Towards a Security and Privacy Co-Creation Method

Christophe Feltus, Erik HA Proper
Luxembourg Institute of Science and Technology,
5, avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg
{firstname.name}@list.lu

Abstract — **Cyber collaboration supports and increases the expansion of value co-creation amongst companies and customers by defining innovative business models and by exploiting new types of infrastructures like those dedicated to social media, collaborative workspaces, or e-supply chains for instance. This proliferation of new types of collaboration generates new types of security and privacy threats to be handled by the companies. The deployment of the appropriate controls to cope with the latter is of great value for the continuity of the day to day business. Therefore, in this paper, we investigate how security and privacy may be regarded as types of value and how they may be considered, in collaborative environments, through the lens of value co-creation. Acknowledging the similarities between security, privacy, and value, we afterwards propose a method to co-create security and privacy and we illustrate how the latter may be deployed in the frame of a financial case-study.**

Keywords: Value cocreation metamodel; security cocreation; privacy cocreation; enterprise collaboration; value cocreation language.

I. Introduction

Cyber collaboration supports and increases the expansion of value co-creation (VCC) amongst companies and customers by exploiting new types of infrastructures like those dedicated to social media, collaborative workspaces, or e-supply chains. The amount and the complexity of these collaborations is at the origin of new types of security breaches which give room to new types of viruses like the ransomware that, according to Kharraz et al. [1], represents forms of cyber-attack hardly resolvable. As cyber collaboration and the resulting VCC is at the origin of new threats, and because the deployment of the appropriate controls to cope with the latter is of great value for the continuity of the business, we propose to investigate, in this paper, how security and privacy may potentially be handled through the lens of value co-creation. Practically, this designed decision is grounded on the motivation that considering security and privacy co-creation (SPCC) may be examined as a specialization of VCC [2]. This assertion is justified by the acknowledgement that value is an abstract concept [3] which expresses a measurable information, of a determined nature, and which represents an *assessment of benefits against sacrifices* [4]. Similarly, the discipline of security and privacy also shared this statement that both represent costs for the company but, in return, generate benefit in terms of protection of their information system (IS).

Unfortunately, despite a plethora of research aiming at depicting the fundamental of VCC (e.g., VCC concepts, value in use, value in exchange, etc.), few contributions have been poured in the area of methods for V/SPCC design and deployment. Therefore, in this paper, we propose an innovative approach to support the VCC of a security and privacy nature and that is related to assets shared between two partners. This method is a four steps approach which is based on the three dimensions of the value co-creation model from [2]: nature of the value, method of VCC, and object concerned by VCC.

The next section reviews the related works regarding SPCC and reminds previous works related to VCC. In section III we present the security co-creation method and in section IV we illustrate it through a case study in the financial domain. Section V concludes and discusses the proposed approach.

Running case study: In the financial sector, a retail bank sells assets to its customers and stores and backups the business information in a data center. To monitor the level of privacy, this bank performs regular privacy impact assessments (PIA). In parallel, to monitor the security of the service delivered, the bank's data center performs security GAP analyses (SGAP) that allow estimating the level of compliance between the real level of security and the expected one. Fig. 1, modeled with the e3value language [5], illustrates the exchange of value in and between both stakeholders (blue links). For the time being, the only exchange of value between both consists in the storage of data for the bank and in the money paid to the data center for the storage. The security and privacy co-creation method aims to propose an approach to discover complementary value co-creation in the fields of privacy and security.

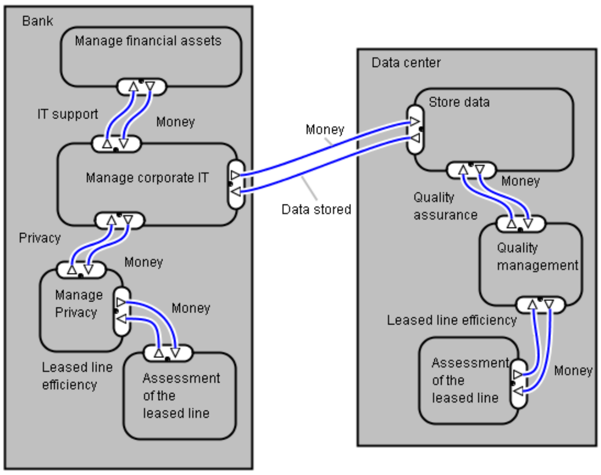

Figure 1. Security and privacy without co-creation - e3value model

The research is supported by the National Research Fund, Luxembourg (http://www.fnr.lu) and financed by the ValCoLa (VCC Language) project.

II. RELATED AND PREVIOUS WORKS

This section first reviews the literature related to the field of security and privacy co-creation and collaborative security, and in the field of VCC more generally, to give an insight on how security, privacy and value co-creation may similarly be handled. Afterwards, the section reminds previous works related to value modeling and to methods of value co-creation.

A. Literature review

As highlighted by Vicini et al. [6], the challenge of security co-creation is twofold: first, to extract the value of the enormous amount of data available in distributed environment, and second, to improve the perception that these data are handled by a trusted system to store privacy protected content. This challenge is especially important when end-users are directly engaged in the co-creation process [7]. Vicini et al. show how it is possible to integrate practical co-creation processes into security and privacy by design methodologies and propose a methodology and guidelines to translate high-level requirements into verifiable low level and technological ones. In [8], Bennaceur et al. address the support of collaborative security in the field of internet of things and explain how the collaborative security tends to exploit and to compose the capability of the connected devise to protect assets from potential harm. The authors propose an approach supported by a dedicated tool to support the above composition using a combination of feature modelling and mediator synthesis. In [9], Martin et al. stress the importance of the collaborative approach to security management in the area of air traffic management, due to the fact that operations and systems become increasingly integrated. Accordingly, they claim that for a successful collaborative approach, security managers need to adopt collaborative leadership skills and approaches. More recently, in [11], Garrido-Pelaz et al. propose a collaborative security approach through the perspective of information sharing which can help to develop early prevention mechanisms. Therefore, they exploit a model for sharing cybersecurity information between dependent organizations that are impacted by different cyber-attacks.

SPCC could be seen as a type of value co-creation. VCC discipline originates from the marketing theory. It aims to define and to explain the mechanisms for the co-generation of value during business exchanges amongst companies [11]-[12]. Vargo et al. [12] [13] formalize it using a framework for defining VCC in the perspective of the service dominant logic (S-DL). According to them, service is the *basis of all exchanges and focuses on the process of value creation rather than on the creation of tangible outputs*. As a result, a service system is *a network of agents and interactions that integrates resources for VCC* [12]. On that basis, value is proposed by a service provider and is determined by a service beneficiary. According to [25], this interaction is defined through situations in which the customer and the provider are involved in each other's practices. Frow et al. [15] propose a framework to assist firms in identifying new opportunities for VCC. Therefore, they provide a strategically important new approach for managers to identify, organize and communicate innovative opportunities. More recently, Chew [16] argues that, in the digital world, service innovation is focused on customer value creation and he proposes an integrated Service Innovation Method (iSIM) for analyzing the interrelationships between the design process elements. At the IS domains level, Gordijn et al. [5] explain that business modeling is not about process but about value exchange between different actors. Accordingly, Gordijn et al. propose e3value to design models that sustain the communication between business and IT groups. In [17], e3value is extended for considering co-creation. Therefore, the authors define the so called *value encounters* which consist in spaces where groups of actors interact to derive value from the groups' resources. The financial case used to illustrate our method is modelled with this e3value language (Fig. 1 and 9). In the same vein, Razo-Zapata et al. propose visual constructs to describe the value co-creation process [18].

B. Value modeling

In our previous work [2], one first contribution consisted in a value creation model structured according to three dimensions (Fig. 2): the nature of the value, the method of value creation, the object concerned by the value.

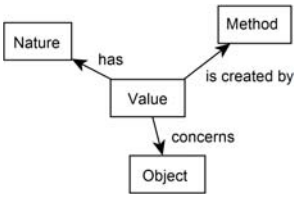

Figure 2. Three value dimensions

These three dimensions of the value creation are defined as:

- **Nature of the value.** The value *has* a nature that expresses a domain of interest and a context that characterize an element of the information system. E.g., security of the IS, actor's responsibility [19], or the data privacy [20].
- **Method (to create value)**. The method is an abstract concept that gathers a set of method elements ordered in steps and achieved in order to *create* value. E.g., process based approach, risk assessment [14], method chunk [21].
- **Object (concerned by the value).** The object *concerned* by the value is the IS element that is better after this value being delivered. E.g., an actor, a process, a data, a server.

In the following, we explain the value creation model and propose three fundamental value co-creation schemas. Based on combinations amongst the latter, more complex VCC schemas may also be designed (e.g., by considering more than one dimension, or for tackling co-creation implying more than two actors). These combinations are not considered in the paper but are available in [2]. The value creation model presented in Fig. 3 includes nine additional concepts which are dedicated to express the three value creation dimensions.

The nature of the value has characteristics that define the value, the latter concerns an object, is created by a method, and is measurable:

- **Characteristics of the Nature of the Value**. This concept expresses the different elements that characterize the nature of the value, or the pillars that found this nature (e.g., availability, confidentiality, portability, etc.).
- **Object**. The object *concerned* by the value is the IS element that is better after this value being delivered. (e.g., an actor, a process, a data).

- **Measure**. The measure corresponds to a property on which calculations can be made for determining the amount of value generated.

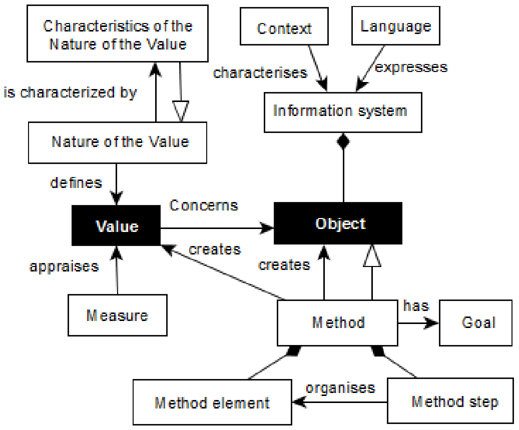

Figure 3: Value creation (VC) model

The method of value creation has a goal, is composed of method elements organized by method steps:

- **Goal**. The goal corresponds to the expected operation on value created by the method (e.g., create value, assess or evaluate value generated, optimize the value).
- **Method element**. The elements of the method correspond to unitary tasks that constitute the method. (e.g., analysis, collection of information, reporting…)
- **Method step**. The method steps consist in the organized and coherent articulations of the method elements (e.g., if-then-else, process elements ordination…)

The objects concerned by the value are impacted by the method. They composed the information system which is characterized by a context and expressed by a language:

- **Information system**. The information system that encompasses the objects concerned by the value.
- **Context**. The context represents the surrounding of the IS (e.g., the sector of the business entity that is concerned by the IS, the rules and regulations related to this sector, etc.)
- **Language.** The language represents the vocabulary used to express the information system of a specific context.

The second contribution of [2] consists in three generic schemas of VCC, built upon the three dimensions of value creation model: nature of the value, method of value creation, and object concerned by the value. The three generic schemas are: (1) **Method-based VCC:** In this first schema, the method is shared by the companies but the nature of the value and the object of value created are different. In this co-creation case, VCC activities achieved by two companies may generate different types of value nature, concerning different objects evolving in different contexts. As a result, the co-creation described in these first schemas happens because enterprises share and achieve activities together that contribute to value creation (e.g., two companies that create value using a shared process-based approach). (2) **Object-based VCC:** This co-creation concerns a unique object that creates value of different natures in different contexts. It concerns two companies that collaborate to co-create value but this value may be of different nature for each of them (e.g., two companies that create two different nature of value for the benefit of a joint network). (3) **Nature-based VCC:** In this third schema, the nature of the value co-created is shared by the companies but the object of value created and the value creation method are different. The VCC activities at the level of each company may be achieved by using different methods and may concern different types of objects from different contexts. However, these different activities concern VCC of the same nature (e.g., two companies protecting the privacy of their customers with different methods).

III. Security and Privacy Co-Creation Method

A. *Security and privacy co-creation*

Security co-creation is an important research topic [6]-[10]. In this paper, we investigate security and privacy co-creation as an instance of value co-creation. Indeed, security and privacy are characteristics of elements of the information system that, when adequately deployed, improve the utilization of the latter. Both security and privacy, according to [2], are themselves defined by the following characteristics: availability, confidentiality, integrity, non-repudiation, etc. (for security) and anonymity, pseudonymity, access to resources, etc. (for privacy). Finally, alike all nature of value, security and privacy are also created by dedicated methods (like risk assessment, cryptography, packet filtering, etc.)

B. *Security and privacy co-creation method*

Based on the three value dimensions and the three co-creation methods presented in Section II.B, the four steps of the SPCC method (Fig. 4) consist, first, in analyzing the value created in each company involved in the SPCC *(Separate assessment*). Afterwards, on the basis of the information collected, the second step consists in searching for potential common opportunities of SPCC regarding one or many of the three value dimensions (method, object and/or nature of the value – *Co-creation analysis*). Thirdly, the method goes on in selecting through the list of opportunities, during an advisory board, which ones of the SPCC the company commits for (*Co-creation commitment*). Finally, step four consists in the deployment of the SPCC within each company's respective information system (*Co-creation deployment*).

1) Separated assessments

This first step aims to collect, assess and model the company's assets that are impacted during the interaction between the partners as well as the activities they have in common and the value generated at each partner side by these activities. At this first step, the value considered is not restricted to a security or a privacy nature but may also concern value of other types like the quality or the usability.

During this step, interviews of the key persons from the companies are performed, existing enterprise models (e.g., architecture model, process model, etc.) are collected (independently of the language they are expressed in), and VC instances of the VC model are generated accordingly.

Input: The input to start the assessment of the companies' contexts is simply "the willingness" to be engaged in the process and the commitment of the managers to support it.

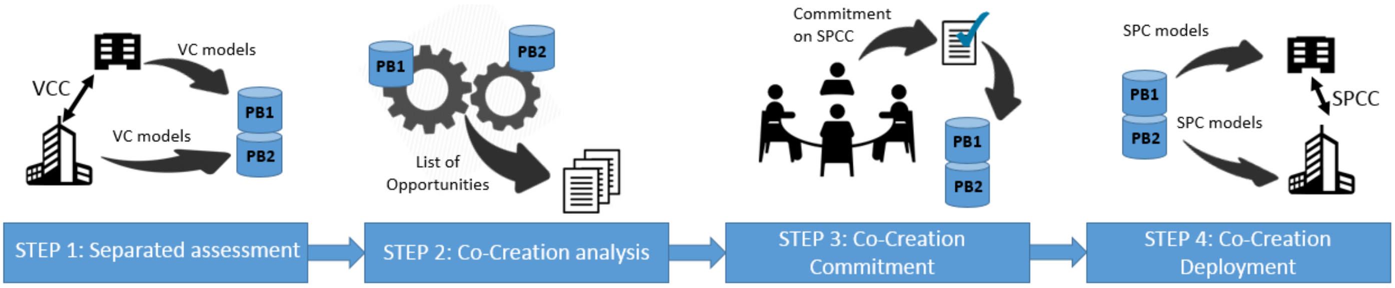
VCC
VC models
VC models
PB1
PB2
PB1
PB2
List of Opportunities
Commitment on SPCC
PB1
PB2
SPC models
SPCC
SPC models
PB1
PB2
STEP 1: Separated assessment
STEP 2: Co-Creation analysis
STEP 3: Co-Creation Commitment
STEP 4: Co-Creation Deployment

Figure 4: Security Co-Creation method

Output: Figures of the companies' business, data and enterprise architecture models, business process, and instantiations of the VC model.

2) *Co-creation analysis*

During this step, all partners' instantiated VC models are compared with the other partners' instantiated VC models. This comparison allows mining the elements that all partner's VC models have in common and where room exists for co-creation. According to the co-creation methods proposed in II.B.2, the analysis focuses on detecting model-based similarities between the types of nature of the value, the value co-creation methods, or the objects concerned by the value. This step may be supported by mining tools for the automatic model matching detection, as explained by Wille et al. [13].

Input: Instantiated VC models from each partners.

Output: Integrated opportunities of security and privacy co-creation models.

3) *Co-creation commitment*

This step is an important one in the process. It implies the decision-makers and managers to analyze which security and privacy co-creations they want to commit for based on the co-creation opportunities detected at step 2. To that end, the co-creation opportunity models are considered as relevant material given their capacity to clearly show impacts and benefits of the co-creations. After the decision being made, the integrated SPCC models are exploited to accordingly transform each respective VC models into a companies' specific security and privacy creation (SPC) models. At this step, two types of company approach may exist: conservative or innovative. In the first case, the company wants to keep working with his ongoing solution but agrees to collaborate in order to support SPCC opportunities. In the second case, the company is likely to accept changing its way of doing and even to adopt the other company's approach.

Input: List of integrated SPCC opportunities.

Output: Security and privacy co-creation commitment from the decision makers and managers, and transformation of the VC models into companies' specific SPC models.

4) *Co-creation deployment*

This step aims at deploying the co-creation activities in the companies' running business. Therefore, each companies' information systems are adapted following the SPC models defined at step 3. These modifications of the companies' IS models are achieved manually or automatically depending of the models at stake and available tools.

Input: Companies' specific SPC models.

Output: Companies' information system adapted following the SPC models.

Table I provides a summary of the manipulations performed at the modeling level.

I. ILLUSTRATION

This section illustrates the deployment of the security co-creation method along the collaboration between a retail bank and a data center. Each step of the method is illustrated phase by phase.

A. *Step 1: Separate assessment*

This step aims at collecting the value co-creation activities from each company. Therefore, the VC activities (including the PIA and the SGAP) are analyzed and the VC model (Fig. 3) is instantiated accordingly.

TABLE I: MODELS' CONTRIBUTIONS DURING METHOD STEPS

	Step 1: Separated assessments	**Step 2: Co-creation analysis**	**Step 3: Co-creation commitment**	**Step 4: Co-creation deployment**
Companies' IS models	Companies' IS models are used to instantiate VC model			Companies' IS models are updated based on SPC instances
VC model and instances	VC instances of the VC model are created	VC instances are used for SPCC opportunities mining		
SPCC instances		SPCC opportunities are mined from each partner's VC instances	SPCC opportunities are proposed and validated by the decision makers	
SPC instances			SPC instances are generated based on selected SPCC	SPC instances are used to update each partners' IS.

Fig. 6 and 7 illustrate this instantiation respectively for the PIA process at the bank level and the SGAP at the data center level. At the bank, the nature of the value is the privacy of the bank customer's financial assets. This privacy is generated by a privacy impact assessment method composed of the following elements: assessment of the leased line (that allows the data storage at the data center), assessment of the web portal, assessment of the value of the privacy, and analysis of the value/impact.

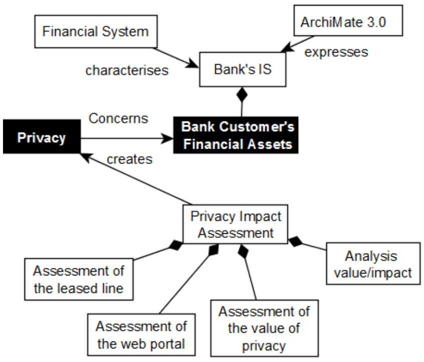
Financial System
ArchiMate 3.0
characterises
Bank's IS
expresses
Concerns
Privacy
Bank Customer's Financial Assets
creates
Privacy Impact Assessment
Analysis value/impact
Assessment of the leased line
Assessment of the web portal
Assessment of the value of privacy

Figure 6: VC instance of the PIA at the bank

The same instantiation of the VC model is afterwards performed at the data center side. At that level, the nature of the value is the security of the data center backup and archiving operations. This security is obtained thanks to a security GAP analysis method which is built on the following four elements: assessment of the leased line, risk analysis, analysis of the cost of the controls, analysis of the business assets and assessment of the impact of a failure.

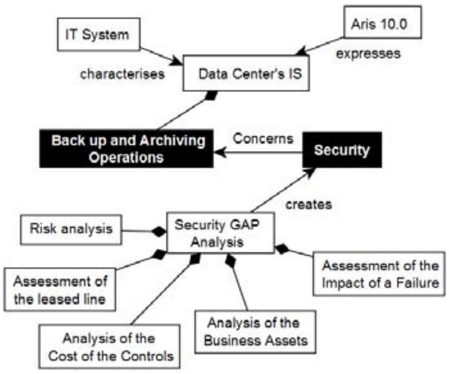
IT System
Aris 10.0
characterises
Data Center's IS
expresses
Back up and Archiving Operations
Concerns
Security
creates
Risk analysis
Security GAP Analysis
Assessment of the Impact of a Failure
Assessment of the leased line
Analysis of the Business Assets
Analysis of the Cost of the Controls

Figure 7: VC instance of the security GAP at the data center

B. Step 2: Co-creation analysis

This step aims to analyze and to detect security and privacy co-creation opportunities between companies. Therefore, the instances of the value creation models from both institutions, defined at step 1 (i.e., PIA and SGPA), are systematically compared with each other in order to identify similarities between concepts. As explained in II.B, the similarities may exist at the nature of the value level, at object of value level, or the value creation method level. Fig. 8 illustrates that both the PIA and the SGAP activities need to assess the leased line that allows the transfer of information from the bank to the data center. In that regard, a potential co-creation opportunity could be to assess it once and share the result amongst the partners.

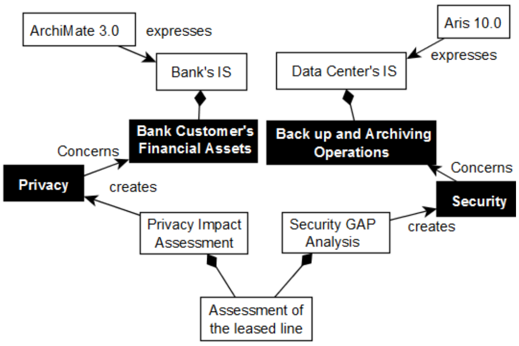

Figure 8: Security and privacy co-creation instance

C. Step 3: Co-creation Commitment

This step aims at taking the decision on which co-creation opportunity is relevant and justified for both companies and on adjusting the VC model of each company accordingly. For instance, after the commitment meeting, decision makers and managers of both companies agree to co-create security and privacy by optimizing the assessment of the leased line. More precisely, the assessment is performed by the data center agents and the results are sold to the bank at a good price. This decision needs to be reflected afterwards in the respective VC model. For instance, in Fig. 9, the element of the method "Assessment of the leased line" (Fig. 6) changed in "Receive subcontracted assessment of the leased line results"

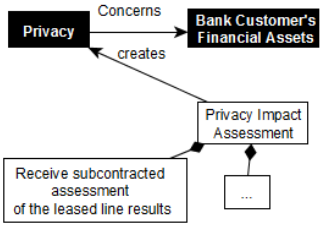
Concerns
Privacy
Bank Customer's Financial Assets
creates
Privacy Impact Assessment
Receive subcontracted assessment of the leased line results
...

Figure 9: Security and privacy co-creation deployment

D. Step 4: Co-creation Deployement

This fourth step concerns the deployment of the co-created value in both ISs of the companies. Only the modeling dimension of this deployment is addressed. Concretely, after pledging commitment for a precise co-creation opportunity, both companies' information systems needs to be updated accordingly. Therefore, the instantiated VC models (SPC models) are mapped with the respective companies' ISs. The latter being expressed in their dedicated IS languages (respectively, ArchiMate 3.0 [22, 24] and Aris 10.0 [23]). Fig. 9 illustrates the new security and privacy value co-created after the achievement of each step of the method, respectively: *Leased line information* and *Money* from the bank to the data center, and *Assessment result* the other way round.

II. Discussion, Conclusion and Future Works

Due to the ongoing developments of collaborative systems, companies are constantly willing to optimize the co-creation of value with their partners. Nowadays, this co-creation that was initially focused on the value of business assets tends to spread over others aspects such as the security and the privacy. This evolution in the creation of security and privacy features calls for new approaches to support companies in investigating and deploying new security and privacy co-creation opportunities. Based on a value creation model and three co-creation schemas, we propose in this paper a four-steps innovative method for security and privacy co-creation that offers the advantage to be:

- simple to understand and deploy,
- adapted for three types of co-creation, to know: method-based, object-based or nature-based co-creation,
- sensitive to decision makers' and managers' commitment that is largely involved during the commitment step,
- independent of the companies information system architecture language (e.g., in the illustration, the bank used ArchiMate 3.0 and the data center used Aris 10.0).

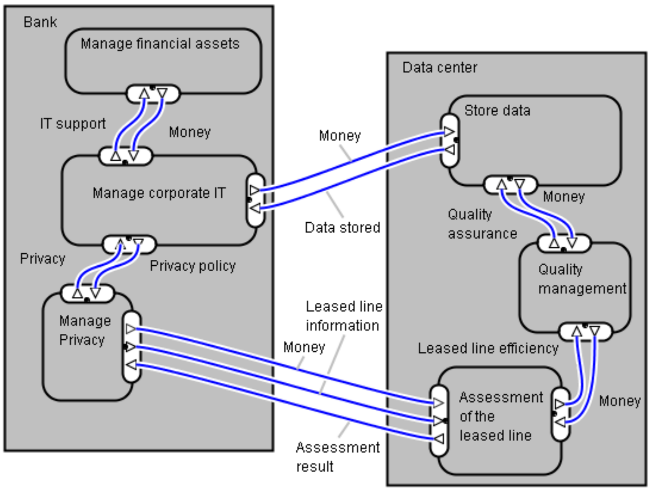

Figure 9: Security and privacy with co-creation - e3value model

As an improvement point, although the illustration happens in a real context setting, further complementary case studies and validations are required to confirm the efficiency of the method. These validations should allow analyzing to what extend the method may also be used to define and deploy security and privacy co-creation in the context of other co-creation schemas (e.g., object- and nature-based co-creation). In parallel, complementary instantiations of the latter should allow verifying to what extend (1) it is adapted and easy to apprehend by security professionals such as consulting companies or other service providers, and (2) it may support the definition of security and privacy co-creation between more than two partners, that is to say in networks of enterprises and business ecosystems.

Another element to be considered in future works consists in equipping the method with the appropriate tools, amongst which a dedicated model mining solution (e.g., [17]). The later would be especially relevant at the co-creation analysis step for detecting the co-creation opportunities by systematical mapping between each value creation instance.

References

[1] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks," in DIMVA 2015, pp. 3-24, DOI: 10.1007/978-3-319-20550-2_1.

[2] C. Feltus, E. Proper, "Conceptualization of an Abstract Language to Support Value Co-Creation", 12th Conference on Information Systems Management (ISM'17), IEEE.

[3] A. Smith, "The Wealth of Nations (1776)," *New York: The Modern Library*. 2000.

[4] V. A. Zeithaml, "Consumer perceptions of price, quality, and value: a means-end model and synthesis of evidence," The journal of marketing, pp. 2-22, Jul. 1988. DOI:10.2307/1251446

[5] J. Gordijn, H. Akkermans, and H. Van Vliet, "Business modelling is not process modelling," In Int. Conf. on Conceptual Modeling, 2000.

[6] S. Vicini, F. Alberti, N. Notario, A. Crespo, J. R. T. Pastoriza and A. Sanna, "Co-creating Security-and-Privacy-by-Design Systems." In ARES 2016. DOI:10.1109/ARES.2016.74

[7] C. K. Prahalad and R. Venkat, "Co-creating unique value with customers," *Strategy & leadership*, vol. 32, no. 3, 2004, pp. 4-9.

[8] A. Bennaceur, T. T. Tun, A. K. Bandara, Y. Yu and B. Nuseibeh, "Feature-driven Mediator Synthesis: Supporting Collaborative Security in the Internet of Things", 2016, Doc. diss., The Open University.

[9] M. Hawley, P. Howard, R. Koelle and P. Saxton, "Collaborative security management: Developing ideas in security management for air traffic control," in ARES 2013, pp. 802-806, DOI: 10.1109/ARES.2013.107

[10] R. Garrido-Pelaz, L. González-Manzano and S. Pastrana, "Shall we collaborate?: A model to analyse the benefits of information sharing," in 2016 WISCS ACM , pp. 15-24, 2016, DOI:10.1145/2994539.2994543

[11] S. L. Vargo and R. F. Lusch, "Service-dominant logic: continuing the evolution," Journal of the Academy of marketing Science, vol. 36, no. 1, pp. 1-10, Mar. 2008. DOI:10.1007/s11747-007-0069-6

[12] S .L. Vargo and R. F. Lusch, "Evolving to a new dominant logic for marketing," Journal of marketing, vol. 68, no. 1, pp. 1-17, Jan. 2004.

[13] D. Wille, S. Holthusen, S. Schulze and I. Schaefer, "Interface variability in family model mining," in Proceedings of the 17th International Software Product Line Conference co-located workshops, pp. 44-51, ACM, August 2013, DOI:10.1145/2499777.2500708

[14] E. Grandry, C. Feltus, E. Dubois, E. 2013. Conceptual integration of enterprise architecture management and security risk management. In *Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2013 17th IEEE International* (pp. 114-123). IEEE.

[15] P. Frow, S. Nenonen, A. F. Payne, and K. Storbacka, "Managing Co-creation Design: A Strategic Approach to Innovation," BJM, vol. 26, no. 3, pp. 463-483, Jul. 2015. DOI: 10.1111/1467-8551.12087

[16] E. K. Chew, "iSIM: An integrated design method for commercializing service innovation," Information Systems Frontiers, vol. 18, no. 3, pp. 457-478, Jun. 2016. DOI: 10.1007/s10796-015-9605-y

[17] H. Weigand, "Value encounters–modeling and analyzing co-creation of value," in Conf. on e-Business, e-Services and e-Society, 2009, pp. 51-64. DOI:10.1007/978-3-642-04280-5_5

[18] I. S. Razo-Zapata, E. K. Chew, and E. Proper, "Visual Modeling for Value (Co-) Creation," in 10th Int. Workshop VMBO 2016.

[19] C. Feltus, M. Petit, and E. Dubois, "Strengthening employee's responsibility to enhance governance of IT: COBIT RACI chart case study, " In *Procs of 1st ACM* WISG '09. ACM, NY, USA, 23-32.4

[20] C. Feltus, E. Grandry, T. Kupper, and J. N. Colin, "Model-Driven Approach for Privacy Management in Business Ecosystem," in *5th Int. Conf. on Model-Driven Eng. and Software Development*, 2017.

[21] J. Ralyté, "Towards situational methods for information systems development: engineering reusable method chunks, " in *Procs. of 13th Int. Conf. on Inf. Sys.Development. Advances in Theory*, Practice and Education. 2004.

[22] A. Josey, M. Lankhorst, I. Band, H. Jonkers, and D. Quartel, "An Introduction to the ArchiMate® 3.0 Specification," White Paper from The Open Group, Jun. 2016

[23] S. Ghatrei, "ARIS Enterprise Architecture's Usage Reviews," Lecture Notes on Software Engineering, 2015, vol. 3, no 1, p. 57.

[24] C. Feltus, E. Dubois, E. Proper, I. Band, M. Petit. 2012. Enhancing the ArchiMate® standard with a responsibility modeling language for access rights management. In *Proceedings of the Fifth International Conference on Security of Information and Networks* (SIN '12). ACM, New York, NY, USA, 12-19.

[25] C. Grönroos, "Service logic revisited: who creates value? And who co-creates?," European business review, vol. 20, no. 4, pp. 298-314, 2008.