Creating Sustainable Knowledge Systems: Towards a Risk and Threat Assessment Framework

Murray E. Jennex
San Diego State University

Alexandra Durcikova
University of Oklahoma

Knowledge is the most important asset to a company. It is key to strategic innovation and alignment, and must be made sustainable. To keep knowledge sustainable, it must be safeguarded. However, knowledge management (KM) and knowledge systems are different than traditional information systems with different threats and operational requirements. Information security professionals recognize that risk assessment is the cornerstone to information security. We build on this perspective and propose that risk assessment techniques need to be applied to KM. We discuss risk assessment frameworks and build on a KM/knowledge system risk assessment framework with a KM/knowledge system specific threat assessment.

Keywords: knowledge management, risk assessment, threat assessment

INTRODUCTION

We live in a knowledge economy and society where knowledge is used to produce economic and societal benefit. Gloet and Samson (2020) show that competitive advantage is driven by strategic innovation which in turn is driven by knowledge and KM/knowledge systems. The effective and sustainable management of knowledge resources is imperative to organizations that would like to leverage their knowledge assets for greater competitive advantage and improved performance (Smith, et al., 2010). A key issue of interest to this paper is how do you keep knowledge relevant and the KM/knowledge system sustainable such that the organizations continues to generate the benefits of knowledge use? We suggest that protecting the organization's knowledge from the unique threats that can cause the knowledge to be lost, disclosed, made obsolete, misused or used inappropriately, etc. is the key to making KM/knowledge systems sustainable and benefit producing.

The key issue to sustaining KM/knowledge systems is to understand the unique security risks and threats that could cause these systems to degrade. Whitman and Mattord (2019) quote Sun Tzu Wu on the importance of knowing yourself and knowing your enemy as a key to success in battle, or in designing and implementing information systems security. To accomplish the knowing of yourself and your enemy the corner stone of information systems/cyber security is the process of risk assessment. Risk assessment is used to know yourself by identifying data/information/knowledge/technology assets (henceforth simplified to knowledge assets), assigning a value and priority to the knowledge assed, and identifying

the threats that could cause the knowledge asset to be disclosed, modified, or destroyed. Risk assessment helps organizations know the enemy by determining the threats that could attack the organization's knowledge assets. Risk management then uses these inputs to analyze the overall risk to the knowledge asset and determine the controls to be used to mitigate or remove the risk. All major security frameworks include a risk assessment and management process. For the United States the Nationals Institute of Standards and Technology (NIST) provides the risk management framework (RMF) as described in special publication, SP 800-12 rev 1 (2012), An Introduction to Information Security, SP 800-37 rev 2 (2018), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, and SP 800-53 rev 5 (2017) (draft), Security and Privacy Controls for Information Systems and Organizations. A similar process is outlined by the International Standards Organization (ISO). ISO27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements and ISO7005:2018, Information technology -- Security techniques -- Information security risk management.

While these are fine risk frameworks, they are generic in nature and are not tailored specifically to knowledge management, KM, or knowledge systems. We do not claim that KM/knowledge systems are so unique as to require their own risk frameworks or that the above-mentioned risk frameworks are not useful. We are stating that KM/knowledge system managers will do a better job of risk assessment/ management of KM/knowledge systems if they have tailored guidance, specifically in two areas: threat assessment and risk analysis. Why do we think KM/knowledge systems need special guidance? We argue that the purpose of KM and knowledge systems are to support the sharing and application of knowledge by supporting decision making, throughout the organization to achieve organizational goals, strategic innovation, and competitive advantage. Since the purpose is to share knowledge the tenets of information security are inherently at odds with KM/knowledge systems. It is our opinion that information security is still needed but should be applied in ways that recognize the uniqueness of knowledge sharing and decision processes. Jennex and Durcikova (2014) examined the integration of KM and security and found that security was not integrated into the KM job functions. Thus, the purpose of this paper is to provide specific guidance and requirements for KM/knowledge systems threat assessments and risk analysis. In addition, this paper is focusing on the risk of knowledge loss from a human source (we will only focus on this asset). Knowledge loss risk is defined as the expected impact to the organization resulting from the loss of a particular expert or knowledge worker. This is consistent with the NIST SP 800-37 rev 2, (2018) risk definition so the NIST risk algorithm will be used as the basis for determining knowledge loss risk.

This paper first starts with an overview of risk and risk management, threats and threat assessment, risk frameworks, and knowledge management (KM)/knowledge systems risk frameworks. This is followed by a KM/knowledge systems specific threat assessment that is based on literature review followed by a KM/knowledge systems risk framework proposal also based on literature review that incorporates the KM/knowledge systems specific risks. The literature review includes analysis of previous case studies and other research.

BACKGROUND: RISK AND RISK ASSESSMENT

The NIST SP 800-37r2 (2018) describes risk as the net negative impact of the exercise of a vulnerability; considering both the probability and the impact of occurrence. Risk is traditionally represented by the following formula:

R(risk) = p(probability of occurrence) x C(consequence of occurrence either represented by some value or by a loss function)

Risk management is the process of identifying risk, assessing risk and taking steps to manage risk by reducing risks to an acceptable level (NIST SP 800-37 rev 2, (2018)). Acceptable level of risk depends on the managers of an organization. For example, for organization A, a loss of $30,000 might be huge risk while for an organization B this amount represents a minor risk. Additionally, Smith et al. (2001) and

Aubert et al. (1998) argue that information systems managers and researchers traditionally define risk in terms of negative consequences describing risk as the possibility of loss or damage and the possibility of suffering harm or loss.

An alternative view by Billington (1997) points out that, when examined closely, "risk" can actually lead to both positive and/or negative consequences. In any particular initiative, he notes, the risks involved could represent different meaning to an organization. Billington (1997) proposes three dimensions of a risk:

1. A hazard that must be minimized or eliminated;
2. An uncertainty about which path should be taken and which must be studied to reduce the variance between anticipated outcomes and actual results; and
3. An opportunity for growth or improvement, which must be assessed to determine how much innovation, initiative and entrepreneurship should be exercised.

Viewing risk as something more than a hazard is highly applicable to risk management in KM (Jennex and Durcikova, 2014). Although KM risks can lead to negative results, they can also represent significant opportunities for savings or business development. For example, losing a subject matter expert who has 30+ years of experience in a particular aspect of a business (due to retirement) might be perceived as a huge risk that can potentially cause a large financial loss. However, this same scenario might open doors to hiring new talent that costs less money (e.g., lower starting salary) that can bring new ways of addressing business problems.

Uncertainty associated with knowledge use, be it due to rapidly changing technology and storage media, to misuse or new and unexpected uses of knowledge or to the basic understanding of the captured knowledge, is one of the biggest challenges a KM manager faces. This is the reason why this paper is focusing on the risk of knowledge loss from a human source, for example, loss of knowledge from particular expert or knowledge worker.

A final note on the risk formula shown above is that it recognizes that determining exact probabilities and values for consequence is difficult. An alternative to probabilities and consequence values proposed by several sources is to utilize relative ranges or scores for the probability and consequence value. When this is done, probability becomes likelihood and consequence value becomes consequence. This paper, as discussed later, uses this approach of utilizing scores and thus uses likelihood and consequence. This also allows a group of employees to agree on a likelihood and score rather than for one employee to come up with these values. While the scoring approach does not provide specific risk values it does provide a relative ranking of risks that provides risk management staff with a prioritized list of risks that allows for the most severe risks to be addressed first.

Practical risk management bases risk assessment on the identification and assessment of threats to the organization's assets. NIST SP 800-30r1 (2012) defines a threat as any event or circumstance that can adversely affect organizational operations or knowledge assets. A threat source is an adversarial or non-adversarial source that could cause damage to a system by exploiting a vulnerability. A vulnerability is defined as a security weakness in the program or an asset's controls. Threat sources can be internal or external to the organization. In addition, threats can be intentional or accidental. Finally, a threat source can be a natural or man-made disaster. Threat assessment is about identifying threat sources and the vulnerabilities they can use to exploit/damage a knowledge asset. The purpose of threat assessments is to identify specific threat sources and the vulnerabilities that would be used to attack the organization's knowledge assets. The Risk Formula and assessment uses the results of threat assessment by using the consequence/damage caused by a threat utilizing a vulnerability and the probability/likelihood of this occurring to determine risk values/ratings.

To assist organizations in performing threat assessments generic threats are proposed. One such set is from Whitman and Mattord (2019) who propose 12 threat categories:

- Compromises to intellectual property
- Deviations in quality of service
- Forces of nature
- Espionage or trespass

- Human error or failure
- Information extortion
- Sabotage or vandalism
- Software attacks
- Technical hardware failures or errors
- Technical software failures or errors
- Technical obsolescence
- Theft

The purpose of this list of threats is to provide organizations a guide as to where to look for knowledge security threats. It should be noted that this threat list includes technical threats, behavioral threats and legal threats. It is our purpose to propose such a list for KM/knowledge systems. Since KM/knowledge systems primarily focus on providing knowledge users with knowledge for making decisions our paper focuses on risks/threats associated with the capture, storage, retrieval, and use of knowledge. Our list considers technical, behavioral, and legal threats, and are generated by analyzing how KM/knowledge systems can be misused or abused with the specifics of how this is done being presented in the next section.

RISK ASSESSMENT FRAMEWORKS

The purpose of any risk assessment framework is to establish rules for what is assessed, who are the main actors that need to be involved in this assessment, creates terminology for assessment, criteria for quantifying, qualifying, and comparing degrees of risk, and provides a way to document all of this (Mackey, 2019). The main purpose of a risk assessment framework is to establish an objective measurement of risk so that an organization can understand risk and take appropriate action to mitigate it and bring it to an acceptable level.

Information technology professionals can choose from several risk assessment frameworks (Mackey, 2019): OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Assessment) and NIST risk assessment framework, ISACA's Risk IT (part of COBIT), and ISO 27005:2008 (part of the ISO 27000 series). While these frameworks differ some in their prescription on how to do risk assessment, they all have the following five parts in common (Fitzgerald et al., 2017):

- Development of risk measurement criteria
- Asset inventory
- Threat identification
- Risk score calculation
- Documentation of existing controls
- Identification of improvements to controls

Researchers and practitioners have been working on risk assessment frameworks for the area of KM/Knowledge Systems. These are discussed below.

KM/KNOWLEDGE SYSTEMS RISK ASSESSMENT FRAMEWORKS

Three KM knowledge system risk assessments have been proposed. Thalman et al. (2014), Padyab et al. (2014), and Ilvonen et al. (2015) have all proposed KM/knowledge systems risk assessment frameworks that are differentiated by the KM/knowledge contexts upon which they focus. Thalman et al. (2014) focused on the knowledge sharing process context as the basis for assessing risk and then mapped the traditional information security framework into a KM security framework. Padyab et al. (2014) also focused on the knowledge sharing process context and then used communication genres and the OCTAVE Allegro risk framework to create a KM/knowledge system risk framework. Ilvonen et al. (2015) expanded the context of their KM risk framework to include the knowledge processes of knowledge creation, knowledge sharing, and management of knowledge; and then fused it with the NIST SP 800-37r2 risk management framework to create their knowledge security risk management framework

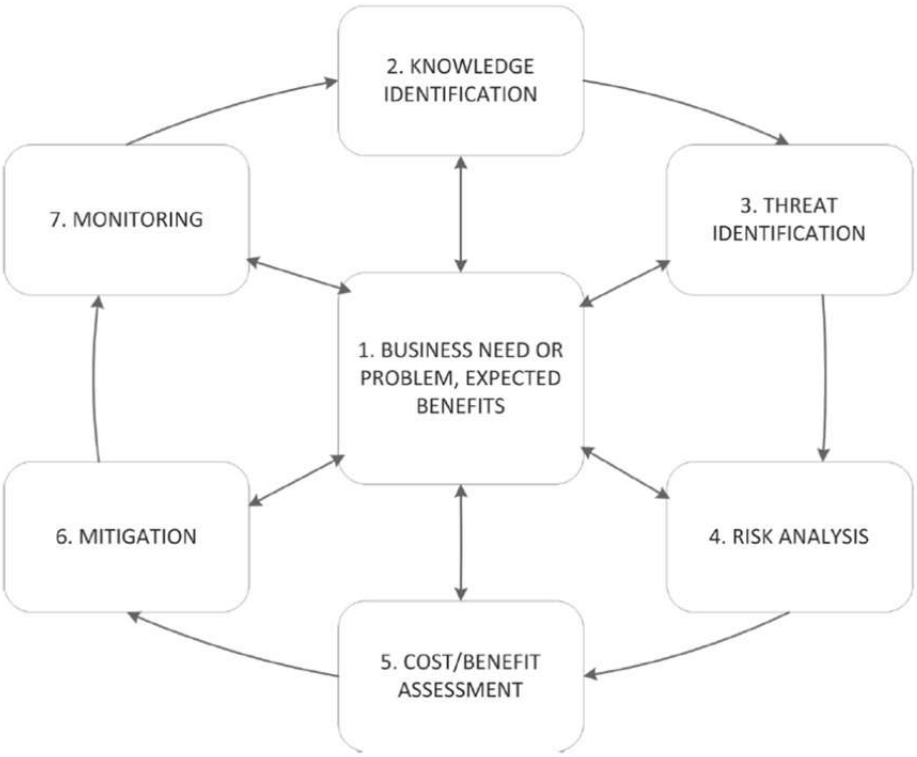
(see Figure 1). Ilvonen et al (2015, p.13) define knowledge security "as the managerial process of organizations to identify threats toward important knowledge and secure the knowledge against those threats." In the first stage, the business case of the intended KM initiative or change to the initiative, and a description of what kind of benefits are sought by the initiative/change are described by an organization. This is followed by knowledge identification that can be done in three ways:

1. examination of different locations, uses, topics and destinations of knowledge.
2. genre-based approach where different actors and their way of communication with other actors are identified.
3. examination of the knowledge systems where the knowledge resides.

Threat identification happens along the lines of external threats and accidental or deliberate internal threats to the knowledge assets. In the risk analysis step, the identified threats are individually analyzed to recognize what kind of risks they may cause and how significant these risks are. Cost/benefit analysis deals with the costs of implementing controls that mitigate these risks. Step six, risk controls that need to be implemented are identified along with a plan for implementing them. Finally, monitoring which is a crucial part of Ilvonen et al (2015) framework provides the organization with situational awareness of the risk environment the organization is facing.

We use the Knowledge Security Risk Management Framework as it uses a fuller context of how knowledge processes fit the overall KM/knowledge systems business processes and is thus a more complete KM/knowledge system risk management framework.

FIGURE 4
KNOWLEDGE SECURITY RISK MANAGEMENT FRAMEWORK (ILVONEN ET AL (2015)



KM/KNOWLEDGE SYSTEM THREAT ASSESSMENT

Figure 1 includes threat identification as a part of the risk management framework. To create a generic set of threats for KM/knowledge systems we start with the basic KM/knowledge system processes of knowledge creation, sharing, and management and then add a further concern from Walsh and Ungson (1991) who identified three contexts in which Organizational Memory (OM) could be misused:

- Automatic retrieval of knowledge may lead to a routine decision response when a non-routine decision response is warranted;
- The controlled retrieval of knowledge may lead to a non-routine decision response when a routine decision response was appropriate;
- A controlled retrieval of knowledge may be appropriately activated in an attempt to elicit a non-routine decision response, but it may be implemented poorly.

Misuse of the OM occurs when organizational members self-servingly select knowledge to support positions that serve their political needs rather than the organization's (Walsh and Ungson, 1991). Also, misuse of OM is a unique threat to knowledge use. These three misuse risks are also applicable to KM/Knowledge Systems as OM is a fundamental and integral part of KM/Knowledge Systems (Jennex et al., 2018) and as such, OM threats are KM/Knowledge Systems threats.

We applied Spears (2012) use of misuse cases to analyze the OM misuses identified by Walsh and Ungson (1991) to generate the following six KM/Knowledge systems specific threats. Each of the KM/Knowledge systems specific threat was then analyzed using three possible threat vectors (sources of attacks): technology, behavioral, and regulatory based attacks applied to KM/knowledge system processes (creation, storing, sharing, and management) to generate the below full set of KM/knowledge system specific generic threats. Studies that illustrate or support the identified threats are also listed.

Failure to Identify and Capture Critical Knowledge in the Knowledge Creation Process

This has been observed in several studies: Jennex and Zyngier (2007) observed that large organizations that relied on humans to identify and capture critical knowledge often failed to sometimes identify and many more times capture critical knowledge. Jennex (2008, 2008a) observed the failure to identify and capture critical knowledge in an engineering organization when identification of what to capture and to what detail to capture knowledge was left to organizational members with different levels of understanding the knowledge. In some cases, very experienced members failed to see the importance of capturing sufficient detail to make the knowledge useful to less experienced members; and having less experienced members mis-identify critical knowledge because they did not know what was important. Finally, Jennex (2010, 2013) observed that many organizations failed to retain captured critical knowledge after a change in storage formats. Particularly observed was the loss of knowledge as organization migrated to newer versions or different word processing packages or to a newer storage media (example is moving from floppy disk drives to laser disks to USB drives). What was observed was that organizations failed to transfer all the knowledge from one format or package to the newer format or package resulting in a loss of knowledge that many times was found out later to be critical knowledge. Aggestam, et al. (2014) found that having a knowledge content process was essential for ensuring that critical knowledge was identified, and captured.

Technical Threats

Technical threats are from using automated tools to identify and capture critical knowledge with the vulnerabilities typically being in the ontologies and taxonomies used to guide the automated tools not accurately reflecting the domains being analyzed. Additional threats are from technical obsolescence leading to the loss of knowledge as the organization migrates to newer technologies.

Behavioral Threats

Behavioral threats are from personnel intentionally or accidently classifying critical knowledge and not recognizing critical knowledge, not capturing enough detail with the knowledge, or failing to capture

it when it is recognized. An additional threat is of personnel resisting organizational changes designed to ensure critical knowledge is identified and captured.

Regulatory Threats

Regulatory/legal threats are from not recognizing a regulatory/legal need to capture mandated knowledge.

Not Having KM Knowledge Creation, Capture, and Use Aligned with Organizational Strategy

Zyngier and Burstein (2012) found that the organizational benefits of KM and knowledge use are not always realized and that management structures of KM governance and KM strategy are necessary. Jennex (2020) found that organizations that had a KM strategy were more apt to realize benefits and proposed KM strategy, knowledge content process, and KM governance as constructs included as necessary for KM success. Aggestam, et al. (2014) found that having a knowledge content process was essential for ensuring the right knowledge for achieving knowledge benefits was captured and stored. Koloniari, et al. (2014) studied KM critical success factors and found KM strategy to be very important and defined the construct as the degree to which the organization links knowledge with its competitive strategy.

Technical Threats

Technical threats are from implementing automated knowledge capture tools without ensuring the rules guiding knowledge capture reflect organizational strategy or that these tools are not maintained as organizational strategy evolves.

Behavioral Threats

Behavioral threats are from personnel intentionally or accidently not aligning KM and knowledge capture, storage, and use with organizational strategy. An additional threat is from personnel resisting organizational changes that would ensure KM alignment with organizational strategy.

Regulatory Threats

Regulatory/legal threats are from not recognizing a regulatory/legal need to capture mandated knowledge.

Disclosing Critical Knowledge to Unauthorized Recipients in the Knowledge Sharing Processes

Jennex (2008, 2008a) observed engineers sharing knowledge based on their own opinions of what was appropriate to share rather than following organizational guidelines. Jennex and Zyngier, (2007) observed members of organizations sharing critical knowledge with unauthorized individuals because the organization had failed to classify disclosure categories of knowledge. Jennex (2010) observed for crises and disasters the issue of what knowledge should be posted on social media and what knowledge should be trusted off of social media. Walters (2012) documents the use of USB drives to capture knowledge from users who plug the drives into their system. This threat has become even more dangerous in the coronavirus pandemic of 2020 as for a period of time most organizations had to shut down in office operations and have workers work remotely from home where the organization has less control over the disclosure of knowledge. We have noted that there was much research on how to improve virtual collaboration during the pandemic, but little on how to do it safely. This was especially the case with one of the main tools used to enable remote working and collaboration, Zoom. Zoom bombing became a major concern early in the crisis as it was easy for uninvited guests to join zoom meetings (Warren, 2020).

Technical Threats

Technical threats are from exploitation of communication vulnerabilities common to all communication systems and is focused on communication processes specific to KM/knowledge systems

(as an example consider an organization using SharePoint as the system for communicating knowledge with the communication vulnerabilities being common to both knowledge and non-knowledge applications, or Zoom being used for remote work and collaboration but not protecting the integrity of meeting members). Additional threats are from storage media by not properly securing access to cloud storage and/or server storage.

Behavioral Threats

Behavioral threats are from intentionally or accidentally failing to maintain access control lists for authorizing approved personnel to access knowledge, posting knowledge to inappropriate forums, not following disclosure processes, not encrypting knowledge in motion, falling victim to social engineering attacks and either disclosing knowledge to unauthorized individuals or allowing malware onto their systems that are collecting and transmitting knowledge to unauthorized individuals.

Regulatory Threats

Regulatory/legal threats are from intentionally or accidentally not complying with disclosure laws such as those dealing with personally identifiable information or patient health knowledge. Other threats are from the intentional theft of intellectual property and from the unintentional loss of intellectual property based on the cloud or collaborative medium on which it was stored or shared (Phelps and Jennex, 2015).

Losing Critical Knowledge by Not Capturing It from Critical Human Sources

Jennex (2014) and Jennex and Durcikova (2013) observed this as an issue and proposed a process for rating knowledge sources and their likelihood of departing as well as providing a score to indicate the time criticality of taking action.

Technical Threats

Technical threats are from technical obsolescence leading to the loss of knowledge as the organization migrates to newer technologies or from failure of the obsolete devices. Additional threats come from the loss of repository devices and not having an appropriate backup process in place. A final threat is from ransom ware encrypting critical knowledge repositories and not being able to recover them through backups or by paying the ransom.

Behavioral Threats

Behavioral threats are from intentionally or accidentally not identifying critical human knowledge repositories and taking actions to capture and store the critical knowledge (this threat is typically not capturing knowledge from retiring personnel but also can occur by not capturing knowledge from personnel departing an organization for reasons other than retirement).

Regulatory Threats

Regulatory/legal threats are from intentionally or accidentally not complying with required knowledge capture (an example of this was Nuclear Regulatory Commission requirements on nuclear stations to capture critical knowledge from employees prior to large scale work force layoffs).

Losing Critical Knowledge by Not Storing It on Nonvolatile Media or by Not Migrating Knowledge with Changing Storage Standards or by Not Meeting Legal Standards for Storing Critical Knowledge

Jennex, (2010, 2013) has reported large scale losses of critical knowledge due to storage media not surviving as long as expected. Losses include NASA losing plans for moon craft, nuclear plants losing documents stored on older storages media such as 8, 5 ¼, and 3 ½ inch floppy disks, microfiche, paper, etc. Additional knowledge losses were observed as organizations migrate to newer softwares or newer versions of software, and changing data storage formats.

Technical Threats

Technical threats are from the failure of storage media, hardware, and/or software. Additional threats are from technical obsolescence leading to the loss of knowledge as the organization migrates to newer technologies or from failure of the obsolete devices. Other threats come from the loss of repository devices and not having an appropriate backup process in place or an installed tracking system. A final threat is from ransom ware encrypting critical knowledge repositories and not being able to recover them through backups or by not paying the ransom.

Behavioral Threats

Behavioral threats are from intentionally or accidentally not following technology procurement processes, selecting providers without checking their technology, not planning for obsolescence, not testing technologies before applying them or while using them, and/or artificially obsoleting technologies before age requires it.

Regulatory Threats

Regulatory/legal threats are from liability issues associated with not following sanctioned or committed storage standards (such as those standards from NIST and ISO)

Giving Bad Advice by Not Using Appropriate Knowledge or by Using Inappropriate Knowledge

This risk is illustrated by high profile errors in decision making such as Jennex (2012) report on the conviction of the scientific panel who told citizens there was little likelihood of a seismic event prior to the 2009 L'Aquila, Italy earthquake that killed 309. Vaughn (2004) and Boin and Fishbacher-Smith, (2011) discuss the decision making process that ignored safety concerns from the contractors prior to the 1986 Challenger space shuttle disaster. Perrow (1981) discusses the human errors made that led to the severity of the 1979 Three Mile Island nuclear disaster. Tackett et al. (2004) discusses how audit failures and bad analysis at Enron, Worldcom, and other companies that led to the creation and implementation of the Sarbanes Oxley Act that makes c-level corporate officers responsible for the data, analysis, and recommendations presented in their public disclosures. For regular decision making, Bloodgood (2015) found content management to be critical to preventing: organizational knowledge base becoming less useful as organization may continue applying knowledge that is sub-optimal, out of date, or inappropriate for the new situations; the presence of the outdated knowledge may lead the organization to focus on misguided learning or may fail to learn sufficiently.

Technical Threats

Technical threats are from search tools not finding relevant knowledge, improperly categorizing or prioritizing knowledge, not using integration tools allowing relevant knowledge to not be incorporated into search results, and/or using visualization technologies that influence decision makers to the wrong option.

Behavioral Threats

Behavioral threats are from decision makers using incomplete knowledge, and/or inappropriately applying knowledge to unsuitable decision contexts. Additional threats are from organizations not managing content to keep it current and relevant.

Regulatory Threats

Regulatory/legal threats are from decision makers not utilizing due care or due diligence in assessing knowledge and focusing on politically correct or desired advice. Another threat is from not giving advice or giving advice based on limiting liability rather than stating the advice suggested by the knowledge system.

The severity and likelihood of the above threats are based on two factors. The first factor is attack surface. Attack surface for knowledge systems is the sum of all the points where the above threats can

have an effect. The more knowledge, knowledge users and creators, and knowledge processes an organization has the larger the attack surface. The larger the attack surface the greater the likelihood of the threat occurring. The second factor is the impact of the threat on the organization. Impact is determined by looking at the three dimensions of impact: confidentiality, availability, and integrity. The first step in determining the severity of each of the dimensions on the organization, usually through financial impact (revenue, income, replacement cost), reputational impact, legal impact, safety impact, and impact on organizational success. The second step is to determine how severe each threat impacts each of the dimensions. The consequence of the threat is the sum of these impacts.

Each of the above knowledge threats is described as threat components of technical, behavioral, and legal threats. Breaking the threat into these three threat components assists risk managers in determining attack surface and consequence to the organization. To further assist in determining consequence to the organization, Table 1 maps the above 6 knowledge system threats to their impact on confidentiality, integrity, and availability.

TABLE 1
IMPACT OF THREATS ON CONFIDENTIALITY, INTEGRITY, AVAILABILITY

Threat	Confidentiality	Integrity	Availability
Failure to identify and capture critical knowledge in the knowledge creation process	Low/moderate impact as not identifying critical knowledge can lead to it being disclosed	High impact as not having critical knowledge impacts total integrity of that which is stored	High impact as knowledge not captured cannot be available
KM knowledge creation, capture, and use not aligned with organizational strategy			High impact as not having knowledge aligned with organizational strategy makes in unavailable for use
Disclosing critical knowledge to unauthorized recipients in the knowledge sharing processes	High impact based on strategic impact		
Losing critical knowledge by not capturing it from critical human sources	Moderate as human sources may not know they possess critical knowledge and inadvertently disclose it	High impact as lost knowledge affects total integrity of that which is stored	High impact as lost knowledge is not available
Losing critical knowledge by not storing it on nonvolatile media, not migrating knowledge with changing storage standards. not meeting legal standards for storing critical knowledge	Moderate impact as not meeting storage standards could lead to inadvertent disclosure	High impact as lost knowledge affects total integrity of that which is stored	High impact as lost knowledge is not available
Giving bad advice by not using appropriate knowledge or by using inappropriate knowledge		High impact as decision do not reflect what the decision made using the correct knowledge would be	

NEWLY PROPOSED RISK ASSESSMENT FRAMEWORK FOR KNOWLEDGE MANAGEMENT/KNOWLEDGE SYSTEMS

Ilvonen, et al. (2015) proposed a risk management framework for KM/knowledge systems as shown in Figure 1. We propose an enhancement to this framework that offers a high-level KM risk assessment. Jennex (2014) proposed a risk management process for assessing knowledge loss risk with departing personnel. This was a form based process that walked managers through the risk assessment process. Jennex and Durcikova (2013) utilized this form based risk assessment process to assess the knowledge loss risk with graduate students and found the form based process to be a good process. Based on this experience and further literature review provided on both general risk assessment frameworks and also on KM/Knowledge systems framework, we are proposing the following template for knowledge risk assessment (Fitzgerald et al., 2017). The definitions and possible values of each category are provided in Table 1. This table provides a worksheet for guiding and documenting a KM risk assessment. The risk management process is driven by an inventory of knowledge assets. In general terms, an asset can be people, knowledge, processes, systems, or applications. We propose that the assets for KM/knowledge systems are the knowledge from a particular expert or knowledge worker, processes that create, capture, and use knowledge, and any hardware that is unique to capturing, storing, and disseminating knowledge.

When creating the risk assessment for KM/knowledge systems, one would identify all the different knowledge assets and then identify every threat to each knowledge asset, following the categories in Table 1. In general, the impact areas are one or several from the following: financial (expenses and revenues), productivity (business operations), reputation (perceptions of customers and society), legal (fines and litigations), and safety (safety or employees, customers, environment). It is important to note that these areas are not exhaustive, and that an organization may remove or add areas. The importance of each area must be ranked as low/medium/high while keeping in mind that not all areas are high impact. Next, the impact of each threat on the asset must be in each are must be evaluated. For example, business leaders must evaluate whether a loss of 1% or 5% of revenue is considered to have a low/medium/high impact. Scenarios must be written out so that anybody who reads them can follow the logic or the arguments. The next step is to calculate the risk score that is the product of the ranking and impact. This score is meaningless by itself, but very useful when we compare the impact of different threats on different assets.

An organization can pick from one to four risk control strategies: accept (taking no action against the treat), mitigate, share, or defer. The only threats that should be accepted would have a very low risk score. Most of the threats will be mitigated (control(s) would be implemented) or shared (e.g., insurance would be purchased). Examples of control could be codification of knowledge that would happen on a regular basis either by automatic agents or by apprentices who shadow a knowledge worker.

In congruence with the traditional risk assessment frameworks, the highest risk score threats must be processed as first and appropriate controls must be initiated.

CONTRIBUTION TO RESEARCH AND PRACTICE

Creation, storage, and reuse of knowledge is a source of both short term and long term competitive advantage for organization (Alavi and Leidner, 2001). Thus, organizations need to pay more attention to safeguard this important asset.

Our contribution to research builds on existing generic risk assessment frameworks and knowledge management frameworks to create an easy way to calculate the risk score for each threat to an asset. Specifically, we contribute to research in the following ways: First, we provide an in-depth discussion of threats to knowledge assets. Nor the generic framework or the knowledge management security risk assessment provide such a guideline. Second, we provide a concrete approach on how to calculate the risk score by identifying possible impact areas, rank the importance of these impact areas, easily score the impact. While the risk score by itself is not that useful, it becomes very useful when compared to risk scores of other threat/asset pairs.

Our contribution to practice is twofold: First, we provide a business-driven approach to identifying and categorizing (low/medium/high) the impact of a threat for five business area – financial, productivity, reputation, legal, and safety. The impact needs to be discussed with managers as they are the best informed what is a high/low impact. Second, our approach offers a use of a template that can be followed by both technical and non-technical staff and thus allows for a faster documentation of assets/threats, their potential impact, and risk mitigation techniques.

TABLE 2
RISK ASSESSMENT FOR KNOWLEDGE MANAGEMENT WORKSHEET

Asset	The object of the risk assessment - knowledge from particular expert or knowledge worker		
Asset Owner/Custodian	Owners have the authority to accept risk. Custodian of the asset are responsible for implementing and maintaining controls that protect the asset.		
Asset Importance	Low/Medium/High		
Threat	Any way an asset could be compromised that would have an impact on a business. See examples in the Knowledge Management/Knowledge System Threat Assessment section of this paper.		
Threat Description	____ Failure to identify and capture critical knowledge in the knowledge creation process. ____ Disclosing critical knowledge to unauthorized recipients in the knowledge sharing processes _____ Losing critical knowledge by not capturing it from critical human sources. _____ Losing critical knowledge by not storing it on nonvolatile media or by not migrating knowledge with changing storage standards _____ Giving bad advice by not using appropriate knowledge.		
Likelihood	Low (1)/ Medium (2)/ High (3)		
Impact on	____ Confidentiality of knowledge _____Integrity of knowledge ____ Availability of knowledge		
Impact Area	**Ranking**	**Impact**	**Score**
Financial	Low (1)/Medium (2)/High (3)	Low (1)/Medium (2)/High (3)	
Productivity	Low (1)/Medium (2)/High (3)	Low (1)/Medium (2)/High (3)	
Reputation	Low (1)/Medium (2)/High (3)	Low (1)/Medium (2)/High (3)	
Legal	Low (1)/Medium (2)/High (3)	Low (1)/Medium (2)/High (3)	
Safety	Low (1)/Medium (2)/High (3)	Low (1)/Medium (2)/High (3)	
		Risk Score (Likelihood x Impact Score)	

Adequacy of Existing Controls	Low/Medium/High
Risk Control Strategy	___ Accept ___ Mitigate ___ Share ____Defer
Risk Mitigation Controls	Description
Control 1	
Control 2	

CONCLUSION

Creating sustainable knowledge and KM/knowledge systems and strategic innovation is not easy. It is more than just building the system and gathering knowledge, you also need to understand and manage the threats that could cause the knowledge to degrade in value, strategic innovation to falter, and the KM/knowledge system to become ineffective. This paper builds on previous generic risk assessment frameworks and the Knowledge Security Risk Assessment Framework (Ilvonen, et al., 2015) to create the risk assessment for knowledge management. This addition to the framework contributes to the current research and practice, by providing a KM/knowledge system specific threat analysis and a template that can be followed to not only capture the knowledge asset, but also to capture the potential threat, it's likelihood, impact, risk score in an easy to understand fashion that streamlines the whole process. Previous research that discussed risk in KM did not provide such a step-by-step approach that is repeatable in any organizations.

Future research will apply the framework in case studies, preferably in organizations that have previously performed risk assessments so that the results from that risk assessment and the risk assessment performed using our proposed threat analysis and risk form can be compared.

ACKNOWLEDGEMENT

This paper was previously presented at the 54th Hawaii International Conference on Systems Sciences. This version expands on that paper with comments received during its presentation.

REFERENCES

Aggestam, L., Durst, S., & Persson, A. (2014). Critical success factors in capturing knowledge for retention in IT-supported repositories. *Information*, 5(4), 558-569.

Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, pp. 107-136.

Aubert, B., Patry, M., & Rivard, S. (1998). Assessing the Risk of IT Outsourcing. *Proceedings of the 31st Hawaii International Conference on Systems Sciences. IEEE Publishing*, pp. 685 – 693.

Billington, J. (1997, March). A Few Things Every Manager Ought to Know About Risk. *Harvard Management Update*, 2(3), 1-12.

Bloodgood, J. M. (2015). The Negative Performance Implications of Industry Dynamism on Organizational Knowledge. *International Journal of Knowledge Management (IJKM)*, 11(1), 52-65.

Boin, A., & Fishbacher-Smith, D. (2011). The importance of failure theories in assessing crisis management: The Columbia space shuttle disaster revisited. *Policy and Society*, 30(2), 77-87.

FitzGerald, J., Dennis, A., & Durcikova, A. (2017). *Business Data Communications and Networking* (13th Edition). Wiley.

Gloet, M., & Samson, D. (2020). Creating Value Through Knowledge Management and Systematic Innovation Capability. In *Knowledge Management, Innovation, and Entrepreneurship in a Changing World* (pp. 1-30). IGI Global.

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(4), 1-18.

ISO 27001:2013. (reviewed 2019). *Information technology -- Security techniques -- Information security management systems – Requirements*. International Standards Organization.

ISO/IEC 27005:2018. (n.d.). *Information technology -- Security techniques -- Information security risk management*. International Standards Organization

Jennex, M. E. (2020). Towards Understanding and Implementing Knowledge Management Strategy. In M. Jennex (Ed.), *Current Issues and Trends in Knowledge Management, Discovery, and Transfer* (pp. 103-125). Hershey, PA: IGI Global. doi:10.4018/978-1-7998-2189-2.ch005

Jennex, M.E. (2008). Impacts from Using Knowledge: A Longitudinal Study From A Nuclear Power Plant. *International Journal of Knowledge Management*, 4(1), 51-64.

Jennex, M.E. (2008a). Exploring System Use as a Measure of Knowledge Management Success. *Journal of Organizational and End User Computing*, 20(1), 50-63.

Jennex, M.E. (2010). *"Preface: Why Knowledge Management?" "Ubiquitous Developments in Knowledge Management: Integrations and Trends*." Edited by Murray E. Jennex. Information Science Reference, Hershey, PA, xviii-xxix.

Jennex, M.E. (2010). Implementing Social Media in Crisis Response Using Knowledge Management. *International Journal of Information Systems for Crisis Response and Management*, 2(4), 20-32.

Jennex, M.E. (2013). Knowledge Management: The Risk of Forgetting. *iKNOW, the magazine for Knowledge Workers*, 3(1), 4-7.

Jennex, M.E. (2014). A Proposed Method for Assessing Knowledge Loss Risk with Departing Personnel. *VINE: The Journal of Information and Knowledge Management Systems*, 44(2), 185-209.

Jennex, M.E., & Durcikova, A. (2013, January). *Assessing Knowledge Loss Risk*. 46th Hawaii International Conference on System Sciences, HICSS46, IEEE Computer Society.

Jennex, M.E., & Durcikova, A. (2014). Integrating KM and Security: Are We Doing Enough? *International Journal of Knowledge Management*, 10(2), 1-12.

Jennex, M.E., & Zyngier, S. (2007). Security as a Contributor to Knowledge Management Success. *Information Systems Frontiers: A Journal of Research and Innovation*, 9(5), 493-504.

Jennex, M.E., (2012). Risk and Reward in Crisis Response. *The International Journal of Information Systems for Crisis Response and Management*, 4(3), i-iii.

Jennex, M.E., Dittes, S., Smolnik, S., Croasdell, D., & King, D. (2018). Knowledge, Innovation, and Entrepreneurial Systems at HICSS. *Communications of the Association for Information Systems*, 43(39). DOI: 10.17705/1CAIS.04339, Retrieved from https://aisel.aisnet.org/cais/vol43/iss1/39

Koloniari, M., Vraimaki, E., Fassoulis, K., Zenelaj, I., & Kourniotis, X. S. (2014*). A study of KM critical success factors in Greek academic libraries*.

Mackey, R., (2019). *Choosing the right information security risk assessment framework*. Techtarget.com, Retrieved June 4, 2019, from https://searchsecurity.techtarget.com/magazineContent/Information-security-risk-assessment-frameworks

NIST SP 800-12 rev 1. (2017). *An Introduction to Information Security*. National Institute of Standards and Technology. Retrieved June 8, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

NIST SP 800-30 rev 1. (2012). *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology. Retrieved June 8, 2019, from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

NIST SP 800-37 rev 2. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. National Institute of

Standards and Technology. Retrieved June 8, 2019, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
NIST SP 800-53 rev 5 (Draft). (2017). *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology. Retrieved June 8, 2019, from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft.
Padyab, A. M., Päivärinta, T., & Harnesk, D. (2014). Genre-Based Approach to Assessing Information and Knowledge Security Risks. *International Journal of Knowledge Management*, 10(2), 13-27.
Perrow, C. (1981). Normal accident at three mile island. *Society*, 18(5), 17-26.
Phelps, M., & Jennex, M.E., (2015). Ownership of Collaborative Works in the Cloud. *International Journal of Knowledge Management*, 11(4), 35-51.
Smith, H.A., McKeen, J.D., & Staples, D.S. (2001). Risk Management in Information Systems: Problems and Potentials. *Communications of AIS*, 7(Article 13).
Smith, T.A., Mills, A.M., & Dion, P., (2010). Linking Business Strategy and Knowledge Management Capabilities for Organizational Effectiveness. *International Journal of Knowledge Management*, 6(3), 22-43.
Spears, J. (2012). Conceptualizing Data Security Threats and Countermeasures in the E-Discovery Process with Misuse Cases. *AMCIS 2012 Proceedings*, Paper 17. Retrieved from http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/17
Tackett, J., Wolf, F., & Claypool, G. (2004). Sarbanes-Oxley and audit failure: A critical examination. *Managerial Auditing Journal*, 19(3), 340-350.
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 (IJKM)*, 10(2), 28-42.
Vaughan, D. (2004). Theorizing disaster: Analogy, historical ethnography, and the Challenger accident. *Ethnography*, 5(3), 315-347.
Walsh, J. P., & Ungson, G. R. (1991). Organizational Memory. *Academy of Management Review*, 16(1), 57-91.
Walters, P. (2012). *The risks of using portable devices*. Carnegie Mellon University. Produced for US-CERT, a government organization. Retrieved from http://www. us-cert. gov.
Warren, T. (2020). *Zoom faces a privacy and security backlash as it surges in popularity*. The Verge. Retrieved April 1, 2020, from https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response
Whitman, M.E., & Mattord, H. J. (2019). *Management of Information Security* (6th edition). Course Technology, Boston, MA.
Zyngier, S., & Burstein, F. (2012). Knowledge management governance: the road to continuous benefits realization. *Journal of Information Technology*, 27(2), 140-155.