Supporting Cyber Resilience with Semantic Wiki

Riku Nykänen
University of Jyväskylä
P.O. Box 35 (Agora)
FIN-40014 University of Jyväskylä, Finland
+358 50 384 3733
riku.t.nykanen@student.jyu.fi

Tommi Kärkkäinen
University of Jyväskylä
P.O. Box 35 (Agora)
FIN-40014 University of Jyväskylä, Finland
+358 40 567 7854
tommi.karkkainen@jyu.fi

ABSTRACT
Cyber resilient organizations, their functions and computing infrastructures, should be tolerant towards rapid and unexpected changes in the environment. Information security is an organization-wide common mission; whose success strongly depends on efficient knowledge sharing. For this purpose, semantic wikis have proved their strength as a flexible collaboration and knowledge sharing platforms. However, there has not been notable academic research on how semantic wikis could be used as information security management platform in organizations for improved cyber resilience. In this paper, we propose to use semantic wiki as an agile information security management platform. More precisely, the wiki contents are based on the structured model of the NIST Special Publication 800-53 information security control catalogue that is extended in the research with the additional properties that support the information security management and especially the security control implementation. We present common uses cases to manage the information security in organizations and how the use cases can be implemented using the semantic wiki platform. As organizations seek cyber resilience, where focus is in the availability of cyber-related assets and services, we extend the control selection with option to focus on availability. The results of the study show that a semantic wiki based information security management and collaboration platform can provide a cost-efficient solution for improved cyber resilience, especially for small and medium sized organizations that struggle to develop information security with the limited resources.

CCS Concepts
• Security and privacy→Systems security, Human and societal aspects of security and privacy

Keywords
Cyber resilience, Risk management; Information security management; Semantic wiki.

OpenSym '16, August 17-19, 2016, Berlin, Germany
 ISBN 978-1-4503-4451-7/16/08$15.00
DOI: http://dx.doi.org/10.1145/2957792.2957803

1. INTRODUCTION
The free Oxford dictionary defines “resilience” as ”the capacity to recover quickly from difficulties; toughness”. Such property has become essential for both organizations and computing systems in Digital Era, because the overall functionality supported by the IT infrastructure should be resilient, i.e., tolerant towards rapid and unexpected changes (shocks, disturbances) in the operative environment [2, 14]. The paradigm of resilience, with multiple perspectives and different conceptualizations, for reliable business management was reviewed in [3], where it was pointed out that resilient business operations should tackle both threats and opportunities of the environment. General resilience taxonomy was proposed in [23], which consisted of four dimensions: i) type of shock or perturbation, ii) target system, iii) type of concern, and iv) type of recovery. As will be shown below, very similar conceptualization underlines information security management processes through recognizing and documenting threats on assets with proper control actions to deal with the risks. Concerning the computing infrastructure, resilience of general self-adaptive software systems was advanced in [6], where the concept of resilience was directly linked to the dependability of software systems by requiring trusted delivery of services when facing changes in the system itself or its execution environment. Two metrics to quantify the contribution of a component to the system’s resilience were derived in [9], in order to advance Critical Infrastructure Protection.

Resilience against information security threats has also become more and more important for all kind of organizations. It has been admitted that constant state of flawless security is unreachable as threat landscape evolves continuously [24]. Risk-aware processes focus on the mitigation of the known risks at the design time, but may fail to ensure continuous business operation in the challenging, unexpected conditions [21]. In any case, to manage the information security, organizations need to recognize all valuable assets, identify threats and risks, respond to risks by appropriate controls, and finally monitor the development [24, 31]. Semantic wikis provide excellent platform and infrastructure for the documentation and maintenance of this valuable information.

Even if all organizations share common threats of modern cyber-age, many organizations still struggle to implement even the fundamental security controls [19]. Without proper documentation, organizations may fail to understand their security baseline, which significantly decreases their cyber resilience. Selection of the most important security controls to mitigate security risks is an essential part of the organizations’ risk management process. There exists a range of quantitative methods that support organizations in their security control selection, but these require existence of detailed numeric input data, like risk realization statistics, life-cycle costs of controls and proper asset valuation, in order to provide valid results [29]. However, for small and medium sized organizations (SMEs)

additional resources are usually required to make the necessary organizational data available and to validate it. Hence, especially for SMEs, there is an obvious need for more agile methods to obtain sufficient cyber resilience against both known and emerging threats.

This paper evaluates possibility to use semantic wiki platform as a basis to manage the necessary knowledge on information security to increase the organizational resilience. We propose to use the semantic wiki to provide a platform of existing common information and cyber security information, which can be used as a technical tool for organizations own risk management processes. The proposal consists of initial asset, risk, and security control data provided in the semantic wiki as well as new functions implemented to wiki for common actions performed as part of risk management process. The evaluation focus on analysis that can semantic wiki platform with presented functions be used to overcome common problems of the information security risk management.

2. BACKGROUND

2.1 Information security risk management

The fact that flawless state of information security is unreachable has been widely accepted by the security experts [24]. The most widely used information security management systems, like ISO/IEC 27001 [18], are therefore risk driven and attempt to reach the best possible level of security with available resources.

There exists number of information security ontologies where some focus on the common concepts, like [4] and [11], and others on the specific subdomains of information security, like cloud computing or incident management [1]. Where more comprehensive ontologies require more expertise, which SMEs usually lack, for our novel approach it is essential to start with a simple core ontology that is easy to comprehend and adopt.

Common Criteria (ISO/IEC 1540) is a product security certification standard, which defines widely accepted common model for the key security concepts. The security concepts and their relations as defined in Common Criteria (CC) are described in Figure 1. The same concepts are also included in more extensive ontologies [4, 11].

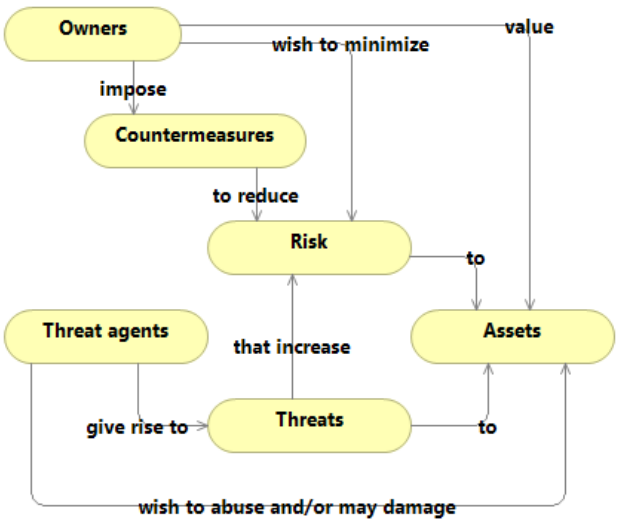

Figure 1 Security concepts and relations by Common Criteria.

In CC, asset is an item, thing or entity that has potential or actual value to an organization (ISO 55000:2014). Control (i.e., countermeasure) is a measure that is modifying risk (ISO/Guide 73:2009). Vulnerability is a weakness of an asset or control that can be exploited by one or more threats (ISO/IEC 27000:2014). Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization (ISO/IEC 27000:2014). Risk is an effect of uncertainty on objectives (ISO/Guide 73:2009). When compared to the resilience taxonomy as proposed in [23] (see Section 1), one can readily identify shocks or perturbations on the target system with threats on assets. Similarly, type of concern and type of recovery in [23] correspond to risks and their countermeasures in CC.

Information security, by the definition, means preservation of confidentiality, integrity and availability (CIA) of information [17]. To preserve all three CIA properties, it is crucial that organizations detect all assets that have an effect to the information security. These are not limited only to physical or information assets, but also organization's processes, culture and other intangible assets should be considered in order to succeed in the asset detection. Information security management system (ISMS) has become the authoritative convention to ensure information security [15]. ISMS defines the organizations security goals, and resources and practices to reach the goals. In addition, it sets how organization monitors and develops its security practices.

Widely used ISO/IEC 27001 ISMS standard applies ISO/IEC 27005 risk management process as part of ISMS implementation [18]. There exists also number of other information security risk management standards and practices like OCTAVE, NIST SP 800-30 and CRAMM. All these share common parts of the risk management process. Table 1 presents typical risk management phases, which have been collected and generalized from multiple specifications by [12].

Table 1. ISRM process phases, tasks and outcomes [12].

Process phase	Typical tasks	Phase outcomes
System characterization	Asset identification	Asset inventory
Threat and vulnerability assessment	Threat and vulnerability identification	List of threats and corresponding vulnerabilities
Risk determination	Likelihood and impact assessment, risk estimation	Risk figures and levels for identified threats
Control identification	Control evaluation	List of recommended controls to mitigate risks
Control evaluation and implementation	Risk treatment; control selection and implementation	List of controls that have reduced risk to acceptable level

Common first task of the risk management process is to know what you have to protect. The knowledge of owned assets, tangible and intangible, are collected to asset inventory. By the definition, asset can be anything that has value for the organization.

The next step in the generalized process by [12] is to identify the vulnerabilities of the assets. Vulnerabilities are accessed by the threats. Hence, we need to identify vulnerabilities and threats that can cause harm to the assets and therefore disrupt organizations operation. As result we should know what to protect (asset

inventory), how it can be harmed (vulnerability inventory), and what can harm it (threat inventory).

After the threat and vulnerability assessment the generalized process by [12] continues with the risk analysis. The risk analysis phase includes assessing threat likelihood and impact of realization of the risk. As the result, we are able to know the risk level and potentially even the damages caused by the realized risks. Risks also can be prioritized by the risk level.

When we are aware which risks have high risk level, the next action is to identify potential controls to mitigate the risks. This is often done using a control catalogue like ISO/IEC 27002 or NIST SP 800-53, which list the common security controls and provide implementation guidance. As the result of control identification, we obtain a list of the potential controls to implement.

The final step of the typical risk management process is to evaluate controls and implement the selected controls. The control selection should take into account already implemented controls, but also costs of the control implementation. Control implementation include development costs (e.g. installation costs), operational costs (e.g. maintenance costs) and response costs (e.g. personnel necessary to operate the countermeasure).

2.2 Challenges of risk management from information security perspective

Comprehensive literature review [13] indicates several challenges in the information security risk management. The encountered common challenges are:

1. To establish asset and control inventory
2. To assign values on assets
3. To predict the risks correctly
4. To avoid overconfidence on the ISMS
5. To share knowledge
6. To balance risk vs. cost trade-offs

The items 1-3 are all related to identification of assets and controls and estimation of values of assets and probabilities of the risks. All these issues are critical for the successful implementation of a quantitative risk analysis method.

Risk analysis methods can generally be divided into two major categories; qualitative and quantitative. Quantitative risk analysis methods rely on derived measures (numbers) to select the best possible risk processing option. Major problem of quantitative methods is lengthy and time-consuming process, which requires detailed information of the asset values and the possible incidents [29]. Qualitative methods are not based on monetary values and mathematics, but merely on the on judgments and perceptions of the evaluated scenario and suitable safeguards for it. Neither of the methods is superior to each other and they are suitable for different kind of organizations [30].

The overconfidence effect is more human problem as we, as humans, tend to assume risk estimates far too optimistic, which biases the outcome of risk, probability, threat and impact assessments. The research [13] also highlights that none of the evaluated eight risk management approaches, including NIST SP 800-30, ISO/IEC 27005, and OCTAVE, does not include any means to overcome the effects of the overconfidence.

Failed knowledge sharing creates a clear deficiency of organizational security and risk management. When independent units of organization, projects and persons share information, their awareness of assets, threats and controls increases, which leads to higher quality of the risk management process. It is noted that knowledge sharing needs motivation and benefits of it must be mutual. Also [16] highlights the continuous communication and tailored messaging as success factors of the effective risk management.

The last of the listed challenges is the risk vs cost trade-offs. As already discussed, it is hard to provide valid input data, including effectiveness values, weights, dependencies, etc, for the risk analysis. In addition, costs caused by successful attacks are almost impossible to calculate, as they are not limited only to financial loss of the attacked organization, but also indirect collateral damages to customers, partners, and other stakeholders. Successful attack may cause also losses not measurable by money as loss of the personal data or reputation. [5, 13] Trade-offs will exist in the control selection as long as we are not able to provide valid input data and metrics for the specific scenario. Hence, even qualitative risk analysis has its own limitations, it is more suitable for SMEs that lack resources, data and competence to implement the more complex quantitative risk analysis.

2.3 Information security knowledge bases

Knowledge is considered as an important resource for organizations to ensure the continuous business operations. Experience and expertise of the employees will help organization to react in accurate manner to exceptions, when these people understand the complexities of the organization and its operations. Hence knowledge of the employees is having important impact to organizational resilience [27].

Importance of the knowledge sharing as part of the information security risk management has been noted in several researches [13, 16]. Organizational information sharing is an omnichannel activity, including discussions, training, documentation, creation of knowledge bases, etc.

It has been identified in [6, 10] that organizations are not inclined to share information security knowledge in the public web portals as security information is seen as valuable asset against competitors. Although inter-organizational security knowledge sharing has hinders, intra-organizational knowledge sharing with wikis has been proven successful [20, 22]. Knowledge sharing has been noted to require personal trust to other peers and similar incentives. Knowledge sharing and collaboration has also been noted to play an important role in the organizational security risk mitigation [28].

Wiki platforms are becoming more and more popular knowledge and information management tools especial for intra-organizational collaboration to facilitate knowledge management between coworkers [20, 22]. Semantic MediaWiki (SMW) extends basic wiki platforms with the ability to represent, query and manage structured information [22]. Wikis, especially with the semantic extensions, have proven their strengths as knowledge sharing and collaboration platforms for wide variety of purposes especially in software engineering, systems management, and knowledge base systems [26]. Hence, SMW can be seen as a potential collaboration platform for cyber security risk management and associated catalogues for SMEs.

In our previous research [26], we created a novel approach to security control catalogue implementation utilizing the Semantic MediaWiki platform. More precisely, we imported existing NIST SP 800-53 [25] control specification to SMW and created presentations, not available in the document format or NIST SP website, to provide additional viewpoints to security control selection. Additionally, semantic queries were implemented to provide viewpoints to the control catalogue that are not possible with document format specification. As a result, SMW was proven

to provide a potential platform to implement more extensive support for the cyber security risk management.

3. KNOWLEDGE BASE FOR INFORMATION SECURITY RISK MANAGEMENT

3.1 Purpose of research

The main purpose of the current research efforts is to assess, by constructing a prototype, whether it is possible to use semantic wiki as platform for information security knowledge base to improve cyber resilience and risk management processes of especially SMEs. For this purpose, we extend the control catalogue metamodel from our previous research [26] with the risk entity types to enable risk management operations. With the proposed extensions organizations are able to use the knowledge base in two different manners: 1) information source in security control selection, or 2) to implement risk management processes.

Additionally, we evaluate whether, using the proposed approach, it is possible to overcome also other common challenges in the information security risk management presented by [13].

3.2 The construction process

Main phases of the actual realization of the prototype were as follows:

1. Extended SMW metamodel with the risk type taxonomy.
   a. Define SMW templates.
   b. Import selected taxonomy.
   c. Create links from control catalogue to risk taxonomy defining, which risk types each security control mitigates.
2. Extend control catalogue to support resilience driven control selection.
   a. Add CIA properties to control catalogue and update Security control semantic form.
   b. Utilize semantic search to support view the controls by CIA properties and existing priorities
3. Provide means to manage risks in the wiki.
   a. Create semantic forms to add, modify and retire risks.
   b. Utilize semantic search to browse and review risks.

The construction process was iterative in the sense that semantic search functions for all the main phases we added and modified after more semantic properties became available.

3.3 Implementation

3.3.1 Extended metamodel

At the first phase of the research, we extended the existing control catalogue metamodel to include risk management related ontology definition.

The initial metamodel of the control catalogue was described in [26]. The catalogue was extended with three new types; risk, risk class and CIA. This extended metamodel is presented as UML diagram in Figure 2. CIA is enumeration of the CIA triage including values of confidentiality, integrity and availability. Purpose of the enumeration is to classify the controls based on the CIA property they preserve and hence help organizations to select controls that provide the best support for organizational security goals. Risk class is used to implement the cyber security risk taxonomy to classify controls by the types of the risk they mitigate. The purpose of the risk class is to help organization to short list controls that are suitable for the identified risk type. As last, the security risk represents an instance of identified, concrete security risk in the organization, such as fire in the "fire in the server room at Abbey Road office". It is added to the metamodel to support basic risk management functions.

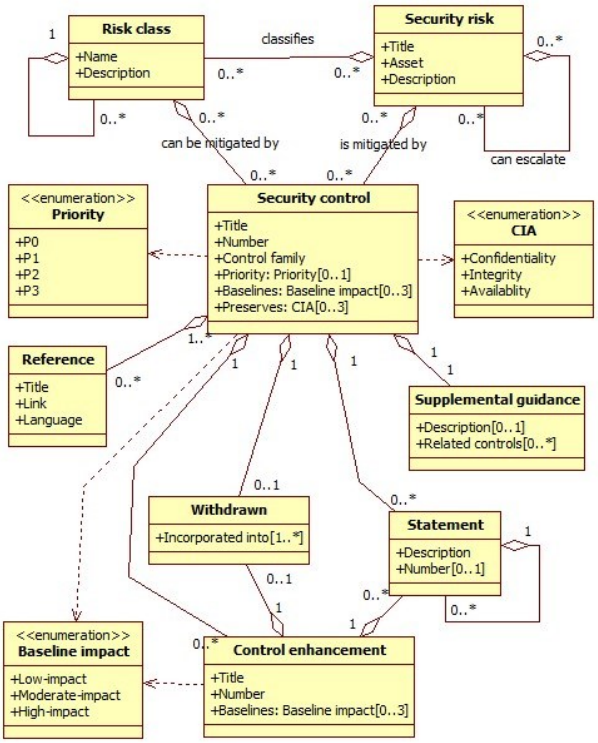

Figure 2: Metamodel UML definition.

3.3.2 Risk taxonomy

In [7] a taxonomy of the operational cyber security risks is defined. The taxonomy has four main classes of the risks.

- actions of people: action, or lack of action, taken by people either deliberately or accidentally, which has impact to cyber security
- systems and technology failures: failures of hardware, software, and information systems
- failed internal processes: problems in the internal business processes that impact the ability to implement, manage, and sustain cyber security, such as process design, execution, and control
- external events: issues originating outside of the organization, such as disasters, legal issues, business issues, and service provider dependencies

Each of the main classes are further divided into multiple subclasses, which are described by their elements. The following list presents subclasses by the main classes.

1. Actions of people
   1.1. Inadvertent
   1.2. Errors
   1.3. Omissions
2. Systems and Technology Failures
   2.1. Hardware
   2.2. Software
   2.3. Systems

3. Failed Internal Processes
    3.1. Process design and execution
    3.2. Process controls
    3.3. Supporting processes
4. External events
    4.1. Disasters
    4.2. Legal issues
    4.3. Business issues
    4.4. Service dependencies

The risks can cascade, which means that a risk in one class can trigger risks in another class. For example, external disaster, like fire, can cause malfunctioning hardware. Due to the cascading effect, it is difficult to predict all actual costs of the realized risks.

The wiki implementation contains taxonomy based on the presented definition by [7]. The HierarchyBuilder extension of SMW can be used to visualize the taxonomy as presented in Figure 3.

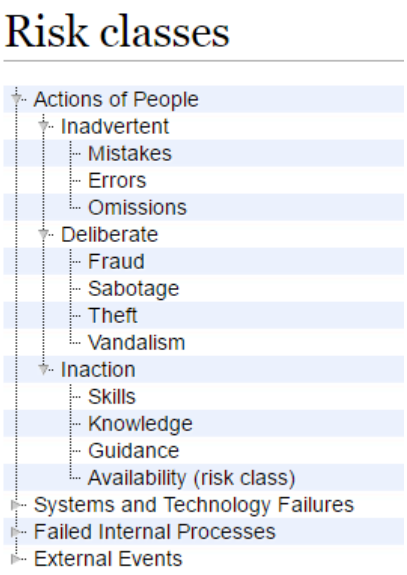

Figure 3 Screen capture of the "Risk classes" wiki page.

Risk class is implemented as page template in the SMW. Instead of separating risk class, subclass and element, we create similar hierarchy using referencing to the parent class. At the prototype implementation, reference is implemented as many-to-one relationship, which means that the risk taxonomy must create a hierarchy. It is possible to later update the relationship to many-to-many enabling also more complex risk taxonomies to be used, if seen necessary.

3.3.3 Control inventory

The control inventory used in the research was based on our previous research [26], where we imported controls of the NIST SP 800-53 [25] specification to SMW. The controls are available by the NIST in XML format and our earlier efforts included XSL transformation of the controls from the NIST defined XML schema to the XML schema used by the SMW page templates.

To help organizations in the control selection based on the aspect of the CIA triage, we added to the NIST SP 800-53 control catalogue metadata which identifies what triage attributes the corresponding control supports. Each control can support one or more of the confidentiality, integrity and availability properties. As described earlier, the organizational resilience is mostly driven by the availability and less dependent on the integrity and confidentiality. This does not mean that integrity and confidentiality should be disregarded, but provides merely one viewpoint to support the control selection by the SMEs. For example, omitting privacy as part of confidentiality can lead to realization of the legal risks and lead to severe sanctions.

Figure 4 Screen capture of controls preserving availability.

The practicability of the SMW and its extension can be seen in Figure 4, where semantic search is associated to Semantic Result Formats extension enabling to filter the controls. NIST SP 800-53 contains 240 active controls and 586 active control enhancements, which makes effective search and filtering capabilities essential. In the figure, the controls ensuring availability are listed and filters limit the display to only controls on low baseline (controls that should be implemented always) and priority level 1 (highest priority controls to implement). With this query and semantic filtering, we are able to display the highest priority controls to implement to maintain the availability. From the cyber security risk management point of view, these are precisely the controls that are critical to support organizational resilience.

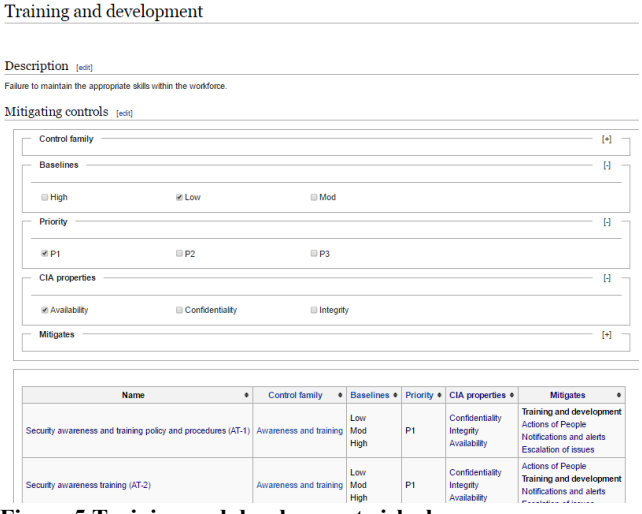

Figure 5 Training and development risk class.

For the risk class template, we created a query that displays the controls that are applicable to mitigate risks of the class. As risk classes are defined in the three levels and each control is attached to a risk class on any level, it is necessary to implement query to find all subclasses of the defined risk class. So instead of searching only the class, we use array of class and its subclasses as the search

criteria. The search is performed to find all controls that have one or more of the items in the mitigation property array. As result, the table of controls mitigating the risk class is displayed on the page of the each risk class as shown in Figure 5 Training and development risk class. To help organizations to select and prioritize the controls, a filter functionality is applied to the search results. Hence, user can select, for example, priority P1 and low baseline security controls, which are the ones expected to be implemented first for all information systems including the ones having even low impact and requiring only the fundamental security controls to be implemented.

3.3.4 Risk management functions

The risk analysis includes evaluation of the risk probability and its impact. One of the most used methods for the risk analysis are the risk matrices. The risk matrix contains two axes; likelihood and impact. The risk matrix is used to identify the high likelihood and high impact risks and decrease either or both the likelihood and the impact to mitigate the risk. However, risk matrices are criticized of not providing sufficient support for good decision making and being limited to only subjective risk evaluation. [8]

Instead of using the risk matrix type of risk analysis, we propose to use queries to identify the risks that need attention. As risks cascade there is a relationship between the risks. Hence, we include in the risk definition an attribute that gives us possibility to define unidirectional cascading relationship between any two risks. With additional queries, we are able to rank the risks by using the cascading measures. For example, if a risk refers to many other risks that will be realized due to realization of the risk, then this is an indication of importance of that particular risk and should be taken into account in the risk analysis and control selection. In the qualitative risk analysis such information can be used to predict risk more accurately and decrease the overconfidence effect.

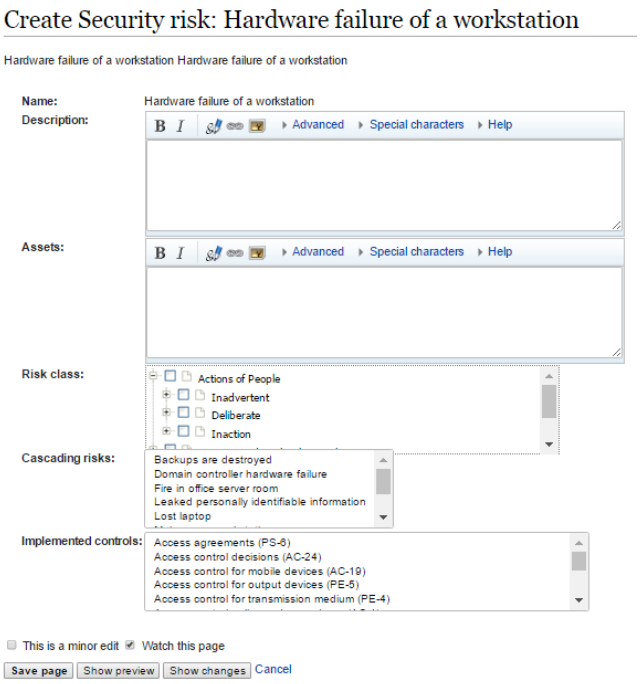

Figure 6 Form to add new security risk.

To allow organizations to manage their own risks with the SMW instance, a security risk template was added. For simplified risk management solution it contains only a limited number of attributes. Each risk has name, description, textual description of assets and risk classes it belongs. Additionally, there are controls that have been implemented to mitigate the risk and list of other risks that can cascade from realization this risk. The security risk form was created to input the risks. The form is presented in Figure 6 Form to add new security risk.

Security risk template is used to review a risk. In addition to displaying user entered information, the template lists security controls that mitigate risk classes defined for the risk, but which are not implemented. Result of such a query is displayed to the user as a list of potential controls. Figure 7 provides screen capture of a sample listing.

Figure 7 Sample risk instance screen capture.

These functions allow organization to use the SMW as a basic risk management platform to identify the risks by using the cyber security risk taxonomy, and perform qualitative risk analysis to evaluate the potential security controls to mitigate the risks. With addition of the CIA properties, the organization is able to filter the set of potential controls to focus on resilience, especially from the availability point of view. Although the resilience is more than implementation of the security controls preserving availability, implemented knowledge base will help users to overcome the lack of knowledge of controls and their effect to cyber resilience of the organization.

4. EVALUATION

4.1 Unique naming requirement

As noted in our earlier research [26], one of the difficulties with the implementation is the unique naming requirement of the wiki pages. Mainly this causes problems with the extensions, like HierarchyBuilder, that use the explicit page names instead of defined properties in the visualization. Example of the problem can be seen in Figure 4, where Availability has disambiguation to refer to the risk class instead of the page Availability, which contains

information of the CIA triage property availability and lists all controls preserving availability.

4.2 Response to risk management challenges

In addition to realizing the prototype we analyzed how the MediaWiki based platform responds to the information security risk management challenges as defined in [13] (see Section 2.2). The first challenge was asset and countermeasure inventory, where the response is partial. The extended control inventory provides the countermeasure, but structured asset inventory is not currently included. This is a notable deficiency in the prototype and should be fixed in the further development. Lack of the asset inventory is also causing lack of support of the second challenge of assigning asset values.

The third challenge by [13] is failed predictions of risks. This challenge is partially solved by the support to identify cascading risk and, hence, having better knowledge of the risk realization probability. Note, though, that because the metamodel does not currently support statistic of the risks or risk types, such an evaluation is a subjective one. This could be solved by extending the metamodel with the statistics and more detailed information of the realized risks and occurred incidents. The problem remains, if no public statistics are available or if statistics are not accurate.

The fourth and fifth challenge by [13] are overconfidence effect and knowledge sharing. With the organizational wiki, we are able to overcome the problem of knowledge sharing at least from the platform point of view. Still the organizational culture must support the knowledge sharing of the cyber security risks and the security controls. The overconfidence effect lead too optimistic risk estimates [13]. This can be at least reduced with the increased knowledge of the related risks and available controls.

Risk vs cost trade-offs is the last challenge by [13]. The prototype is not currently able to respond to this challenge as the risk analysis uses qualitative approach instead of supporting quantitative information. As noted by in [13], solution would require detailed risk management approach, which is not seen suitable for SMEs because of the necessary resource allocation needed.

Overall it can be seen that the prototype partially solves problems, especially with knowledge sharing, and the proposed approach increases the overall understanding of the risks and their relationships. Lack of asset inventory can be seen as deficiency that should be analyzed in detail and solved in further development, but technical limitations from SMW point of view do not limit such extension.

4.3 Improved cyber resilience

Cyber resilience and ensuring cyber asset and service availability has become critical topic, when number of cyber threats is increasing and protection from the all threats is financially unfeasible. To support availability aspect, we introduced traditional information security CIA properties to control catalogue to help the controls selection from availability point of view.

In the NIST SP 800-53 control catalogue there is 115 low impact level controls and 87 of those are on priority level 1. These are the controls that are expected to be implemented in all information systems at the first phase. If we wish to focus on the resilience and the controls especially supporting availability, we can reduce the number of these first phase controls in our classification to about 50 controls.

Limitation of the usage of the CIA properties is that many controls support all three properties, but have direct impact on one property. Example of such control is AC-3 Access Enforcement. Primarily it supports confidentiality, but it has also impact on the availability. Although, we are able to provide support for cyber resilience using the CIA properties, extended classification should be introduced in the future.

4.4 Limitations of the research

Current metamodel does not include asset inventory and support asset-driven approach to security control selection. More comprehensive security risk management taxonomies are readily available [27]. In order to help organizations in the identification of the assets, use of such a taxonomy should be realized.

5. DISCUSSION

Our proposed semantic wiki based approach to manage information security risk knowledge within the organizations provides a technical platform for organizations to start controlled cyber security risk management. While the proposed platform has publicly available information as prefilled contents, it provides, especially for SMEs lacking extensive cyber security skills, easier way to exclude the irrelevant risks and controls rather than inventing appropriate controls with limited knowledge.

SMW has proven to be a valid platform to share the structured information within the organizations. Where people are used to user interface familiar from Wikipedia, there is a low barrier to start using such a system in the collaboration. With the semantic search functions, we are able to find the risks that have high cascading effect to availability, the most import CIA property from the resilience point of view.

Although current implementation provides basic functionalities for the risk analysis, the current metamodel has its limitations. Current model of the wiki is based on the NIST SP 800-53 control catalog. The catalogue is not complete set of security controls, although it is comprehensive. To create an extensive information security knowledge base, we need to create a true ontology for semantic wiki that harmonizes concepts from the main data sources.

Assets and countermeasures are ontologically connected through vulnerabilities and threats. Vulnerabilities exist in the assets and are used by the treats where countermeasures mitigate the threats. These concepts are excluded from the metamodel as it is not seen essential for the SME point of view to maintain threat and vulnerability catalogues. Although it is information that has meaning for the risk analysis, it should be further considered whether there would be centralized repository for threats and vulnerabilities, which can be replicated to organization specific wiki instances. Also asset and risk taxonomies could include centralized management.

Metamodel excludes elements of the incident management, which would be essential for a continuous risk management process. When incident information would be available in the wiki, it could be linked to assets or asset types and also to risks. This would enable an organization to monitor effectiveness of the implemented controls and provides statistical information for the quantitative risk analysis.

Our research continues with extending and generalizing the metamodel to be able to provide more extensive platform for SMEs to manage their information and cyber security risks. The future research focuses to develop cyber risk management platform for SMEs based on the SMW, which has proven its strengths as a platform for security knowledge bases.

6. REFERENCES

[1] Arbanas, K. and Čubrilo, M. Ontology in Information Security. Journal of Information and Organizational Sciences, 39, 2 (2015).

[2] Bhamra, R., Dani, S. and Burnard, K. Resilience: the concept, a literature review and future directions. Int J Prod Res, 49, 18 (09/15 2011), 5375-5393.

[3] Birkie, S. E., Trucco, P. and Kaulio, M. State-of-the-Art Review on Operational Resilience: Concept, Scope and Gaps. (2013), 273-280. DOI=10.1007/978-3-642-40361-3_35.

[4] Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R. and Toval, A. Basis for an integrated security ontology according to a systematic review of existing proposals. Computer Standards & Interfaces, 33, 4 (6 2011), 372-388. DOI=10.1016/j.csi.2010.12.002.

[5] Caldwell, T. The true cost of being hacked. Computer Fraud & Security, 2014, 6 (6 2014), 8-13. DOI=http://dx.doi.org/10.1016/S1361-3723(14)70500-7.

[6] Camara, J., de Lemos, R., Laranjeiro, N., Ventura, R. and Vieira, M. Robustness-Driven Resilience Evaluation of Self-Adaptive Software Systems. IEEE Transactions on Dependable and Secure Computing, PP, 99 (2015), 1-1.

[7] Cebula, J. J., Popeck, M. and Young, L. A Taxonomy of Operational Cyber Security Risks Version 2. (2014).

[8] Cox, L. A. What's Wrong with Risk Matrices? Risk Analysis, 28, 2 (2008), 497-512.

[9] [9] Fang, Y. P., Pedroni, N. and Zio, E. Resilience-Based Component Importance Measures for Critical Infrastructure Network Systems. IEEE Transactions on Reliability, PP, 99 (2016), 1-11. DOI=10.1109/TR.2016.2521761.

[10] Feledi, D. and Fenz, S. Challenges of Web-Based Information Security Knowledge Sharing. Proceedings of the Seventh International Conference on Availability, Reliability and Security (ARES), 2012, 514-521.

[11] Fenz, S. and Ekelhart, A. Formalizing information security knowledge. In Anonymous Proceedings of the 4th international Symposium on information, Computer, and Communications Security. ACM, 2009, 183-194.

[12] Fenz, S. and Ekelhart, A. Verification, Validation, and Evaluation in Information Security Risk Management. Security & Privacy, IEEE, 9, 2 (2011), 58-65.

[13] Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. Current challenges in information security risk management. Info Mngmnt & Comp Security, 22, 5 (11/10; 2015/12 2014), 410-430. DOI=10.1108/IMCS-07-2013-0053.

[14] Hilton, J., Wright, C. and Kiparoglou, V. Building resilience into systems. In Anonymous Systems Conference (SysCon), 2012 IEEE International, 2012, 1-8.

[15] Humphreys, E. Information security management standards: Compliance, governance and risk management. Information Security Technical Report, 13, 4 (11 2008), 247-255.

[16] Hunt, R. Why governance, risk and compliance projects fail – and how to prevent it. Computer Fraud & Security, 2014, 6 (6 2014), 5-7.

[17] ISO/IEC 27000:2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO copyright office, Geneva, Switzerland, 2014.

[18] ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. ISO copyright office, Geneva, Switzerland, 2013.

[19] Julisch, K. Understanding and overcoming cyber security anti-patterns. Computer Networks, 57, 10 (7/5 2013), 2206-2211. DOI=http://dx.doi.org/10.1016/j.comnet.2012.11.023.

[20] Kleiner, F., Abecker, A. and Brinkmann, S. F. WiSyMon: Managing Systems Monitoring Information in Semantic Wikis. Third International Conference on Advances in Semantic Processing, 2009. SEMAPRO '09, 2009, 77-85.

[21] Koslowski, T. and Zimmermann, C. Towards a Detective Approach to Process-Centered Resilience. In Proceedings of the Security and Trust Management: 9th International Workshop, STM 2013, Egham, UK, September 12-13, 2013. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, 176-190.

[22] [22] Lahoud, I., Monticolo, D. and Hilaire, V. A semantic wiki to share and reuse knowledge into extended enterprise. In Tenth International Conference on Signal-Image Technology and Internet-Based Systems (SITIS), 2014. IEEE, 2014, 702-708.

[23] Maruyama, H., Legaspi, R., Minami, K. and Yamagata, Y. General resilience: Taxonomy and strategies. International Conference and Utility Exhibition on Green Energy for Sustainable Development (ICUE), 2014, 1-8.

[24] Müller, G., Koslowski, T. G. and Accorsi, R. Resilience-A New Research Field in Business Information Systems? Business Information Systems Workshops. Springer, 2013, 3-14.

[25] NIST Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology, 2013.

[26] Nykänen, R. and Kärkkäinen, T. Tailorable Representation of Security Control Catalog on Semantic Wiki. Submitted, 2016.

[27] P. Shamala and R. Ahmad. A proposed taxonomy of assets for information security risk assessment (ISRA). Fourth World Congress on Information and Communication Technologies (WICT), 2014, 29-33.

[28] Safa, N. S., Solms, R. v. and Futcher, L. Human aspects of information security in organisations. Computer Fraud & Security, 2016, 2 (2 2016), 15-18.

[29] Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. Taxonomy of information security risk assessment (ISRA). Computers & Security. 57 (3 2016), 14-30.

[30] Tatar, Ü. and Karabacak, B. An hierarchical asset valuation method for information security risk analysis. In Anonymous Information Society (i-Society), 2012 International Conference on. (). , 2012, 286-291.

[31] Zahoransky, R. M., Brenig, C. and Koslowski, T. Towards a Process-Centered Resilience Framework. 2015 10th International Conference on Availability, Reliability and Security (ARES), 2015, 266-273.