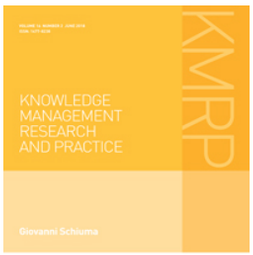

Knowledge Management Research & Practice

ISSN: 1477-8238 (Print) 1477-8246 (Online) Journal homepage: www.tandfonline.com/journals/tkmr20

Reconciling digital transformation and knowledge protection: a research agenda

Ilona Ilvonen, Stefan Thalmann, Markus Manhart & Christian Sillaber

To cite this article: Ilona Ilvonen, Stefan Thalmann, Markus Manhart & Christian Sillaber (2018) Reconciling digital transformation and knowledge protection: a research agenda, Knowledge Management Research & Practice, 16:2, 235-244, DOI: 10.1080/14778238.2018.1445427

To link to this article: https://doi.org/10.1080/14778238.2018.1445427

KNOWLEDGE MANAGEMENT RESEARCH & PRACTICE
2018, VOL. 16, NO. 2, 235–244
https://doi.org/10.1080/14778238.2018.1445427

THE OPERATIONAL RESEARCH SOCIETY
Taylor & Francis
Taylor & Francis Group

ORIGINAL ARTICLE

Reconciling digital transformation and knowledge protection: a research agenda

Ilona Ilvonen[a], Stefan Thalmann[b], Markus Manhart[c] and Christian Sillaber[c]

[a]Laboratory of Industrial and Information Management, Tampere University of Technology, Tampere, Finland; [b]Pro2Future & Know-Center, Graz University of Technology, Graz, Austria; [c]Department of Computer Science, University of Innsbruck, Innsbruck, Austria

ABSTRACT

Digital transformation revolutionises the way people work not only in office settings but also in physical work settings such as manufacturing or construction. New ways of combining digital and physical innovations and intensified inter-organisational collaborations are key characteristics for success. Knowledge sharing becomes increasingly important, but its inter-organisational nature and the blurring of organisational boundaries create new challenges for the protection of knowledge. Existing research on knowledge protection mostly focuses on single organisations or on dyadic relationships. Complex sharing arrangements and especially sharing in networks has received little attention so far. This paper presents a literature review, integrating the perspectives of the base domains of knowledge, strategy, innovation, and information security management with the goal to identify knowledge protection requirements in the era of digital transformation. Five avenues for future research on knowledge protection to support organisations coping with challenges imposed by digital transformation are presented.

ARTICLE HISTORY
Received 29 March 2017
Revised 20 October 2017
Accepted 21 February 2018

KEYWORDS
Knowledge protection; knowledge sharing; networks; knowledge management; digital transformation; industry 4.0; computer-integrated manufacturing; literature review

1. Introduction

Digital transformation creates new challenges for the protection of knowledge a firm holds. Industry 4.0 describes the digital transformation and interlinking of companies working together in supply chains (Kagermann, Lukas, & Wahlster, 2011). Digital transformation means development towards digitally interlinking not only machines and IT infrastructure but also people (Spath et al., 2013). The development increases (1) the importance of technology platforms, (2) emergence of distributed innovations, and (3) prevalence of combinatorial innovation (Yoo, Boland, Lyytinen, & Majchrzak, 2012). In the transforming organisations, employees have to acquire increasingly complex knowledge in increasingly shorter time and collaborate with more people to develop innovations (Sherehiy & Karwowski, 2014). Collaboration and knowledge exchange happen across supply chains, and organisational boundaries are blurring. However, the close collaboration and exchange of knowledge increase the risk of unintended knowledge spillovers.

Currently, digital transformation of operations is mostly viewed from a technical perspective, emphasising the importance of technology platforms and their integration. The role of humans is widely neglected (Bhamu & Sangwan, 2014), although the knowledge required for innovations is bound to people. As a result, the focus is on technical information security aspects. However, pure technical approaches cannot provide adequate protection from a knowledge perspective (Olander, Hurmelinna-Laukkanen, & Vanhala, 2014). Even if there is no focus on knowledge protection in the literature on digital innovation, research on knowledge protection can be found in different domains. Building on this observation, we investigate KP from different research domains with the goal to reflect this research in the light of the changes caused by the digital transformation, leading to the research question:

What are the challenges for knowledge protection in the era of digital transformation?

To address this research question, the paper presents a structured literature review and introduces findings from five base research domains. Propositions for a research agenda to further the understanding of the capabilities needed for KP for digital transformation are presented.

2. Related work

Digital transformation is changing work environments, both in offices and on shop floors (Lasi, Fettke, Kemper, Feld, & Hoffmann, 2014). Decentralisation, virtualisation, and networks intensify the way employees interact

CONTACT Ilona Ilvonen ilona.ilvonen@tut.fi

and work together (Brettel, Friederichsen, Keller, & Rosenberg, 2014). In particular, connected products force companies to closely integrate with selected customers and supply chain partners (Chick, Huchzermeier, & Netessine, 2014), which is facilitated by an increased number of virtual communication channels available to exchange knowledge (Pawlowski et al., 2014). However, this increased number of communication channels not only fosters intended knowledge transfers but also reduces control over them (Hamel, Doz, & Prahalad, 1989). This problem is exacerbated by recent developments in the field of social media and mobile technologies that seem to promise to support organisations in their knowledge sharing (Bruck, Motiwalla, & Foerster, 2012), but also create challenges for KP.

Digital transformation also changes the way employees interact with each other (Mazmanian, Orlikowski, & Yates, 2013). Devices can be used regardless of time and location, and boundaries between work and leisure time blur (Wang & Shen, 2011). As a result, employees find it increasingly challenging to distinguish between sharing knowledge important to themselves and important for their jobs/sharing knowledge about themselves and sharing knowledge about their jobs (Väyrynen, Hekkala, & Liias, 2013) or to identify direct vulnerabilities of online knowledge sharing (Jarvenpaa & Majchrzak, 2010). The use of social media challenges KP, since social software bridges private and business life, is highly individual and often lacks quality approval (Von Krogh, 2012).

Knowledge is the most important source of competitive advantage (Grant, 2002) and this holds especially true in times of digital transformation. However, although knowledge is of such importance, organisations struggle with the protection of knowledge due to its close relation to humans and its tacit nature (Thalmann, Manhart, Ceravolo, & Azzini, 2014). In contrast to information security, no widely accepted guidelines exist in the domain of KP.

Due to the specific characteristics of knowledge, existing approaches in information security cannot be directly transferred to knowledge protection (Manhart & Thalmann, 2015). We argue that the intensive cross-organisational knowledge sharing caused by the digital transformation requires appropriate ways to protect the critical knowledge on the one hand and to intensively participate in knowledge-sharing activities intended to create digital innovations on the other hand.

3. Procedure

This paper presents a structured literature review (Webster, & Watson, 2002). The review was undertaken in three stages: (1) identifying the relevant literature, (2) structuring the review, and (3) contributing to theory.

In stage (1), a full review of top journals of the base domains was conducted (see Appendix 1, for list of journals and keywords). The review was conducted in fall 2016, and focused on articles published after the year 2005. The selection of journals was based on their rankings, if available (Azar & Brock, 2008; Crossan & Apaydin, 2010; Serenko & Bontis, 2013). Appendix 1 shows the domains and journals covered. To identify potentially relevant papers, the building-blocks approach (Rowley & Slack, 2004) was applied, transforming relevant concepts into search statements and extending the statements using synonyms and related terms. More precisely, the authors selected articles according to their match to (a) three key search terms we combined with protection: knowledge, idea, innovation and (b) six search terms we combined with knowledge: security, spillover, risk, leakage, exploitation, and appropriation. Close to four hundred (or either, 372) articles matching these key terms were then distributed amongst the authors for abstract scanning. Each author was responsible for at least one set of papers that focused on a core domain and included a set of papers (e.g., knowledge management literature, strategic management literature, risk management literature). The authors rejected articles that did not have their core foci on KP, represented by the search term. The authors came up with a sum of 69 articles that they consider as having their core focus on KP. This set included relevant literature identified by backward and forward searches of highly cited and relevant articles (Webster, & Watson, 2002). Articles that focus on knowledge *about* protection instead of protection *of* knowledge were excluded from the in-depth analysis.

In stage (2), a concept matrix (Webster, & Watson, 2002) that identifies the main elements of analysis was developed. The starting elements of the concept matrix were adapted from the work of Seidel, Müller-Wienbergen, and Becker (2010), such as "domain", "research methods", or "role of IS". One column each was defined to cover how the papers consider the knowledge artefact (What is knowledge?), risk of losing knowledge (Why is KP necessary?), and its scope (What are applied KP management approaches?). The concept matrix was iteratively refined and extended (Webster, & Watson, 2002) with each new insight gained from the literature. The matrix was a highly valuable tool to identify patterns within and across the base domains. More precisely, multiple discussions amongst the authors using the matrix as discussion artefact strengthened the authors' consensus about the core theme of the paper. The authors recognised that digital transformation, which was covered in several papers, has crucial impact on the three dimensions described above: knowledge artefact, risk, and KP management approaches. The constant discussion allowed the authors to propose research avenues to counter risks and lack of management approaches for KP in the era of digital transformation.

In stage (3), the authors develop a research agenda considering organisations' needs of KP in the era of

digital transformation. Taking the research agenda into account, the authors develop a KP definition that (a) considers new challenges towards KP imposed by digital transformation and (b) incorporates the specifics of the identified base domains. The authors consider the research agenda and the resulting KP definition as the essence of their synthesis of their findings across the base domains aligned with their research question.

4. Results

The results of the review are structured according the supply chain risk and risk management framework (Norrman & Lindroth, 2004). The framework focuses on main areas relevant for managing risks in interconnected business processes. We selected the framework as the growing interconnection between businesses is one of the major effects caused by digitisation which is highly relevant for managing knowledge. As we discussed in the background, this trend makes the balancing of knowledge sharing and protection in inter-organisational collaborations more challenging. Hence, organisations have to manage the resulting risks properly. Based on this insight, we structured our results according the three dimensions: (1) unit of analysis, describing the knowledge that needs to be protected, (2) risks that threaten the unit of analysis, and (3) the management approaches suited to address the threats.

4.1. Unit of analysis

The review focuses on both tacit and explicit knowledge (Nonaka & Takeuchi, 1995) because the terms are widely used in Knowledge Management (KM). KM literature that addresses KP focuses on both tacit and explicit knowledge (e.g., Jennex & Durcikova, 2014). The tacit component is considered to be employees obtaining organisational knowledge (Gonzalez, 2016) and KM literature recognises knowledge as a source of competitive advantage (Randeree, 2006; Sarigianni, Thalmann, & Manhart, 2015), where tacit knowledge is considered as key to sustain competitiveness (Ilvonen, Jussila, & Kärkkäinen, 2015). Also the general management domain has articles that emphasise the tacit, social, or procedural nature of knowledge (e.g., Loebbecke, Van Fenema, & Powell, 2016; Marabelli & Newell, 2012; Trkman & Desouza, 2012).

In KM literature explicit knowledge is discussed as documents stored in KM systems (Joe, Yoong, & Patel, 2013), and as innovations or IPR (Phelps & Jennex, 2015). The documentability and patentability of knowledge is frequently discussed in strategic management (Ceccagnoli, 2009; Di Stefano, King, & Verona, 2014; Reitzig & Puranam, 2009) as well as innovation management (Thomä & Bizer, 2013, Shu, Wang, Gao, & Liu, 2015), information security (Zeng, Yu, & Lin, 2011), and general management (Hannah, 2005). Of interest is knowledge that is important for generating innovation (Amara, Landry, & Traoré, 2008; Jean, Sinkovics, & Hiebaum, 2014).

Strategic management literature focuses on the importance and value of knowledge. Knowledge should be protected and held tightly within the firm to ensure value creation and capturing (Alnuaimi & George, 2015) and that the organisation benefits most from the knowledge (Moschini & Yerokhin, 2008). In innovation management, there are views that explicit or tacit knowledge alone is not necessarily valuable, but the complex combination of them both is what has the potential to give companies competitive advantage (Ritala & Hurmelinna-Laukkanen, 2013).

The summary in Table 1 shows that the common distinction between tacit and explicit knowledge does not necessarily address the needs of KP efforts. While tacitness and explicitness help in identifying where the knowledge resides and how it is transferred and shared, the importance of the knowledge is the factor that most contributes to the need to protect it.

4.2. Risks

In KM literature, the main risk for knowledge is loss: either to externals or through lack of internal retention. Loss to externals can happen by employee turnover, or diluting boundaries of the organisations through networking IT like social software or cloud storage (e.g., Phelps & Jennex, 2015), which is a key feature brought on by digital transformation. Knowledge can also be threatened through ineffective or missing transfer practices that ensure knowledge is not bound to a single resource like a system or an employee (e.g., Krylova et al., 2016).

The main risks discussed in strategic management and innovation management are unwanted knowledge spillovers (e.g., Baldwin & Henkel, 2015; Castellaneta, Conti, & Kacperczyk, 2016; Roy & Sivakumar, 2011; Zanarone, Lo, & Madsen, 2016) and appropriation of the knowledge by competitors (Di Stefano et al., 2014;

Table 1. Knowledge as a unit of analysis.

Concept	Definition	Domains
Tacit knowledge	Knowledge that is embedded in the minds of individual persons. Maybe difficult to express in words, based on experiences	Knowledge management, strategic management, innovation management, general management
Explicit knowledge	Knowledge that is expressed in a documented format, and in writing. Easy to store and transfer	All domains
Important (patentable) knowledge	Knowledge that has particular competitive value to an organisation and that can be used in innovations	Strategic management, innovation management, general management

Giarratana & Mariani, 2014; Moschini & Yerokhin, 2008; Shu et al., 2015). The negative impact of both risks is that they might reduce the revenue of the company. The knowledge leakage perspective focuses mostly on knowledge which can be secured only to a very limited extent by IPR or other formal protection measures (Di Stefano et al., 2014; Thomä & Bizer, 2013). The appropriation perspective focuses mostly on knowledge which is patentable, with the goal to optimally design the IPR regime (Reitzig & Puranam, 2009). Timing of knowledge disclosure is essential to ensure that an organisation can exploit the knowledge best. The general management literature examines the same risks, but more from the point of view of individual employees: if knowledge is bound to procedures and social interactions, then the individual employees play a big role in how and when it is disclosed or spilled (Jarvenpaa & Majchrzak, 2016; Loebbecke et al., 2016; Marabelli & Newell, 2012).

In information security management, risks to knowledge are considered through the lens of confidentiality, integrity, and availability (Ilvonen et al., 2015). The leakage perspective focuses mostly on confidentiality mechanisms (Ahmad, Bosua, & Scheepers, 2014) where risks are either unintentional spillover or intentional theft of knowledge (Tan, Wong, & Chung, 2016). The risks presented above are summarised in Table 2. Combining these risk perspectives will result in a more comprehensive approach to KP.

4.3. Management approaches

KM literature discusses numerous protection measures like awareness trainings (Levy, 2011), ambiguity through different access rights (Randeree, 2006), or risk management frameworks (Ilvonen et al., 2015; Thalmann et al., 2014) and knowledge retention strategies (Coffey & Eskridge, 2008), which all focus on applying measures at the organisational level. KM assumes that protection activities are under the control of the organisation, although the measures are informal in nature. Also, other domains acknowledge informal protection mechanisms such as social norms and values (Di Stefano et al., 2014), organisational design (Baldwin & Henkel, 2015), secrecy and lead time (Amara et al., 2008; Harabi, 1995), or design complexity (Amara et al., 2008).

Innovation management and strategic management literature focus more on the formal protection mechanisms such as optimal design of an IPR regime in the light of an appropriation perspective. While the knowledge is bound to be public in some form or another, formal protection mechanisms are needed to stop competitors from directly utilising it (Arundel, 2001; Hertzfeld, Link, & Vonortas, 2006). At the inter-organisational level, there is a trade-off between measures facilitating sharing and measures enforcing protection to maximise the outcome of collaborative innovation projects (Bogers, 2011). At the organisational level, patents (Amara et al., 2008; Encaoua, Guellec, & Martinez, 2006; Harabi, 1995; Kaiser, 2002), trademarks (Amara et al., 2008; Kaiser, 2002), and copyrights (Amara et al., 2008) are used as protection mechanisms.

The management approach to protecting sensitive knowledge in the information security literature focuses on the design, selection, and implementation of technical and organisational measures that protect communication channels and/or data storages and prevent unwanted behaviour (Tan et al., 2016). General management literature acknowledges the need for formal and technical protection measures (Loebbecke et al., 2016; Trkman & Desouza, 2012). However, the challenges in regard to tacit knowledge are also evident (Trkman & Desouza, 2012). Capabilities to protect knowledge in different contexts are tied to individuals (Jarvenpaa & Majchrzak, 2016) although they are also needed at the organisational level (Loebbecke et al., 2016).

All domains contrast the effort needed to implement and to enforce the protection mechanism with the expected benefits. Also, cases in which less protection can be valuable are discussed (Alnuaimi & George, 2015; Moschini & Yerokhin, 2008). In Table 3, the different managerial approaches to KP are presented. The formal and informal protection mechanisms are very different in nature, and in many organisations, the challenge is to find a good mix of measures that works for the organisation.

5. Research agenda

Based on the results of our literature review, we discuss the finding in the light of digital innovation. As a key results, we propose five research avenues for research on knowledge protection in the context of digital transformation.

Table 2. Knowledge risks.

Risk / threat	Description	Domains
Knowledge loss	Knowledge is no longer available to the organisation, and it maybe available to the competitors.	Knowledge management
Spillover	Knowledge that is important for competitive position ends up in the hands of competitors	Strategic management, innovation management, general management
Theft of knowledge	Knowledge (or information) is actively stolen from the organisation repositories	Information security management
Misappropriation	Failure to prevent competitors from utilising patentable knowledge by failing to follow correct IPR regime	Innovation management, strategic management

Table 3. Knowledge protection management mechanisms.

Managerial approach	Description	Domains
Formal methods		
Legal	Patents, trademarks, copyright, licencing, confidentiality agreements	Strategic management, innovation management, general management, information security management
Technical	Technical constraints for access, protection of communication channels, systems, and storage	Information security management
Informal methods		
Secrecy	Restricting the sharing of knowledge to a limited number of people	Knowledge management, innovation management
Complexity, ambiguity	Complexity of design, spreading knowledge to large amount of actors so that only a few have access to the big picture of the (product) design process	Knowledge management, innovation management, strategic management
Education	Awareness training of employees, educating employees about the rules of conduct and the importance of knowledge	Knowledge management, information security management, innovation management
Social norms	Agreement and commitment between members of different organisations to behave in certain way to protect their knowledge	Strategic management, general management

5.1. P1: Clarifying which manifestations of knowledge are to be protected

The concept of knowledge as a unit of analysis takes many forms, and focusing on tacit and explicit knowledge is a long-standing tradition in KM. Digital transformation, in integrating and digitalising different communication channels, blurs the line between different manifestations of knowledge, which is a challenge. For example, communication increasingly takes place in digital environments: informal communication that has traditionally been in tacit form (speech) become explicit in various forms, for example, chat discussion threads. The focus of KP should be on the various manifestations of knowledge that have an important impact on the competitiveness of the organisation.

The very key in digital transformation is that it changes the technological environments in which people work and interact, and increases the role of technological platforms (Yoo et al., 2012). However, the technology platforms themselves cannot solve the problem of knowledge identification. The tensions between the organisational level, where KP is managed, the individual level, where knowledge is held, and the technology platform, where that knowledge is being communicated, need to be found and addressed. This needs to be done on the organisational level, but in the end, the people involved in knowledge exchanges are the ones that make the choice to share or not to share knowledge. Thus, their role in identifying important knowledge is essential. Although there is literature that acknowledges this issue, more research on how it can be achieved in a more systematic way, is needed.

5.2. P2: Redefining the knowledge boundaries of an organisation

Digital transformation leads to increased complexity of innovation processes, geographical dispersion of innovation and a distribution across multiple organisations (Von Hippel, 2009), which challenges the KP efforts. Innovations are created in a collaborative manner, involving business partners as well as customers and the required heterogeneity of knowledge and knowledge sources demands inter-organisational collaboration (Yoo et al., 2012). This means taking communication of important knowledge away of the core of the organisation to the edges, which imposes knowledge risks (Loebbecke et al., 2016). So far, KP-related research has mainly focused on environments that are simple and adhere to a traditional setting of two organisations engaging in clearly defined collaboration in a defined time frame and with a clear objective. However, complex networks of organisations, alternative work models, and the blurring lines between organisations are widely neglected (Pahnke, Mcdonald, Wang, & Hallen, 2015).

Besides the short-term exploitation of innovations, knowledge collaborations have long-term effects. Hence, organisations should think about how they can maintain their competitive advantage, for example, by requiring non-disclosure agreements or social media awareness training programmes. Research in this regard focuses on collaborations in dyadic relationships, neglecting more complex collaboration structures (Pahnke et al., 2015). The complexity and intensity of the collaboration needed in a digitised work environment require more coordination amongst the collaborators. Also, research should go beyond simple dyadic relationships in innovation collaborations (Barrett, Oborn, Orlikowski, & Yates, 2012) and propose controls for better coordination on the network level.

Addressing the risks listed in Table 2 requires an understanding of what knowledge is important for a certain activity, and where it resides. Protection measures applicable in network arrangements become necessary. Research on informal measures like social norms and psychological contracts seems promising for future research in this area.

5.3. P3: Management support: knowledge protection toolbox

Digital transformation and changes in the use of technology changes the value creation models, structures and financial emphasises of an organisation (Yoo et al., 2012). Companies do not longer only communicate and function within their geographically bounded business units but need to manage, collaborate, and act on an international and distributed level (Brennan et al., 2015). As a consequence, the complexity of interactions rises and tool support is needed. Although we do not claim to solve the entire challenge with knowledge protection tools, we argue that a toolbox of knowledge protection mechanisms is one key element in addressing changes caused by digital transformation in organisations.

Table 3 lists multiple managerial approaches to KP that are studied across the domains. A combination of formal and informal protection mechanisms seems most promising for successful KP. However, the selection of an appropriate mix of protection mechanisms is difficult. This is why a broad approach to KP is needed that acknowledges the different manifestations of knowledge and the complex operating environment of an organisation.

Table 2 lists risks the important knowledge of an organisation faces. An interesting question is how well the identified risks and the current protection mechanisms correspond to each other. Studies have mainly concentrated on one narrow aspect of KP at a time, and thus there is no research on how well the available management tools answer to KP needs of organisations. More research on what would constitute an appropriate KP toolbox for different types of organisations would complement the existing literature.

5.4. P4: Process guidance: Decision support for individuals

The transforming digital environment poses challenges for individuals who navigate the complex organisational landscape, collaborate with each other, and share knowledge to achieve their work goals (Pawlowski et al., 2014). As individual employees have to work faster and more collaboratively in digital innovation environments (Dery, Sebastian, & van der Meulen, 2017), knowledge protection becomes more and more important in such network settings (Loebbecke et al., 2016). However, the mechanisms that are discussed in KP literature are of managerial character and abstract in nature (Manhart & Thalmann, 2015). Furthermore, due to the increasing organisational complexity decision-making needs to be shifted away from a central instance towards decentralised instances (Stock & Seliger, 2016). Hence, individuals need decision support embedded in their daily work processes. Individuals are faced with numerous work task decisions everyday where they consider knowledge-sharing consequences for themselves and for their organisation.

KP research on the individual level is scarce. The design of technological tools that can support knowledge-sharing decisions using, for example, visualisations or other data-driven approaches would be a good complement to the organisational level approaches.

5.5. P5: Managing the balance between sharing and protection

Globally operating industrial organisations develop strategies to simultaneously share and protect knowledge in order to participate in the global innovation system (Spencer, 2003). Literature clearly states that neither a pure protection nor a pure sharing strategy is the most successful one, rather a well-balanced mixture (Loebbecke et al., 2016). However, finding this balance between adequate sharing and KP is a challenge that organisations need to solve (Loebbecke et al., 2016). The next step is to understand when and where a piece of knowledge embedded in organisational capabilities generates value or superior performance (Eisenhardt, Furr, & Bingham, 2010). How this understanding can be achieved, and how individuals make value decisions considering knowledge should therefore be further studied in various domains. Research streams on organisational capabilities (Wilden, Devinney, & Dowling, 2016) should address the question how organisations can balance sharing and protecting to generate superior performance.

A promising avenue of study would be to combine the perspectives of organisational-level formal protection mechanisms, and individual-level informal mechanisms, and see how well they complement each other. Promising research relating the individual-level to organisational performance has been done under the term micro-foundations (Argote & Ren, 2012; Teece, 2007). This stream should extend research towards balancing sharing and protecting on the individual level and, hence, provide answers on how balancing can drive organisational performance on the individual level.

6. Conclusions

This paper finds answers to the research question, "What are the challenges for knowledge protection in the era of digital transformation?" by relating the characteristics of digital transformation and the elements of knowledge risk management together. The paper presents a research agenda that would work towards solving the challenges identified. The paper shows that KP has received different degrees of attention from various research domains. These perspectives on KP are integrated and reflected from the point of view of digital transformation. KP is a cross-disciplinary research field, where knowledge and insights from different research domains can contribute to better understanding of what kind of knowledge organisations need to protect. Also in practice,

protection strategy and measures need to be designed by a team of experts from different domains, and the presented research agenda can also serve practitioners as a guideline for developing KP initiatives.

Based on the literature review, we define KP as a set of capabilities comprising and enforcing technical, organisational, and legal mechanisms to protect knowledge that is of strategic or operational importance to an organisation. KP focuses on both (1) external threats of leakage and exploitation by unauthorised parties and (2) internal threats of unavailability and loss, and the challenges discussed above relate to both, internal and external threats. What makes these threats more difficult to address, is the digital transformation that constantly changes the operating landscape of the organisations, and drives the development of complex networks the organisations participate in. Organisations need technical and managerial protection measures to meet the requirements of distributed and scalable infrastructures of digital transformation. The intensified collaboration on new digital platforms demands more research beyond studies on dyadic organisational relationships.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

Pro2Future and the Know-Center are funded within the Austrian COMET Program –"Competence Centers for Excellent Technologies" – under the auspices of the Austrian Federal Ministry of Transport, Innovation and Technology, the Austrian Federal Ministry of Science, Research and Economy and of the Provinces of Upper Austria and Styria. COMET is managed by the Austrian Research Promotion Agency FFG. This work has also been funded by the Finnish foundation for economic education.

References

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security, 42*, 27–39.

Alnuaimi, T., & George, G. (2015). Appropriability and the retrieval of knowledge after spillovers. *Strategic Management Journal, 37*(7), 1263–1279.

Amara, N., Landry, R., & Traoré, N. (2008). Managing the protection of innovations in knowledge-intensive business services. *Research Policy, 37*, 1530–1547.

Argote, L., & Ren, Y. (2012). Transactive memory systems: A microfoundation of dynamic capabilities. *Journal of Management Studies, 49*, 1375–1382.

Arundel, A. (2001). The relative effectiveness of patents and secrecy for appropriation. *Research Policy, 30*, 611–624.

Azar, O. H., & Brock, D. M. (2008). A citation-based ranking of strategic management journals. *Journal of Economics & Management Strategy, 17*, 781–802.

Baldwin, C. Y., & Henkel, J. (2015). Modularity and intellectual property protection. *Strategic Management Journal, 36*, 1637–1655.

Barrett, M., Oborn, E., Orlikowski, W. J., & Yates, J. (2012). Reconfiguring boundary relations: Robotic innovations in pharmacy work. *Organization Science, 23*, 1448–1466.

Bhamu, Jaiprakash, & Sangwan, Kuldip Singh (2014). Lean manufacturing: Literature review and research issues. *International Journal of Operations & Production Management, 34*(7), 876–940.

Bogers, M. (2011). The open innovation paradox: Knowledge sharing and protection in R&D collaborations. *European Journal of Innovation Management, 14*, 93–117.

Brennan, L., Ferdows, K., Godsell, J., Golini, R., Keegan, R., Kinkel, S., … Taylor, M. (2015). Manufacturing in the world: Where next? *International Journal of Operations & Production Management, 35*(9), 1253–1274.

Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014). How virtualization, decentralization and network building change the manufacturing landscape: An Industry 4.0 Perspective. *International Journal of Mechanical, Industrial Science and Engineering, 8*(1), 37–44.

Bruck, P. A., Motiwalla, L., & Foerster, F. (2012). *Mobile learning with Micro-content: A framework and evaluation*. 25th Bled eConference. Bled: AIS.

Castellaneta, F., Conti, R., & Kacperczyk, A. (2016). Money secrets: How does trade secret legal protection affect firm market value? Evidence from the uniform trade secret act. *Strategic Management Journal, 38*(4), 834–853.

Ceccagnoli, M. (2009). Appropriability, preemption, and firm performance. *Strategic Management Journal, 30*, 81–98.

Chick, S. E., Huchzermeier, A., & Netessine, S. (2014). Europe's solution factories. *Harvard business review, 92*, 111–115.

Coffey, J. W., & Eskridge, T. (2008). Case studies of knowledge modeling for knowledge preservation and sharing in the US nuclear power industry. *Journal of Information & Knowledge Management, 7*, 173–185.

Crossan, M. M., & Apaydin, M. (2010). A multi-dimensional framework of organizational innovation: A systematic review of the literature. *Journal of Management Studies, 47*, 1154–1191.

Dery, K., Sebastian, I. M., & van der Meulen, N. (2017). The digital workplace is key to digital innovation. *MIS Quarterly Executive, 16*(2), 135–152.

Di Stefano, G., King, A. A., & Verona, G. (2014). Kitchen confidential? Norms for the use of transferred knowledge in gourmet cuisine. *Strategic Management Journal, 35*, 1645–1670.

Eisenhardt, K. M., Furr, N. R., & Bingham, C. B. (2010). CROSSROADS-Microfoundations of performance: Balancing efficiency and flexibility in dynamic environments. *Organization Science, 21*, 1263–1273.

Encaoua, D., Guellec, D., & Martinez, C. (2006). Patent systems for encouraging innovation: Lessons from economic analysis. *Research Policy, 35*, 1423–1440.

Giarratana, M. S., & Mariani, M. (2014). The relationship between knowledge sourcing and fear of imitation. *Strategic Management Journal, 35*, 1144–1163.

Gonzalez, R. V. D. (2016). Knowledge Retention in the Service Industry. *International Journal of Knowledge Management (IJKM), 12*, 45–59.

Grant, R. M. (2002). The knowledge-based view of the firm. In C. Choo & N. Bontis (Eds.), *The strategic Management of Intellectual capital and organizational knowledge* (pp. 133–148). Oxford University Press.

Hamel, G., Doz, Y. L., & Prahalad, C. K. (1989). Collaborate with your Competitors and Win. *Harvard Business Review, 67*, 133–139.

Hannah, D. R. (2005). Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets. *Organization Science, 16*, 71–84.

Harabi, N. (1995). Appropriability of technical innovations an empirical analysis. *Research Policy, 24*, 981–992.

Hertzfeld, H. R., Link, A. N., & Vonortas, N. S. (2006). Intellectual property protection mechanisms in research partnerships. *Research Policy, 35*, 825–838.

Ilvonen, I., Jussila, J. J., & Kärkkäinen, H. (2015). Towards a business-driven process model for knowledge security risk management: Making sense of knowledge risks. *International Journal of Knowledge Management (IJKM), 11*, 1–18.

Jarvenpaa, S., & Majchrzak, A. (2010). Research commentary-vigilant interaction in knowledge collaboration: Challenges of online user participation under ambivalence. *Information Systems Research, 21*, 773–784.

Jarvenpaa, S., & Majchrzak, A. (2016). Interactive self-regulatory theory for sharing and protecting in inter-organizational collaborations. *Academy of Management Review, 41*, 9–27.

Jean, R. J., Sinkovics, R. R., & Hiebaum, T. P. (2014). The effects of supplier involvement and knowledge protection on product innovation in customer–supplier relationships: A study of global automotive suppliers in China. *Journal of Product Innovation Management, 31*, 98–113.

Jennex, M., & Durcikova, A. (2014). Integrating IS security with knowledge management: Are we doing enough? *International Journal of Knowledge Management, 10*(2), 1–12.

Joe, C., Yoong, P., & Patel, K. (2013). Knowledge loss when older experts leave knowledge-intensive organisations. *Journal of Knowledge Management, 17*, 913–927.

Kagermann, H., Lukas, W.-D. & Wahlster, W. (2011) *Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution*. VDI Nachrichten, 13, 2011.

Kaiser, U. (2002). Measuring knowledge spillovers in manufacturing and services: An empirical assessment of alternative approaches. *Research Policy, 31*, 125–144.

Krylova, K. O., Krylova, K. O., Vera, D., Vera, D., Crossan, M., & Crossan, M. (2016). Knowledge transfer in knowledge-intensive organizations: The crucial role of improvisation in transferring and protecting knowledge. *Journal of Knowledge Management, 20*(5), 1045–1064

Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. Business & Information. *Systems Engineering, 6*(4), 239–242.

Levy, M. (2011). Knowledge retention: Minimizing organizational business loss. *Journal of Knowledge Management, 15*, 582–600.

Manhart, M., & Thalmann, S. (2015). Protecting organizational knowledge: A structured literature review. *Journal of Knowledge Management, 19*, 190–211.

Marabelli, M., & Newell, S. (2012). Knowledge risks in organizational networks: The practice perspective. *Journal of Strategic Information Systems, 21*, 18–30.

Mazmanian, M., Orlikowski, W. J., & Yates, J. (2013). The autonomy paradox: The implications of mobile email devices for knowledge professionals. *Organization Science, 24*, 1–21.

Moschini, G., & Yerokhin, O. (2008). Patents, research exemption, and the incentive for sequential innovation. *Journal of Economics & Management Strategy, 17*, 379–412.

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company*. New York, NY: Oxford University Press.

Norrman, A., & Lindroth, R. (2004). Categorization of supply chain risk and risk management. In C. Brindley (Ed.), *Supply Chain Risk* (pp. 14–27). Farnham: Ashgate Publishing.

Olander, H., Hurmelinna-Laukkanen, P., & Vanhala, M. (2014). Mission: Possible but sensitive – Knowledge protection mechanisms serving different purposes. *International Journal of Innovation Management, 18*, 1440012.

Pahnke, E., Mcdonald, R., Wang, D., & Hallen, B. (2015). Exposed: Venture capital, competitor ties, and entrepreneurial innovation. *Academy of Management Journal, 58*, 1334–1360.

Pawlowski, J. M., Bick, M., Peinl, R., Thalmann, S., Maier, R., Hetmank, D.-W.-I. L., … Pirkkalainen, H. (2014). Social knowledge environments. *Business & Information Systems Engineering, 6*, 81–88.

Phelps, M., & Jennex, M. E. (2015). Ownership of collaborative works in the cloud. *International Journal of Knowledge Management (IJKM), 11*, 35–51.

Randeree, E. (2006). Knowledge management: Securing the future. *Journal of knowledge management, 10*, 145–156.

Reitzig, M., & Puranam, P. (2009). Value appropriation as an organizational capability: The case of IP protection through patents. *Strategic Management Journal, 30*, 765–789.

Ritala, P., & Hurmelinna-Laukkanen, P. (2013). Incremental and radical innovation in coopetition – The role of absorptive capacity and appropriability. *Journal of Product Innovation Management, 30*, 154–169.

Rowley, J., & Slack, F. (2004). Conducting a literature review. *Management Research News, 27*, 31–39.

Roy, S., & Sivakumar, K. (2011). Managing intellectual property in global outsourcing for innovation generation. *Journal of Product Innovation Management, 28*(1), 48–62.

Sarigianni, C., Thalmann, S., & Manhart, M. (2015). Knowledge risks of social media in the financial industry. *International Journal of Knowledge Management, 11*, 19–34.

Seidel, S., Müller-Wienbergen, F., & Becker, J. (2010). The concept of creativity in the information systems discipline: Past, present, and prospects. *Communications of the Association for Information Systems, 27*, 14–15.

Serenko, A., & Bontis, N. (2013). Global ranking of knowledge management and intellectual capital academic journals: 2013 Update. *Journal of Knowledge Management, 17*, 307–326.

Sherehiy, Bohdana, & Karwowski, Waldemar (2014). The relationship between work organization and workforce agility in small manufacturing enterprises. *International Journal of Industrial Ergonomics, 44*(3), 466–473.

Shu, C., Wang, Q., Gao, S., & Liu, C. (2015). Firm patenting, innovations, and government institutional support as a double-edged sword. *Journal of Product Innovation Management, 32*, 290–305.

Spath, D., Ganschar, O., Gerlach, S., Hämmerle, M., Krause, T., & Schlund, S. (2013). *Produktionsarbeit der Zukunft-Industrie 4.0*. Stuttgart: Fraunhofer Verlag.

Spencer, J. W. (2003). Firms' knowledge-sharing strategies in the global innovation system: Empirical evidence from the flat panel display industry. *Strategic Management Journal, 24*, 217–233.

Stock, T., & Seliger, G. (2016). Opportunities of sustainable manufacturing in industry 4.0. *Procedia CIRP, 40*, 36–541.

Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and knowledge leakage in supply chain. *Information Systems Frontiers, 18*(3), 621–638.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*, 1319–1350.

Thalmann, S., Manhart, M., Ceravolo, P., & Azzini, A. (2014). An integrated risk management framework: Measuring the success of organizational knowledge protection. *International Journal of Knowledge Management, 10*(2), 28–42.

Thomä, J., & Bizer, K. (2013). To protect or not to protect? Modes of appropriability in the small enterprise sector. *Research Policy, 42*(1), 35–49.

Trkman, P., & Desouza, K. C. (2012). Knowledge risks in organizational networks: An exploratory Framework. *Journal of Strategic Information Systems, 21*, 1–17.

Väyrynen, K., Hekkala, R., & Liias, T. (2013). Knowledge protection challenges of social media encountered by organizations. *Journal of Organizational Computing and Electronic Commerce, 23*, 34–55.

Von Hippel, E. (2009). Democratizing innovation: The evolving phenomenon of user innovation. *International Journal of Innovation Science, 1*, 29–40.

Von Krogh, G. (2012). How does social software change knowledge management? Toward a strategic research agenda. *The Journal of Strategic Information Systems, 21*, 154–164.

Wang, M., & Shen, R. (2011). Message design for mobile learning: Learning theories, human cognition and design principles. *British Journal of Educational Technology, 43*, 561–575.

Webster, J., & Watson, R.T. (2002) Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly* (pp. xiii–xxiii).

Wilden, R., Devinney, T. M., & Dowling, G. R. (2016). The architecture of dynamic capability research identifying the building blocks of a configurational approach. *The Academy of Management Annals, 10*, 997–1076.

Yoo, Y., Boland, R. J., Jr, Lyytinen, K., & Majchrzak, A. (2012). Organizing for innovation in the digitized world. *Organization Science, 23*, 1398–1408.

Zanarone, G., Lo, D., & Madsen, T. L. (2016). The double-edged effect of knowledge acquisition: How contracts safeguard pre-existing resources. *Strategic Management Journal, 37*(10), 2104–2120.

Zeng, W., Yu, H., & Lin, C.-Y. (2011). *Multimedia security technologies for digital rights management*. Amsterdam: Academic Press.

Appendix 1. Search domains, journals and number of articles scanned

Domain	Strategic Management	Knowledge Management	Information Security	Innovation Management	General Management	Sr Scholars Basket of 8	
Journals	*Strategic Management Journal, Journal of Economics & Management Strategy, Long Range Planning, Strategic Organisation, Strategic Entrepreneurship Journal*	*Journal of Knowledge Management, International Journal of Knowledge Management, Knowledge Management Research & Practice, Journal of Information & Knowledge Management*	*Computers and Security, Information and Computer Security, ACM Transactions on Information and System Security, IEEE Transactions on Information Forensics and Security*	*Research Policy, Journal of Product Innovation Management, Regional Studies, Technovation*	*Management Science, Organisation Science, Administrative Science Quarterly, Academy of Management Journal, Academy of Management Review*	*European Journal of Information Management, Information Systems Journal, Information Systems Research, Journal of AIS, Journal of Information Technology, Journal of MIS, Journal of Strategic Information Systems, MIS Quarterly*	
Keywords							Sum
Knowledge Protection	10	6	2	10	6	12	46
Intellectual Property Protection	11	2	7	14	6	6	46
Know How Protection	2	0	0	0	1	1	4
Idea Protection	1	0	0	1	0	1	3
Innovation Protection	7	0	2	9	1	4	23
Knowledge Security	3	3	1	4	2	21	34
Knowledge Spillover	8	0	2	15	5	6	36
Knowledge Risk	23	10	2	19	3	42	99
Knowledge Leakage	4	5	1	1	1	1	13
Knowledge exploitation/ appropriation	16	1	0	40	2	9	68
Abstract scan	85	27	17	113	27	103	372
Full paper review	16	18	6	8	8	13	69