the diversity of IT systems supporting knowledge storage and their continuous development. Therefore, it will be necessary to adapt the method of assigning operations to S&S groups to the specificity of the KMT system used in the given organization.

Another limitation is related to dynamic development of IT technology and its impact on KMT security, e.g. work
development on a quantum computer may create a danger of deciphering data transmission in the network (Abd El-Latif et al., 2018; Ribordy et al., 2000). This development forces KMT designers to continuously improve security to eliminate the vulnerability of the system to new threats on an ongoing basis.

Taking into account these various challenges and problems that an organization must face, the article proposes an introduction of S&S groups to KMT. Thanks to them, it is possible to select various security and sharing policies for various types of knowledge within one IT system. This allows to apply in KMT different security policies for different categories of knowledge processed in the system. For example, you can process documents and contracts in the accounting department in a different security regime, operational knowledge in another regime, as well as knowledge building a competitive advantage in some other one. Thanks to this, the proposed framework enables simultaneously sharing knowledge necessary for the enterprise development and protecting the most confidential knowledge. Moreover, the flexibility of the system means that the security levels and sharing levels of each S&S group can be changed in the future so that:

- S&S groups can be modified based on current system performance audits,
- current vulnerabilities and threats to IT systems can be taken into account in S&S groups security, adapting system security to the dynamically changing world of cybersecurity threats.

Despite the high flexibility of the solution related to assigning knowledge to S&S groups, there is also a potential barrier to its implementation. It is related to the higher cost of introducing the system to the organization, resulting from the need to develop one’s methodology for assigning operations to particular S&S groups. However, this investment pays off not only by increasing the efficiency of the organization’s operation (resulting, i.e. from a better knowledge flow, including the tacit knowledge transfer), but, also, by increasing the security of its key memory resources. Therefore, its undertaking by the organization seems fully justified.

**Case study of using S&S groups**

Because in the presented concept of S&S groups, there is no one method of assigning operations on knowledge to S&S security (see Figure 2), for a better explanation of the mechanism of their operation, we will use the example of the KMT system intended for storage of documents (Document Management System – DMS) dedicated to research groups at a university or at a research and development institute.

The case study will be based on a simplified design of a DMS for a project group implementing a research grant at the Military University of Technology (Warsaw, Poland). This group is composed of an interdisciplinary team of scientists which bases its operation on the paradigm of a green organization according to the Laloux typology (Laloux, 2014). The goals of the group (hereinafter referred to short as the ‘RID group’) include: research activities as part of the implementation of grants, rapid development of scientists participating in projects and increasing the potential of the organization to gain a competitive advantage.

We use a combination of role-based and attribute-based control systems – where the RBAC system establishes your high-level security before fine-tuning additional variables through an ABAC system. The knowledge of the RID group was divided based on its importance in building a competitive advantage and the degree of confidentiality. These two parameters result in four possible combinations:

**Knowledge categories in the DMS for the RID group**

- **Category 1 – containing knowledge available but not allowing to build a competitive advantage**, which is collected in the knowledge management system and used by employees, but is not of key importance for the success of the organization. This category will include: the organization’s articles published by the team and publicly available teaching materials.
- **Category 2 – containing knowledge available and allowing to build a competitive advantage**, which is not confidential, but its proper processing and use in making decisions and carrying out tasks allows to build the success of the organization. This category will include: key references that have been verified by team members and selected teaching materials intended for graduate students and new team members.
- **Category 3 – containing confidential knowledge, but not allowing to build a competitive advantage**, disclosure of which exposes the organization to the risk related to the leakage of sensitive data. This category will include: personal data or confidentiality agreements.
- **Category 4 – containing confidential knowledge and allowing to build a competitive advantage**, disclosure of which could result in the loss of the innovation attribute of this knowledge and expose the organization to the risk related to the leakage of strategic data. This category will include: measurement data,
Figure 2. Diagram of the security and sharing groups concept. In the list of operations, a single operation has been marked with two numerical indices (e.g., 1,1), where the first is the number of the knowledge category and the second is the operation number in this category.

unpublished manuscripts or unsent project applications.

The following sets of operations are possible for the designated categories in the presented DMS:

| Operations for knowledge category no. 1: | Operations for knowledge category no. 2: |
|----------------------------------------|----------------------------------------|
| Op. (1,1) add your own published article | Op. (2,1) add key reference |
| Op. (1,2) download your own published article | Op. (2,2) download key reference |
| Op. (1,3) delete your own published article | Op. (2,3) delete key reference |
| Op. (1,4) add generally available materials | Op. (2,4) add teaching materials for graduate students |
| Op. (1,5) download generally available materials and new team members | Op. (2,5) download teaching materials for graduate students and new team members |
| Op. (1,6) delete generally available materials and new team members | Op. (2,6) delete teaching materials for graduate students and new team members |

Operations for knowledge category no. 3:
| Operations for knowledge category no. 4: |
|----------------------------------------|
| Op. (3,1) add personal data | Op. (4,1) add measurement data |
| Op. (3,2) download personal data | Op. (4,2) download measurement data |
| Op. (3,3) delete personal data | Op. (4,3) delete measurement data |
| Op. (3,4) add contract | Op. (4,4) add unpublished manuscript |
| Op. (3,5) download contract | Op. (4,5) download unpublished manuscript |
| Op. (3,6) delete contract | Op. (4,6) delete unpublished manuscript |
| Op. (4,7) add unsent project application | Op. (4,8) download unsent project application |
| Op. (4,9) delete unsent project application |

After establishing the lists of operations on knowledge, one should define the required security and sharing levels for them allowing to assign individual knowledge operations to S&S groups.

**Proposed levels of required system security for the RID group**

- X1 – access to the system after logging in with a password and login, automatic logout after 15 min of inactivity.
- X2 – access to the system for a logged-in user connecting from a trusted IP address, automatic logout after 15 min of inactivity.
- X3 – access to the system for a logged-in user connecting from a trusted IP address and a trusted device (verified machine address), automatic logout after 10 min of inactivity.
- X4 – access to the system for the logged-in user connecting from a trusted IP address and a trusted device (verified machine address) and having a decryption key, because the documents in the system are encrypted at this level, automatic logout after 5 min of inactivity.

**Proposed levels of system sharing for the RID group**

- Y1 – all members of the RID group.
Y2 – dedicated groups that should have access to a given resource of knowledge due to the tasks performed, e.g. theoretical team, measurement team.

Y3 – authors and team leaders.

Y4 – team leaders only.

After establishing the lists of knowledge operations, levels of required security and levels of sharing, we can proceed to assign individual knowledge operations to S&S groups. In the RID research group, the assignment is as follows:

In Figure 3, several knowledge operations from individual categories are assigned to S&S groups as follows:

- Operations on knowledge from category no. 1 (available, but not allowing to build a competitive advantage) were assigned to the S&S group with the maximum level of sharing and minimum security. To create a handy knowledge repository that can be used practically without restrictions.

- Operations on knowledge from category no. 2 (available and allowing to build competitive advantage) were assigned to S&S groups that ensure a wide sharing of knowledge and protect it against deletion.

- Operations on knowledge from category no. 3 (confidential, but not allowing to build competitive advantage) were assigned to the S&S group with a high level of security and a limited level of sharing. Because these operations relate to confidential knowledge, the leakage of which may result in, for example, contractual penalties, legal restrictions or a decrease in trust on the part of cooperators.

- Operations on knowledge from category no. 4 (confidential and allowing to build competitive advantage) were assigned to S&S groups with the highest security level. On the other hand, the level of sharing was selected in such a way as to enable the processing of this knowledge, but only to the extent that is necessary to build a competitive advantage – while ensuring its confidentiality, integrity and availability attributes.

In this way, we determine the possible compromise between the strength of security and the free flow of knowledge in the DMS. It should be noted that the group assignment to the S&S groups shown in Figure 3 can be regarded as temporary and may change dynamically. Thus it can be adapted to changes in the organization’s environment, such as working remotely during a COVID 19 pandemic (Figure 4) or increasing the alert level regarding threats in cyberspace from ALFA-CRP to CHARLIE-CRP in Poland in February 21, 2022 (Figure 5). In the first case, we propose to reduce security and facilitate access to knowledge for employees. However, if these changes were not introduced, employees would have to send documents by e-mail to perform their duties, which further would reduce the security of shared knowledge. In the second case, due to a significant increase in risk and possible compliance issues, we propose the opposite solution.
Figure 4. Knowledge operations’ assignment to S&S groups in an organization with a remote work system during a COVID 19 pandemic.

Moreover, reassigning knowledge to S&S groups will not require costly system rebuilding. Therefore, introducing them into the system will increase the level of the organizational resilience understood as the ability of a company to anticipate, plan and respond to difficulties when they occur. This shows that the concept is versatile because it offers the possibility of addressing different resolutions of the availability-safety dilemma (Figures 3–5).

Figure 5. Knowledge operations’ assignment to S&S groups in alert level threats in cyberspace CHARLIE-CRP.

**Summary**

Based on the analysis of the challenges faced by contemporary organizations building a competitive advantage based on knowledge, this paper proposes the concept of security and sharing groups – S&S. These groups allow to design dedicated knowledge management tools – KMT, tailored to the type and nature of any organization because it offers opportunities to design agile and open knowledge management systems.
It shows that S&S groups allow the organization to respond dynamically to changes in its environment such as new cyber threats or new data protection regulations. Thanks to S&S groups we could create more conscious policies for managing the availability of knowledge in an organization by allowing it to share knowledge of a different nature on different security principles and it helps organizations continually manage and mitigate risk during change.

The presented concept should significantly help KMT creators to ensure the security of information systems intended for storing knowledge in organizations, but without denying access to its resources to employees. It also allows, within a single KMT system, to apply several different security and sharing policies for different knowledge resources which enables the creation of ‘tailor-made’ tools for storing organizational memory that will support knowledge sharing in the organization.

Notes

1. ISO/IEC 27002:2005(en) Information technology — Security techniques — Code of practice for information security management, p.1.
2. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018, access: 2020.04.18.
3. Y Global Information Security Survey (GISS) 2018–2019.
4. https://www.ey.com/en_gl/advisory/global-information-security-survey-2018-2019, access 2020.04.18.
5. The value of knowledge resources is understood as the value of specific knowledge resources for building organization’s competitive advantage.
6. The sensitivity of knowledge should be determined on the basis of the vulnerability to, i.e. confidentiality and integrity of the knowledge resource concerned.
7. The team is implementing a grant entitled: ‘Development and experimental verification of new concepts of quantum transport characterization in complex semiconductor heterostructures’, financed under the program of the Minister of Science and Higher Education under the name ‘Regional Initiative of Excellence’ in 2019–2022, project number 014/RID/2018/19, funding amount of PLN 4 589 200.00.
8. Whether knowledge allows to build a competitive advantage can be determined, inter alia, by using VRIO criteria or by commissioning an audit of the organization’s knowledge.
9. For example regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Funding

Project financed under the program of Polish Ministry of Education and Science under the name ‘Regional Initiative of Excellence’ in 2019–2022, project number 014/RID/2018/19, funding amount of PLN 4 589 200.00.

References

Abd El-Latif, A. A., Abd-El-Atty, B., & Talha, M. (2018). Robust encryption of quantum medical images. IEEE Access, 6, 1073–1081. https://doi.org/10.1109/ACCESS.2017.2777869
Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. MIS Quarterly, 25(1), 107–136. https://doi.org/10.2307/3250961
Anderson, R. (2001). Why information security is hard – An economic perspective. Seventeenth Annual Computer Security Applications Conference (pp. 358–365). IEEE, December.
Andress, J. (2011). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice. Elsevier Science.
Asrar-ul-Haq, M., & Anwar, S. (2016). A systematic review of knowledge management and knowledge sharing: Trends, issues, and challenges. Cogent Business & Management, 3(1). https://doi.org/10.1080/23311975.2015.1127744
Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 21. https://doi.org/10.1177/014920639101700109
Bartol, K. M., & Srivastava, A. (2002). Encouraging knowledge sharing: The role of organizational reward systems. Journal of Leadership & Organizational Studies, 9(1), 64–76. https://doi.org/10.1177/10717919020090105
Branscomb, L. M., & Thomas, J. C. (1984). Ease of use: A system design challenge. IBM Systems Journal, 23(3), 224–235. https://doi.org/10.1147/sj.23.3.0224
Carlsson, M., Ahlfeldt, H., Thurin, A., & Wיגertz, O. (1996). Terminology support for development of sharable knowledge modules. Medical Informatics, 21(3), 207–214. https://doi.org/10.3109/1463932960923538
Cerchione, R., Esposito, E., & Spadaro, M. R. (2015). The spread of knowledge management in SMEs: A scenario in evolution. Sustainability, 7(8), 10210–10232. https://doi.org/10.3390/su70810210
Cole, R. E. (1998). Introduction. California Management Review, 40(3), 15–20. https://doi.org/10.2307/41165940
Conner, K. R. (1991). A historical comparison of resource-based theory and five schools of thought within industrial organization economics: Do we have a new theory of the firm? Journal of Management, 17(1), 121–154. https://doi.org/10.1177/014920639101700109
Corso, M., Martini, A., Pellegrini, L., & Paolucci, E. (2005). Knowledge management systems in continuous product innovation. Intelligent knowledge-based systems: Business and technology in the new millennium. C. T. Leondes. Boston, MA, Springer US: 36–66.
Davis, F. D. (1989). Perceived usefulness, Perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/2490008
Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. Information Systems Journal, 11(2), 127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Disclosure statement

No potential conflict of interest was reported by the author(s).
Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293–314. https://doi.org/10.1002/isj.20575.2006.00219.x

Drucker, P. F. (1994). The age of social transformation. The Atlantic Monthly, 274(5), 53.

Drucker, P. F. (1999). Post-capitalist society. Science Publishing Company PWN.

Galleu, B. (2001). Knowledge management systems: Surveying the landscape. International Journal of Management Reviews, 3(1), 61–77. https://doi.org/10.1111/1468-2370.00054

Harris, S. (2002). Mike Meyers’ CISSP(R) Certification Passport, McGraw-Hill Osborne.

Huber, G. P. (1991). Organizational learning: The contributing processes and the literatures. Organization Science, 2(1), 88–115. https://doi.org/10.1287/orsc.2.1.88

Jordan, J., & Lowe, J. (2004). Protecting strategic knowledge: Insights from collaborative agreements in the aerospace sector. Technology Analysis & Strategic Management, 16(2), 241–259. https://doi.org/10.1080/09537320410001682900

Kim, D., & Solomon, M. G. (2010). Fundamentals of Information Security. Jones & Bartlett Learning.

King, W. R. (1999). Integrating knowledge management into strategy. Information Systems Management, 16(4), 70–72. https://doi.org/10.1177/107809879901600402

Kogut, B., & Zander, U. (1992). Knowledge of the firm, combinative capabilities, and the replication of technology. Organization Science, 3(3), 383–397. https://doi.org/10.1287/orsc.3.3.383

Kundra, E. (2016). Alvin Toffler’s concept of the supersymbolic economy. Economic Studies. Science Papers of the University of Economics in Katowice, Poland 259.

Laloux, F. (2014). Reinventing organizations inspired by the next stage in human. S.L., Nelson Parker.

Manikpuri, M. M. (2017). Biometric security systems for beginner. eBooks2go Incorporated.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. Organization Science, 5(1), 34–51. https://doi.org/10.1287/orsc.5.1.34

Nonaka, I., & Takeuchi, H. (1995). The knowledge-creating company: How Japanese companies create the dynamics of innovation. Oxford University Press.

Park, J., & Sandhu, R. (2004). The UCONABC usage control model. ACM Transactions on Information and System Security, 7(1), 128–174. https://doi.org/10.1145/984334.984339

Penrose, E. T. (1958). The theory of the growth of the firm. Wiley.

Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O., & Zbinden, H. (2000). Fast and user-friendly quantum key distribution.

Spender, J.-C. (1996a). Making knowledge the basis of a dynamic theory of the firm. Strategic Management Journal, 17(52), 45–62. https://doi.org/10.1002/smj.4250171106

Tan, S., Teo, H.-H., Tan, B., & Wei, K.-K. (1998). Integration of ERM and enterprise architecture: Plus ça change. Information Systems Journal, 8(3), 383–397. https://doi.org/10.1023/A:1020228716551 DailyLifePress.

Vandenbosch, B., & Ginzberg, M. J. (1996). Lotus notes® and collaboration: Fundamentals of identity management. CRC Press.

Walsh, J. P., & Ungson, G. R. (1991). Organizational memory. The Academy of Management Review, 16(1), 57–91. https://doi.org/10.2307/258607

Weber, M., & Hager, R. (2004). A resource based view of the firm. Strategic Management Journal, 5(2), 5. https://doi.org/10.1002/smj.4250050207

Zhang, Z., Yang, Q. Pei, and J. Ma (2007). Research on usage control model with delegation characteristics based on OM-AM methodology. 2007 IFIP international conference on network and parallel computing workshops (NPC 2007).18-21 September.