An Efficient Security Data-driven Approach for Implementing Risk Assessment

Alireza Shameli-Sendi
Faculty of Computer Science and Engineering, Shahid Beheshti University (SBU), Tehran, Iran
Email: {a_shameli@sbu.ac.ir}

Abstract—Information security implementation in an organization regardless of its business processes will not be effective. Current approaches to risk assessment have moved towards business process-oriented ones. Thus, in new approaches, assets are got attention based on the business processes involved. But existing approaches that are based on business processes have their drawbacks. For example, we need to detail processes to know what security data is produced or used in tasks, and what are their importance from the organization's point of view. Security data certainly has different meanings. How security data moves in an organization's network environment is another important point. Therefore, the main task in information security would be protecting security data, from the point of creation location to storage.

In this paper, several improvements over other solutions are presented. The business processes of the organization are categorized according to security concerns (called fear stories). In the next improvement, we have gone one step further in the business processes, which is extracting the organization's security data. Therefore, security data plays a key role in our model. The next improvement is the introduction of the security data life cycle (creation, edit, display, process, transfer, store), and its adaptation to the asset layers (logical, physical, and human) through a series of predefined patterns. Thus, in this model, a multi-organization pyramid of security needs will be formed, each pyramid being a hierarchical multi-layer, involving security concerns, related business processes, extracted security data, assets involved, identified risks and optimal combination of security controls. At the end of the paper, we will show how the model presented in this paper will effectively improve the popular risk assessment methods such as CVSS (Common Vulnerability Scoring System) and OWASP (Open Web Application Security Project).

Keywords—Risk assessment; Business process; Security data; Vulnerability; Threat; CVSS; OWASP; Security concerns; Security requirement;

1 Introduction

The data of an organization is the most important information about the organization. With increasing generation and exploitation of the data in the organization, providing the security of data becomes more complex [1]. The probability of the endangering of data will cause a huge impact on the organization itself [4]. Unfortunately, risk assessment models are not adaptable to the dynamic environment of the organization [13], [19], while an appropriate solution is necessary that is highly effective and adaptable to the business type of an organization and at the same time can secure the information of it with low financial and time cost [5], [49].

Business process modeling is an activity to help us identify the organization data [42]. According to Weske [2] "a business process consists of a set of activities that are performed in coordination in an organizational and technical environment. These activities jointly realize a business goal". Activities inside business processes should be analyzed by security experts to extract the main important security data which may be targeted by the attackers to be exploited [7]. Before going further, we need to define the security data which is explained as follows: "*Security data is important organizational information that is produced by performing a task in a business process and is important to the organization in terms of confidentiality, integrity, availability, or any combination of them*". Finally, security assessment needed to be performed on extracted security data.

Information security risk assessment is one of the important stages in Information security management systems [3], [12]. Risk assessment helps an organization to get an overview of all risks in the organization [8], [47] which later can help the organization to choose the best combination of security controls to mitigate them [9], [43]. Todays, the structures of the organizations are so different and the existence of an information security management system that can be adopted by different organizations can be so helpful [10], [18]. Note that, nowadays information security is not limited to the physical and logical assets of an organization, and factors such as employee behavior and social factors also affect information security [6], [20].

Various approaches have been presented to assess information security risk. Most of these approaches [14]–[16] are asset-based which suffer several main limitations. Valuing an organization asset is not easy, and most of the time, valuation is wrong. Moreover, we have no knowledge of the percentage of assets participation involved in important organizational business processes and organizational data [44], [45]. These limitations reduce the accuracy of risk calculation in asset-based approaches [4], [17].

In newer approaches [5], [21], [24], [26], there has been a tendency towards business process-based approaches. This is because of the higher value of critical business assets in making more revenue. Current approaches have some limitations. For example, in [10] the risk is calculated concerning

vulnerabilities of a business process and its related assets. But a process might have various security data with different degrees of importance. In many works, the risk is identified and analyzed in the business layer regardless of any relationship to organization assets. Note that the vulnerabilities and countermeasures deployment location depend on the type of assets. Furthermore, the majority of work focused on BPMN (Business Process Model and Notation) visual extensions to cover security requirements. They do not provide a real solution to help effective implementation.

In this paper, for the first time, the concept of "*fear stories*" is introduced. They are expressed by the top executives of an organization. The structure of the security assessment presented in this paper starts with fear stories and ultimately leads to the choice of the best combination of security controls to address them. The hierarchical structure of top-down risk assessment would be: 1) the organization's fear stories, 2) related business processes, 3) extracted security data, 4) assets involved, 5) risks extracted, and 6) selected optimal security controls.

The main contributions of the proposed approach are as follows:

- Risk assessment presented in this paper begins with the extraction of the organization's fear stories. They are a series of important cards arranged in order of priority, and each card alone will create an important pyramid of security need that should ultimately be secured by choosing security controls.
- We extend the BPMN notations to show security data. The security data in the business processes expresses the importance of the assets.
- For the first time, we used the security data life cycle to link to the assets of the organization as well as improve the method of calculating risk. The security data extracted in the business processes should be mapped to the context of the organization (networks and employees). Therefore, they will have several states, which are: 1) data creation location, 2) data editing locations, 2) displayed locations, 2) data crossing locations, 2) data processing locations, 2) data storage locations. To know each state, security data will be mapped to three layers of assets, logical, physical, and human.
- To map security data life cycle to three layers of assets, several patterns are introduced in this paper, for the first time. These patterns, which are based on the type of assets, facilitate the mapping process.
- Risk assessment methods, such as CVSS or OWASP, have provided accurate metrics for evaluation, but the security assessor in many cases requires accurate knowledge of the organization's environment in order to accurately quantify each metric. For the first time in this paper, we have been able to effectively improve many metrics of these methods based on the idea proposed.

The rest of this paper is organized as follows: Section 2 provides the background to our study about risk assessment and the limitations of different approaches in this area. We also investigate the studies about security requirements extension to the BPMN. The proposed model will be discussed in Section 3. At the end of Section 3, we provide a comprehensive discussion, how our model can improve the famous risk rating methods. Section 4 discusses the various experimental results. Finally, Section 5 makes some concluding remarks.

2 Related Work

Business process management and risk assessment in an organization are usually performed as two separate activities and are not closely related. Effective research in this area has begun in recent years to effectively link security risk assessment to an organization's business processes. Research conducted in previous years can be classified into several categories. For example, some work [27], [29]–[32], [50], [51] has sought to provide notations into the visual environment of business processes to illustrate what security concerns may exist in the process. Some research [10], [33], [36] seeks to link processes to organizational goals and organizational assets to determine the importance of assets through organizational goals, as well as to identify asset threats from the analysis of asset-related processes. In some work, process-level risk calculation is proposed [39], [40], [46], [50]. It is based on the activities in the process and how the activities in the process are linked such as sequential, parallel, etc. influence in risk calculation. Some work [32], [34], [35] extends UML (Unified Modeling Language) to aid the security-aware development of software systems. Protecting personal data is another issue that has been the focus of some researchers. For example in [23], they proposed to extend data flow diagrams (DFDs) for collecting and using personal data in the organization. Then, the organization can identify potential incidents to each personal data. In the following, we review the work done and their shortcomings in detail.

Khanmohammadi and Houmb [10] introduced a risk assessment approach that focuses on business processes and the assets are involved in risk calculation indirectly. In this approach, the value of each business process is determined by the business objectives of the organization. They believe that it is easier for domain experts to analyze the risks regarding the business processes as [50] and [32], both emphasize the alignment between business experts and information security experts for risk analysis using the business process. Although in [10], [32], [50] the evaluation of each asset value is based on its related process's data, but they do not describe how to extract the data and do not introduce a new solution to assess risk impact.

Ahmed and Matulevičius [50] presented an approach to align business processes and security requirements using BPMN visual extensions as provided in [29]. The possibility of expressing safe asset, risk, and risk treatment are explored using the capabilities of BPMN. In this way, the requirements and security controls are expressed by the BPMN elements. According to [50], BPMN is the only business modeling language that supports security analysis. Moreover, Altuhhova et al. [30] explored various aspects of BPMN and they aligned the BPMN structure with key aspects of information security risk management.

TABLE 1: Summary of existing information security risk assessment approaches

Work	Year	Adding Security Notation In Business Process	Linking Business Process to Assets	Risk Assessment In Business Process Level	UML/DFD Extension For Security-aware	Data Protection
A. Manna et al. [36]	2020		✓	✓		✓
A. J. Varela-Vaca et al. [40]	2019		✓	✓		
S. C. Cha and K. H. Yeh [23]	2018				✓	✓
D. Olifer et al. [33]	2017		✓		✓	
V. M. Belov et al. [25]	2017		✓			
P. Shedden et al. [45]	2016	✓	✓			
W. Labda et al. [11]	2014	✓				✓
N. Ahmed and R. Matulevicius [50]	2014	✓		✓		✓
O. Altuhhova et al. [30]	2013	✓	✓			
S. Taubenberger et al. [51]	2013		✓			✓
I. Soomro and N. Ahmed [35]	2013				✓	
B. Xue et al. [39]	2012			✓		
O. Altuhhova et al. [46]	2012			✓		
E. W. Cope et al. [27]	2010	✓				
K. Khanmohammadi and S. H. Houmb [10]	2010		✓	✓		
M. Menzel et al. [38]	2009		✓			
J. H. Lambert et al. [31]	2006			✓		
P. Herrmann and G. Herrmann [32]	2006				✓	
N. Nagaratnam et al. [37]	2005				✓	
J. Jurjens [34]	2002				✓	

In [51] a method for risk assessment with the purpose of reducing vulnerability detection error is proposed by analyzing the security requirements of information assets in business process models. The points of entry, processing and transferring of information assets in the business process are identified and related security requirements are reviewed. Failure to meet these security requirements indicates a vulnerability. By examining security requirements in the business process, the technical and organizational problems of information security are covered simultaneously.

Nagaratnam et al. [37] expressed an approach to identify and monitor security requirements in the context of business processes, but it did not analyze security goals, their conceptual models, and their relationship to the business process related entities. Menzel et al. [38] proposed an approach to describe security requirements at the business process layer and their translation to concrete security configuration. They introduced an enhancement for business process modeling to express trust, confidentiality and integrity requirements on an abstract level. The model presented by them provides no method for asset valuation or risk assessment.

Varela-Vaca et al. [40] addressed the problem of automatic security risk management in the BPMS (Business Process Management System). The idea presented in [40] is very close to the idea of Ahmed and Matulevičius [50]. Both believe to detect risks inside business processes and then select the optimal countermeasures to mitigate risks. Ahmed and Matulevičius map the risks identified in business processes to predefined patterns, which are famous solutions to mitigate risks. While Varela-Vaca et al. select the best countermeasure based on the risk reduction amount. Both models suffer a main drawback. Risk assessment is independent of asset vulnerabilities. There is also no relationship between processes and assets. Therefore, we do not know the flow of security data in the network environment. The key question is where the optimal countermeasures should be applied.

In [32], they introduced the MoSSBP framework for analyzing business process security requirements to secure business processes. However, this framework is based on an object-oriented model, using the UML Activity Diagram, which is not a standard way of displaying business processes. In [34], Jurjens presents a UML extension called UMLsec only for UML-based developments.

An overview of the aforementioned research of information security risk assessment is given in Table 1.

3 Proposed Model

There are several reasons for information security implementation failure in organizations. One of the major reasons is the lack of direct supervision of the senior manager on security project implementation. Our proposed model covered this cavity via senior management observation. In the first step, the senior manager collaborates to extract the fear stories of the organization. Then, it is determined which business processes are related to each fear story. The severity value of the fear stories is the criterion for prioritizing business processes. Since we start information security implementation from the top level of the organization management, the manager pursues fear story elimination. Compare this solution with the current ones in which it starts to secure from the assets, the lowest level of the organization, and therefore there is no step-by-step supervision of senior management over the security implementation.

Another benefit of considering fear stories at the start point is to categorize and prioritize the organization's business processes. Certainly, it is impossible to secure all processes of the organization at once, which fails the security establishment. Defining and prioritizing fear stories turn a security project into an agile and repetitive solution that is beyond the scope of this paper. Therefore, a series of fear stories are listed, if we consider each as a card, the cards are prioritized by the CEO (Chief Executive Officer) of the organization. Each card contains a set of related business processes. Afterward,

Fig. 1: Pyramid of organization security needs

valuable security data, which is fundamental from the security perspective, is extracted from the business processes. This security data is associated with confidentiality, integrity, availability or any combination thereof [28].

In our solution, several questions are asked about security data. For example, *where the security data is generated (by which human, what hardware, which logical asset)*? *what assets it passes through*? and *where the security data is stored*? This emphasises the security data life cycle. It consists of six states in the proposed solution: *create*, *edit*, *process*, *display*, *transfer*, and *store*.

Notably, assets are not valued alone in our solution. The value of the asset is calculated based on its content, which is the number of security data and their types. Next, asset vulnerabilities are extracted and the impact of each vulnerability on security data is analyzed. This analysis correctly and accurately evokes the risks and ultimately provides appropriate security controls for each risk.

As illustrated in Figure 1, each card or fear story forms a pyramid, comprising security concerns, related business processes (contains security data), assets involved, risks and optimal combination of security controls. These pyramids are the security requirements planned to be secured.

Furthermore, the proposed model provides the following seven benefits for organizations:

- Identify organization data from a security perspective on confidentiality, integrity, and availability indicators
- Identify safe and unsafe business processes
- recognize the severity of the risks involved in the processes
- Identify the number of vulnerabilities available for each fear story to occur
- Determine the severity of the risk associated with each fear story

Details about our approach will be provided in the remaining sections.

3.1 Fear Story

One of the major problems for organizations is the lack of trust of senior managers or the head of the organization for the usefulness of risk assessment and implementation of an information security management system. This is also one of the most important failures of security system implementation. To address this challenge, we will begin implementation from the top of the organization by extracting fear stories. If an organization does not have a list of security concerns, then it does not need to evaluate the security and implement the information security management system. If senior executives are committed to addressing the security concerns they have raised, this will increase the robustness of the implementation.

Interviews or questionnaires are two efficient methods to extract fear stories. Maybe, someone asks: *what is the meaning of the fear story exactly*? Generally, the fear story is not a vulnerability or a risk. A fear story is a threat that is concerned before being hit. Fear stories are simple enough that the executive manager can learn to declare them in a few minutes. Fear stories should be written on index cards. Then, they are prioritized by the top manager to indicate which are most important from the security perspective.

The inaccurate fear stories may be difficult to interpret. Therefore, the negotiation between the top manager and security expert can help to make the fear stories more precise. Even in many times, this negotiation enables us to break down a general fear story to perceptible fear stories. Note that a general or abstract fear story may cover the majority of the business processes, and then, it drives us away from the philosophy of agile (iterative and incremental) implementation of information security.

It is important to note that the expertise and experience of a security professional is crucial to assisting senior managers in identifying fear stories, and the inability to perform this skill creates inefficient security pyramids (see Figure 1) in the organization.

3.2 Security Data Identification

From the security perspective, one of the fundamental tasks is to identify strategic data that is circulating in business processes, which is targeted by attackers. Therefore, it is essential to design business processes such that they are intelligible for security experts. Business processes are usually described by a Business Analyst or Business Owner. The task name in a business process sometimes is not clear for the Security Analyst. So, clarifying them requires interactions between business and security experts. Then, the input data of each task is determined in the business process. In general, the sources of inputs are from 1) the current business process, namely a previous task, or 2) another business process, or 3) outside the organization. Next, we need to know what processing is done on the input data inside the task. Eventually, the output data of each task is analyzed. All of these steps help us to understand the data circulating in the business processes.

3.3 Data Valuation

We argue that the model presented in this paper is security data-driven rather than business process-driven, which means addressing more details in risk assessment. Thus, the concept of an asset also reformed in our proposed solution. The primary asset is the security data extracted from the business processes and the security expert duty is to protect them. So, the data are the context of the organization and are critical assets that need to be targeted by the security expert.

TABLE 2: Summary description of security data valuation metrics

Metric	ID	Low Value (1-2)	Medium Value (3-6)	High Value (7-10)
Reputation	R			✓
Closure	C			✓
Bankruptcy	B			✓
Future of Business	FB		✓	
Staff Concern	SC	✓		
Customer Concern	CC	✓		
Financial Health	FH		✓	
Occupational Health	OH		✓	

Logical assets, such as operating system, or physical assets, like switches, would be non-critical assets.

To evaluate the data valuation, we propose the parameters presented in Table 2 and prioritize them in three different levels: *low*, *medium*, and *high*. To know the data valuation, first the high critical metrics are evaluated at the first step. Once the answer for any of those three criteria, *organization reputation*, *organization closure*, and *organization bankruptcy*, is yes, the data valuation should be between 7 and 10. Otherwise, the next three criteria, *occupational health*, *financial health*, and *business future*, are investigated. The two rest metrics, *staff concern* and *customer concern*, are used to check the low level. One of the advantages of this model is that there are multiple criteria at each level to determine the data valuation since in some cases experts are not able to answer the criteria explicitly.

The data value is between 1 and 10, divided into three levels: low (1-2), medium (3-6), and high (7-10). The security data valuation is evaluated as follows:

$$\mathrm{D_{value}}=\begin{cases} H_{value} & \text{if } \ H_{in}=1 \\ M_{value} & \text{else if } \ M_{in}=1 \\ L_{value} & \text{else if } \ L_{in}=1 \end{cases} \tag{1}$$

where H_{in}, M_{in}, and L_{in} are three checkers and each of which verifies the level of importance of the data value. For example, if the top level, H_{in}, equals one, it means that one of the "Reputation", "Closure", or "Bankruptcy" metrics will be compromised after an attack on the given security data. Note that, if multiple levels are activated together, the highest level of computation is set. Those checkers are defined as follows:

$$\mathrm{H_{in}}=\begin{cases} 1 & \text{if } \ R+C+B\geq 1 \\ 0 & \text{else} \end{cases} \tag{2}$$

$$\mathrm{M_{in}}=\begin{cases} 1 & \text{if } \ FB+FH+OH\geq 1 \\ 0 & \text{else} \end{cases} \tag{3}$$

$$\mathrm{L_{in}}=\begin{cases} 1 & \text{if } \ SC+CC\geq 1 \\ 0 & \text{else} \end{cases} \tag{4}$$

Once it has been determined at what level the data is placed, its value should be calculated. As shown in equations (5), (6), and (7), the formula for calculating the value at each level is equal to the base value of the level ($H_{base}, M_{base}, L_{base}$) plus the value acquired at the level (X_{level}) plus the lower level value (Y_{level}). The base level values are 1, 3, and 7.

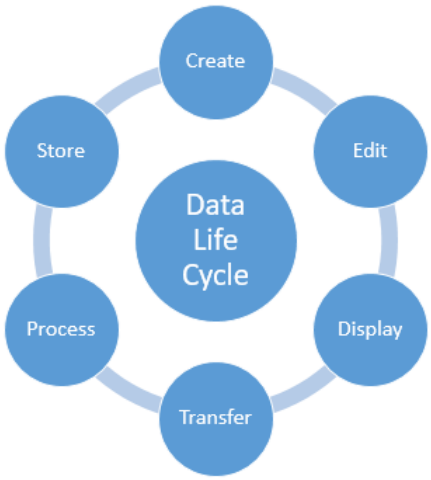

Fig. 2: Six states of security data life cycle

$$\mathrm{H_{value}}= H_{base}+X_{level}+Y_{lower} \tag{5}$$

$$\mathrm{M_{value}}= M_{base}+X_{level}+Y_{lower} \tag{6}$$

$$\mathrm{L_{value}}= L_{base}+X_{level}+Y_{lower} \tag{7}$$

To calculate the level score, we need to check how many metrics are activated in the related level. Because a metric has caused the data value to be at that level, a number is subtracted from the total.

$$\mathrm{X_{level}}=\begin{cases} (R+C+B)-1 & \text{if } \ H_{in}=1 \\ (FB+FH+OH)-1 & \text{else if } \ M_{in}=1 \\ (SC+CC)-1 & \text{else if } \ L_{in}=1 \end{cases} \tag{8}$$

To calculate the lower level score, its checker variable should be validated. If it is equal to one, a number is added to the total.

$$\mathrm{Y_{lower}}=\begin{cases} M_{in} & \text{if } \ H_{in}=1 \\ L_{in} & \text{else if } \ M_{in}=1 \\ 0 & \text{else if } \ L_{in}=1 \end{cases} \tag{9}$$

Now, we provide an example of how to calculate data value based on the formula explained in this section. Suppose all valuation metrics for a data are valuable (see Table 2). So three checkers will be equal to one (see (2)-(4), H_{in}, M_{in}, and L_{in}). This means that each checker states that the data must obtain the value of the corresponding level. But the data

value is calculated based on the highest level (H_{value} in this example). To calculate H_{value}, three values must be specified (see (5)). The base value is equal to seven. The level value counts the number of active metrics at the same level which is equal to three, but since there is a base number, it decreases by one unit. So the level value is two. The value of the data will increase if its lower level checker, which is the second level for this example, equals one (see (9), M_{in}). Since the second level checker equals one, the final value of the data will be 10.

3.4 Mapping Security Data to Assets

Assets in the presented model are classified into three categories: *physical* (e.g., server or switch), *logical* (e.g., Apache service or operating system), and *human* (organizational staff). On the other hand, as shown in Figure 2, the data life cycle comprises six states: *creation*, *edit*, *display*, *process*, *transfer*, and *store*. When discussing data-to-asset mapping, it is important to consider which categories are mapped to each state of a data life cycle. For example, to open a bank account, one of the most critical data is the SIN (Social Insurance Number) number of the account holder. This data is produced for the first time on the computer of the bank clerk. Table 3 shows the events that occur for the data life cycle only at that location. The bank clerk is able to create, edit, and view the data. As shown, three types of logical assets are involved with this data on his computer. The first one is the operating system that sends data for transmission over the network. The second is the front-end of the web banking software that runs on the client-side and includes all states except the store. The last one is Chrome software which performs the display and transfer states as well as the processing operation. In the physical layer, data is transmitted over the network by the bank clerk's computer.

Several patterns are provided to expedite the mapping operation. Generally, a data circulates in three places: *client-side*, *network-side*, and *server-side*. On the client-side, there are several assets such as computers, software users, operating systems, client-side commercial software, web platforms. In the network-side, transmission equipments, such as switch and routers are located. On the server-side, there are the following assets: servers, operating systems, services (such as web, email, etc.), databases, and administrators.

During the mapping, we came up with some predefined patterns. Therefore, they do not need to be filled in by a security expert. In the software implemented to fulfill the approach presented in this paper, the security expert only determines the assets in the client, network, and server sides. Then, based on the predefined patterns, the mapping operation is performed automatically. Tables 4-6 represent the predefined patterns. The security expert can insert any template to our patterns regarding the services and software available in the target organization.

The asset value in our model is calculated based on the data it contains. Each security data consists of six states. These states can be distributed across different assets. For example, data created in an asset is transferred between several assets and then stored in another location. The importance of the states is different. It is determined by the vulnerabilities of the assets as well as the status of the attacks on them. For example, if vulnerabilities and attacks on equipment that are involved in data storage are high in the organization, then the weight of the "*store*" state will be higher than other states. The important point is that the amount of weight is not constant and varies based on the status of the current vulnerabilities, the emergence of new vulnerabilities, and the number of attacks on assets. The asset value, based on the proposed model, can be calculated as follows:

$$AssetValue(a_k, S(Data)) = \sum_{d_i \in S(Data)} \Big(\sum_{s_j \in \{create,\ldots,store\}} (I(a_k, d_i(s_j)) \times W(s_j)) \times \sum_{\delta \in \{C,I,A\}} d_i^{\delta} \Big) \tag{10}$$

where $I(a_k, d_i(s_j))$ is the relationship between asset a_k and state s_j of security data d_i. $W(s_j)$ expresses the importance of state s_j. d_i^{δ} indicates the value of data from CIA (Confidentiality, Integrity, and Availability) aspect.

$$I(a_k, d_i(s_j))) = \begin{cases} 1 & \text{if asset } a_k \text{ has relationship with security data } d_i \text{ for state } s_j \\ 0 & \text{else} \end{cases} \tag{11}$$

$$W(s_j) = \frac{\sum_{a_i \in A} (P(a_i, s_j) \times (V_{a_i} + T_{a_i}))}{\sum_{s_k \in \{create,\ldots,store\}} \sum_{a_i \in A} (P(a_i, s_k) \times (V_{a_i} + T_{a_i}))} \tag{12}$$

where $P(a_i, s_j) \in [0, 1]$ is the relationship between asset a_i and state s_j, which is indicated based on predefined patterns (see Tables 4,5, and 6). V_{a_i} and T_{a_i} represent the total vulnerabilities and attacks on asset a_i.

3.5 Famous Risk Rating Methods Improvement

In this section, we thoroughly discuss the need of changing the popular formulas for calculating risk severity. One of the major problems in calculating risk severity is the proximity of the output of the risk values and the uncertainty of the estimator in selecting the parameter values. Therefore, one of the basic requirements in the field of risk management is to improve the accuracy of risk assessment in the applied formulas.

In some formulas for risk assessment, the value of asset is directly used in calculating risk. In CVSS, OWASP and DREAD methods, there is no direct asset value in the parameters of these methods. In the following, we examine the formulas of these methods and the changes required in risk calculation.

In the classic method, for example, the calculation of risk severity consists of three parameters: *asset value*, *severity of vulnerability*, and *probability of attack*. There are two methods for calculating asset value: *qualitative* and *quantitative* [48]. In the qualitative method, assets are valued on the basis of qualitative values such as low, medium, high. While in the quantitative method, the choice is from a numerical range [22]. In both methods, this choice is based on the experience of the security appraiser, which would be certainly error prone.

TABLE 3: Asset and security data mapping in the e-banking software in client-side

Asset Type	Asset Name	Create	Edit	Transfer	Display	Process	Store
Human	Mr. Smith	✓	✓		✓		
Logical	Windows Operating System			✓			
Logical	Chrome			✓	✓	✓	
Logical	e-banking software (Client Side)	✓	✓	✓	✓	✓	
Physical	PC			✓			

TABLE 4: Predefined patterns of data life cycle states for client-side

Asset Type	Asset Name	Create	Edit	Transfer	Display	Process	Store
Human	User	✓	✓		✓		
Human	Manager		✓		✓		
Human	Executive Manager				✓		
Logical	Operating System			✓			
Logical	Web Platform			✓	✓	✓	
Logical	Software (Front)	✓	✓	✓	✓	✓	
Physical	PC			✓			

TABLE 5: Predefined patterns of data life cycle states for network-side

Asset Type	Asset Name	Create	Edit	Transfer	Display	Process	Store
Physical	Switch			✓			
Physical	Firewall			✓		✓	

TABLE 6: Predefined patterns of data life cycle states for server-side

Asset Type	Asset Name	Create	Edit	Transfer	Display	Process	Store
Human	Admin	✓	✓		✓		
logical	Operating System			✓			
logical	Web Service			✓			
logical	Software (back-end)			✓			
logical	Database						✓
Physical	Server			✓			✓

We presented an idea in which, assets are valued automatically based on the value of the security data contained therein. Thus, the accuracy of classic method can be significantly improved based on our proposed model.

CVSS[1] is a widely accepted standard which provides security professionals with a quite complex scoring system for publicly released vulnerability notifications. CVSS is composed of three metric groups, *Base*, *Temporal*, and *Environmental*, each consisting of a set of metrics. In the following, these groups are explained, briefly.

In the first part of the formula (called Base), in confidentiality, integrity, and availability impact metrics, the security expert is asked whether the vulnerability related to a given risk affects the CIA parameters, regardless of the organization environment. The third part of the formula considers the environmental content of the organization. Security Requirements enable the assessor to apply the importance of the affected asset in a given organization in terms of confidentiality, integrity, and availability. Also, the modified base metrics enable the assessor to adjust appropriately the whole base metrics within the analyst's environment. The important matter is that the evaluator has no knowledge of whether the considered asset contains security data and which value (low, medium, high) should be selected. The idea presented in this paper properly guides the evaluator in choosing the right amount of basic and environmental parameters. Below we explain how this will be improved by our model.

For each risk, we show what degree of devastation occurs with respect to each of the security indicators. Indeed, in our model, there is a chain of business processes up to a risk. From business processes, we can extract security data. We then attach the security data to the assets based on their lifecycle. Now, if the security expert identifies asset vulnerabilities that ultimately lead to the extraction of risks, we will know what impact each risk will have on the asset's security data. It is important to note that when identifying a vulnerability, we must determine its effect on security indicators. A vulnerability, for example, may not affect the integrity of information. Therefore all security data contained in that asset will remain secure.

The metrics of OWASP technique are divided into four categories[2] 1) *Threat Agent*, 2) *Vulnerability*, 3) *Technical Impact*, and 4) *Business Impact*. The model presented in this paper can improve five metrics of this technique, three in technical impact criteria and two in business impact. In the technical impact factors, there are three metrics of loss of

1. https://www.first.org/cvss/specification-document

2. https://www.owasp-risk-rating.com/

confidentiality, integrity, and availability. The evaluator has six choices for each metric. We need the information to decide how much damage a given risk will cause to our organization if for example confidentiality is compromised. If we look at the options, we see that one option is to disclose minimal critical data or the other is to disclose extensive critical data. The key question is how the evaluator should decide. As explained in CVSS metrics improvement, we can improve these three metrics based on the same concept of a chain from business processes to risk. Moreover, in the business impact factors, there are two metrics which can be improved by our solution: 1) *Financial damage*, and 2) *Reputation damage*. As explained in Section 3.3, a number of organizational indicators were expressed to evaluate the data, which included the same two metrics of OWASP technique. Based on our model, we can show the security data associated with these two metrics to the security expert so that she/he can choose the right option in terms of cost and reputation damage.

DREAD is another risk assessment model which provides five metrics for rating as following:

- Damage: reflects how bad an attack would be.
- Reproducibility: reflects how easy it is to reproduce the attack.
- Exploitability: reflects the amount of attempt to launch the attack.
- Affected users: reflects the number of impacted people.
- Discoverability: reflects how easy it is to discover the vulnerability.

In the DREAD method, there is no parameter regarding the effect of the attack on the asset as well as the CIA criteria. The first parameter is damage metric, which expresses the level of information leaking. This parameter can be linked to the security data. Therefore, the evaluator can determine the damage level for each asset based on the security data involved in.

4 RESULT

In this Section, we validate the proposed approach in a real world example. The target organization is a welfare office which provides insurance and financial services. Details about our implementation will be provided in the remaining sections.

4.1 The Structure and Processes of the Organization

This organization has three departments named financial, warehouse and insurance that perform different tasks and are interlinked in some business processes. Due to space limitations, seven important business processes are selected as shown in Table 7. The processes are modeled using BPMN2.0. Some tasks in the processes are performed manually and some of them are executed by software systems, each marked with a corresponding symbol. In each BPMN diagram, information such as the activity in progress, the type of activity, its performer, and data related to that activity can be displayed. But there is no standard symbol to represent the security criteria of the related extracted data. For this purpose, we used a new symbol to specify the security criteria (Confidentiality (C), Integrity (I), Availability (A)) of each data. So, the BPMN meta-model has been extended with seven security notations supporting: C, I, A, C-I, C-A, I-A, C-I-A.

TABLE 7: The selected business processes in the welfare office

Departments	Business Process Name
Insurance	bp_1: Payment of medical expenses bp_2: Financial assistance to the disabled
Warehouse	bp_3: Departure of goods from warehouse bp_4: Delivery of goods to the warehouse
Financial	bp_5: Credit card blocking bp_6: Credit card issuance bp_7: Payment of consulting fees

TABLE 8: The assets in the scope of our security assessment

Department	Human Asset	Physical Asset	Logical Asset
Financial	$user_1$: Matthew	$PC - F_1$	Windows 7 Chrome 22 Financial System Automation System
	$user_2$: Julien	$PC - F_2$	Windows 7 Chrome 21 E-card System
Warehouse	$user_3$: Benjamin	$PC - W_1$	Windows 8.1 Chrome 27 Automation System Warehouse System
	$user_4$: Lucas	$PC - W_2$	Windows 7 Chrome 24 Automation System Warehouse System
	$user_5$: Oliver	$PC - W_3$	Windows 7 Chrome 27 Warehouse System
Insurance	$user_6$: Jack	$PC - I_1$	Windows 7 Chrome 20 Insurance System
	$user_7$: John	$PC - I_2$	Windows 10 Chrome 21 Automation System

4.2 Network Topology

The target organization consists of several different departments, all connected by a LAN, which is used to run software systems. Some systems are also connected to an Internet network to serve outsiders. There is also an IT department where the systems and database servers are located. In each department, each personal computer can only be used by one person locked with a password. For a better understanding of the organization network, its structure is given in Figure 3. It should be noted that in our proposed solution, assets are classified into three categories: *Physical*, *Logical* and *Human*. Table 8 represents some of the assets in the scope of our security assessment in the welfare office.

4.3 Evaluation

4.3.1 Fear Story Identification

Four security concerns were identified based on interviews with senior executives in the target organization, including:

- Issuing unauthorized cards
- Embezzlement in the warehouse

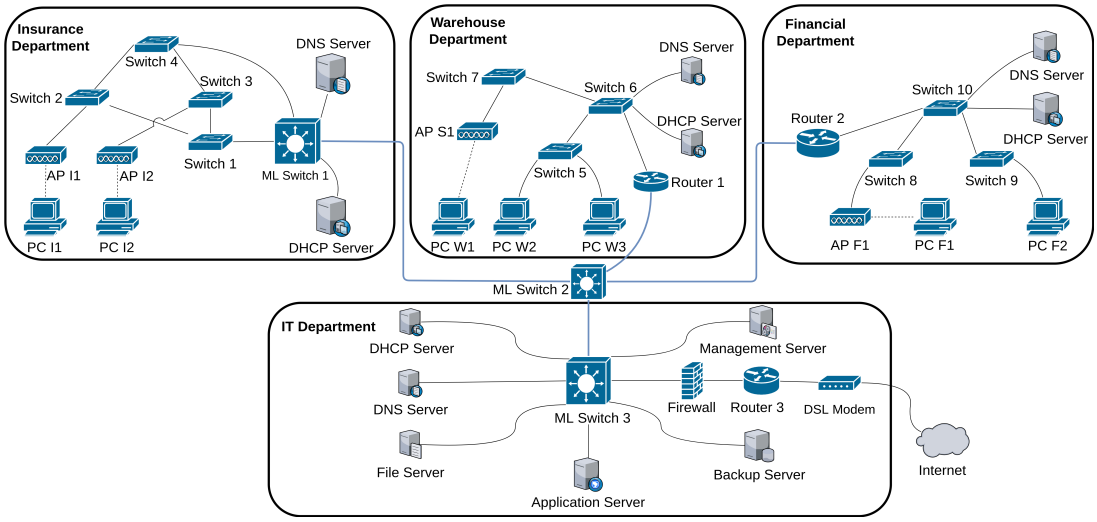

Fig. 3: The network topology of the target organization

TABLE 9: The selected business processes in the welfare office

Fear Story	Type	Score	Business Process Name
Issuing unauthorized cards	Security (Integrity)	10	bp_5: Credit card blocking bp_6: Credit card issuance
Embezzlement in the warehouse	Security (Integrity)	10	bp_3: Departure of goods from warehouse bp_4: Delivery of goods to the warehouse
Employee Disease Disclosure	Security (Confidentiality)	9	bp_1: Payment of medical expenses bp_2: Financial assistance to the disabled
Disclosure of consultation information	Strategic (Business)	5	bp_7: Consulting fees

- Employee disease disclosure
- Disclosure of consultation information

Then, we asked them to prioritize the fear stories to know the most important ones from the security perspective. Table 9 represents the scoring results. As seen, three fear stories have the highest rating and one fear story the average. After the fear stories identification step and prioritizing them, we started to link each of them to the related business processes. In other words, the pyramids of security need began to form. By examining the first important fear story, "*Issuing Unauthorized Cards*", we came to the conclusion that two business processes within the financial department are related to this fear story: 1) "*Credit Card Blocking*" and 2) "*Credit Card Issuance*".

Embezzlement in the warehouse was another major fear story of the organization. After investigations, it became clear that the two business processes involved in the removal of the goods from the warehouse and the delivery of the goods to the warehouse, which belonged to the warehouse department, were related to this fear story.

Another major fear story that received a rating of 9 out of 10 was the lack of disclosure of staff illnesses as seen in Table 9. The chief executive of the organization never wants an unauthorized employee of the organization to know and disclose employee-specific illness information. Moreover, information on financial assistance to persons with disabilities should not be disclosed. In the interview with the senior director of the organization, it became clear that he did not want this information to be made available to competing organizations or others. By examining the organization's processes, it was found that the organization has two processes, namely, "Payment of medical expenses" and "Financial assistance to the disabled", which are strongly related to this security concern. Disclosing consultancy information is another security concern for the organization. They do not want their competitors to be aware of their consulting information (e.g., subject, consultant, fees). In this organization, there is only a business process of consultations, named "Payment of consulting fees".

4.3.2 Security Data Extraction

In this section, we discuss seven business processes in detail. Next, we will analyze how to extract security data in the processes. Figure 4 illustrates the "Credit card issuance" business process. In the process of issuing a Credit Card, the applicant submits his/her application and documents to the financial department. After checking the submitted information, it is entered into the E-card system. Then, a new account is created and the card and PIN are delivered to the applicant. As shown in Figure 4, only one security data is generated in this process that is "New Card Information", in which the criteria of Confidentiality and Integrity are of great importance.

In the process of blocking the credit card, as seen in Figure 5, the applicant submits the request for blocking the card to

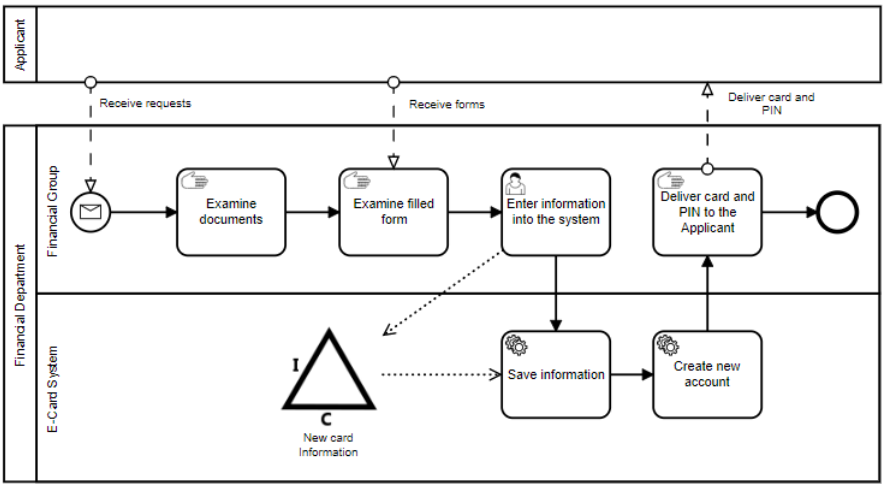

Fig. 4: Credit card issuance business process and related security data

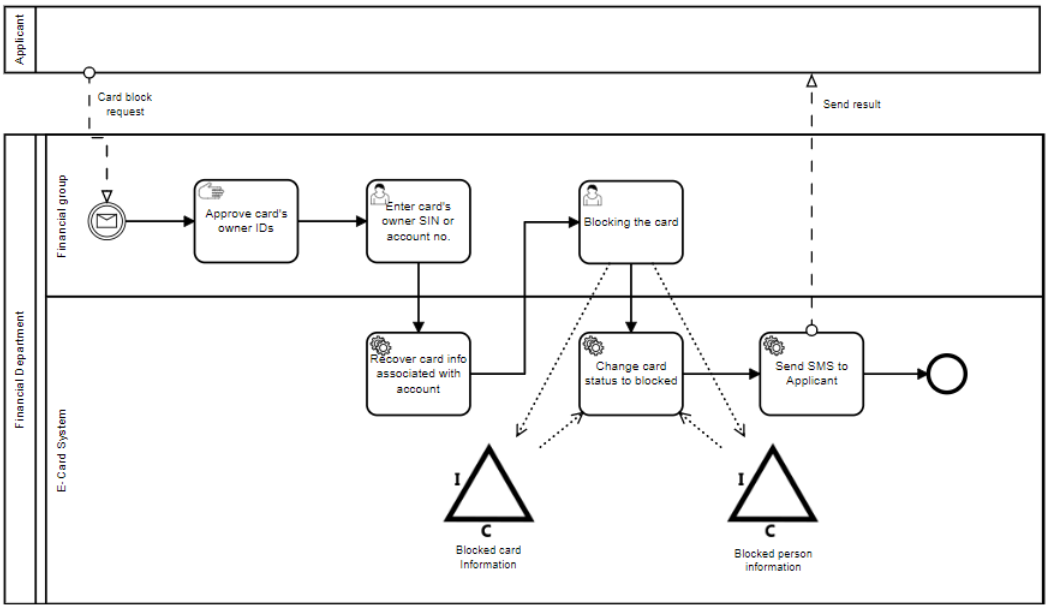

Fig. 5: Credit card blocking business process and related security data

the financial department. The account holder's request is first checked. Then, the account number of the applicant is entered into the credit card system to retrieve card information. All retrieved information must be matched with the applicant's documents. Then, the curator changes the card status to "blocked". The security data of this process is personal and card information. That is, no other person's card should be blocked at all, and the information on the card and the personal information should not be disclosed.

The person receiving the medical bill submits his or her application in person to the insurance department. After reviewing and scanning the documents, the application is sent to the insurance company through the insurance system for verification purpose. Upon receipt of the result and the applicant being authorized, a payment request is sent to the financial department through the interoperability between insurance and financial systems. Then, the applicant must enter his bank card information through the financial system. As shown in Figure 6, three security data are extracted in this process. The first data is the medical information of the applicant, the confidentiality and integrity of which is important. The second data is the medical records of the applicant sent from the insurance system to the insurance company. The third data is the applicant bank card information which is entered by the applicant to pay the financial system and its integrity is important.

As seen in Figure 7, in the process of financial assistance to persons with disabilities, the applicant submits his application to the insurance department. After checking the document, the authorized applicant's information is sent to the financial department through the automation system. The responsible person in the financial department then enters the information into the financial system and after completing the relevant process in the system, expenses are deposited into the bank cards, which have already been registered in the financial system. There are three security data in this process. The first data is called "Disabled Unapproved". This data is generated in the automation system where information integrity

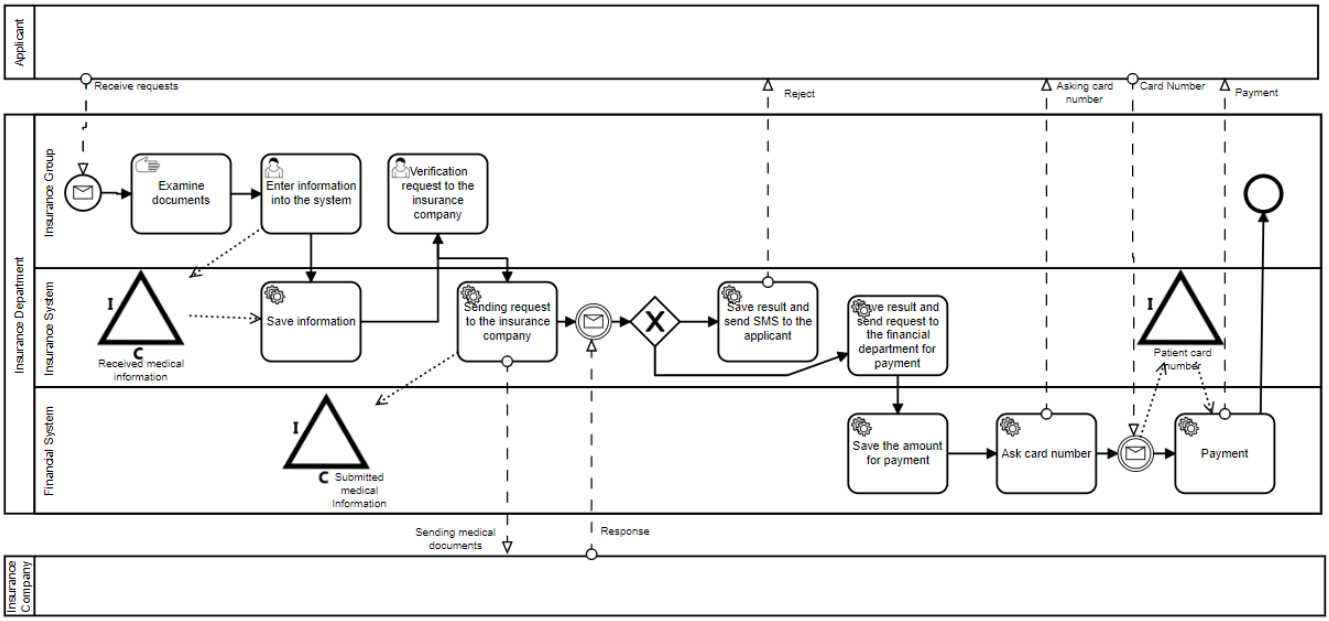

Fig. 6: Payment of medical expenses business process and related security data

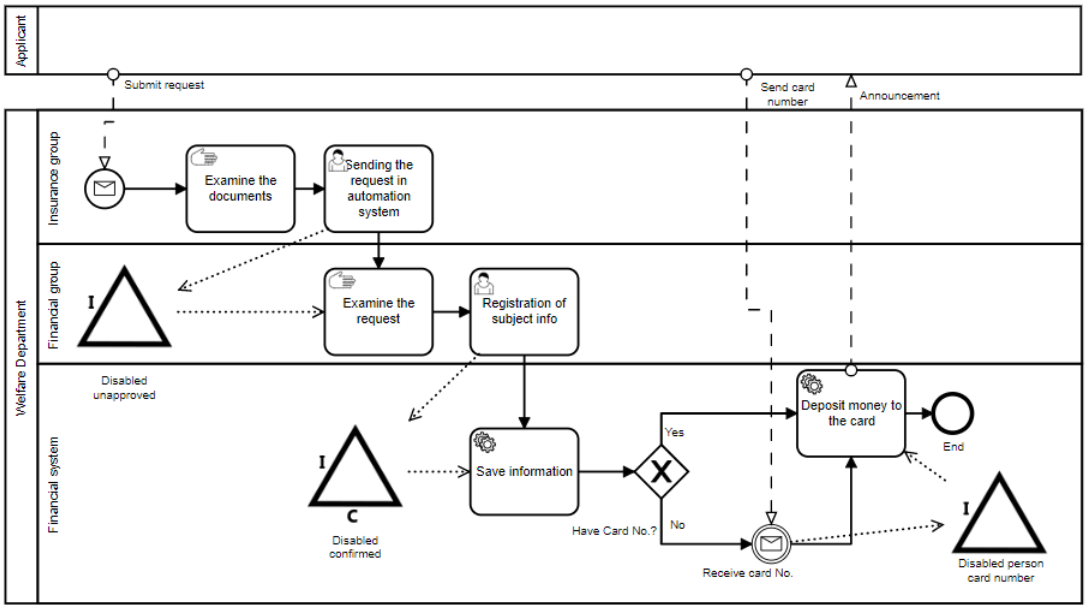

Fig. 7: Financial assistance to the disabled business process and related security data

is considerable. This means that no one must be added or removed from the list. The second data is called ”Disabled Confirmed”, generated and placed in the financial system for payment in which confidentiality and integrity of information are important. The third data is the bank card number that the disabled person identifies in order to be deposited into the account.

The request for payment of the consultation fee is sent to the financial department through the automation system. As shown in Figure 8, a security data named ”Unapproved Consultation Fee” with high confidentiality is created in the automation system. After receiving the consultant and cost information through the automation system in the financial department, the financial officer provides a request to the financial system. The chief financial officer will decide whether or not to pay or part of the costs. The system sends the result to the applicant after creating the billing statement. Therefore, there is another important security data in the financial system about the cost of consulting named ”Approved Consultation Fee”.

The purchasing and delivering of goods process is such that the goods are purchased and then, notified to the warehouse manager via the automation system. The goods are delivered to the warehouse and their information is stored in the warehouse system. As seen in Figure 9, there are two security data in this process; first is the purchased item notified to the warehouse through the automation system. The integrity of this data is preserved and decreasing, increasing and even modifying the type of the purchased item are inhibited. The second is an

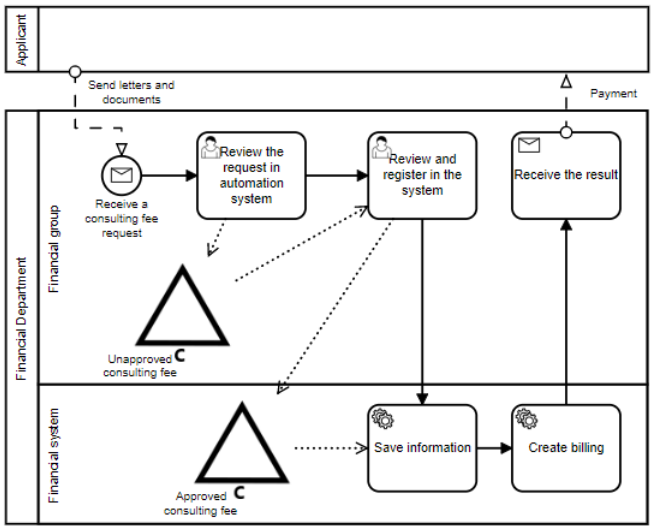

Fig. 8: Payment of consulting fees business process and related security data

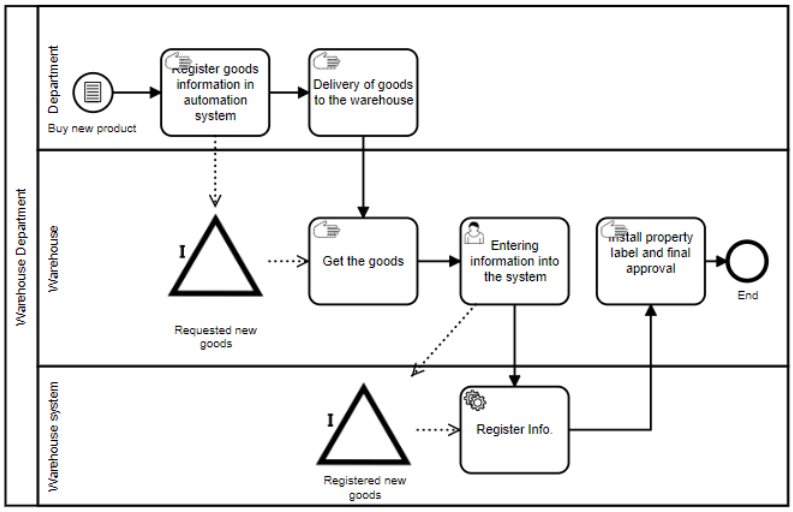

Fig. 9: Delivery of goods to the warehouse business process and related security data

approved and registered product in the warehouse system, whose integrity is also remarkable.

In the process of delivering the goods, as seen in Figure 10, the request for the goods is first given to the warehouse manager through the automation system and then recorded in the warehouse system after checking the warehouse inventory. The warehouse manager approves and then, updates the information in the system and the goods are delivered. There are two security data in the process; the first is the goods requested through the automation system which its integrity should not be altered. Increasing or decreasing of the requested goods is prevented and even the type of goods should not be modified, while the request is done. The second is the registered and approved goods in the warehouse system, whose integrity is important.

4.3.3 Security Data Analysis

It is important to know the distribution of business processes based on the gender of the security data, as seen in Figure 11. If any of the security indicators is breached (e.g., confidentiality), we can easily find out which processes have been affected.

One of the major drawbacks of the previous models was that we had no knowledge of the amount and type of security data in our organization. Figure 12 shows the number of security data in our case study according to their type. Since our indicators are confidentiality, integrity and availability, we have seven different combinations of data. As Figure 12 shows, only three types of data are extracted in the defined scope. A total of fifteen data were extracted and as seen the contribution of confidentiality data type is less than other types.

In the proposed model, we provided a set of organizational indicators for evaluating security data, including: *Reputation*, *Closure*, *Bankruptcy*, *Future of Business*, *Staff Concern*, *Customer Concern*, *Financial Health*, *Occupational Health*. Table 10 represents how security indicators of each data are evaluated (see (1)). Therefore, a link has been established between the security data value and business indicators that can provide important analytics for senior executives of the organization. For example, we can answer the question of

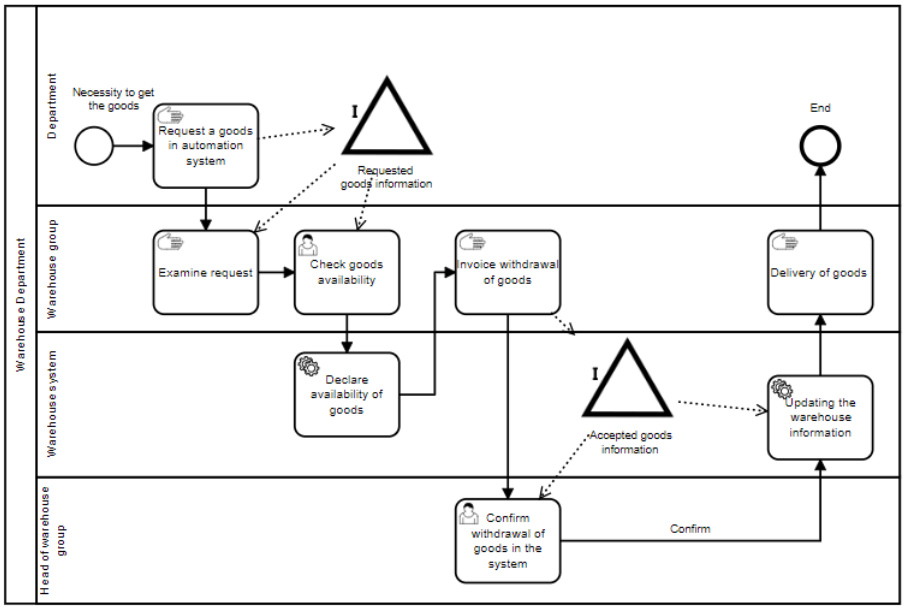

Fig. 10: Departure of goods from warehouse business process and related security data

TABLE 10: Security data value

Data Name	Data Type	Reputation	Closure	Bankruptcy	Future of Business	Staff Concern	Customer Concern	Financial Health	Occupational Health	Value
Blocked Card Information	C								✓	3
	I					✓		✓	✓	5
Blocked Person Information	C					✓				1
	I					✓		✓	✓	5
New Card Information	C					✓				1
	I					✓			✓	4
Received Medical Information	C		✓		✓	✓			✓	8
	I					✓		✓	✓	5
Submitted Medical Information	C		✓		✓	✓			✓	8
	I					✓		✓	✓	5
Patient Card Number	I					✓		✓	✓	5
Disabled Unapproved	I					✓		✓	✓	5
Disabled Confirmed	C					✓		✓		4
	I					✓		✓	✓	5
Disabled Person Card Number	I					✓		✓	✓	5
Unapproved Consulting Fee	C	✓			✓		✓		✓	8
Approved Consulting Fee	C	✓			✓		✓		✓	8
Requested New Goods	I				✓			✓	✓	5
Registered New Goods	I				✓			✓	✓	5
Requested Goods Information	I				✓			✓	✓	5
Accepted Goods Information	I				✓			✓	✓	5

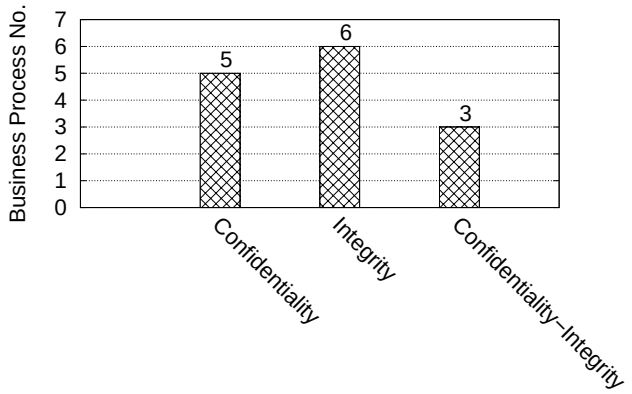

Fig. 11: Distribution of data types based on security indicators to business processes

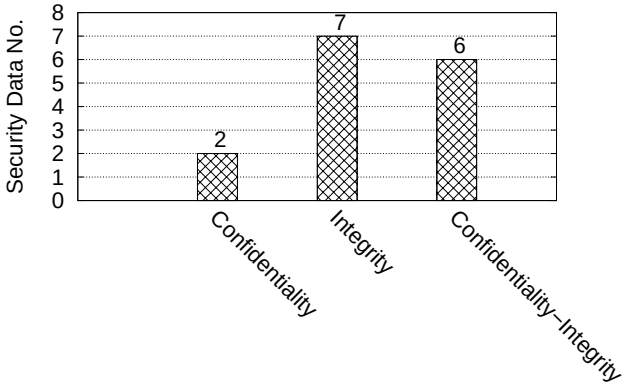

Fig. 12: Type and number of security data available within our case study

what percentage and how much security data can influence the future of an organization's business? What data are they? What are the business processes related to? This information can help us to know which business processes and security data need to be taken care of if a specific indicator is important to our organization.

Figure 13 represents the correlation between security data and organizational indicators. Important points that can be deduced from this figure are: 1) from the fifteen security data identified within the project scope, only two security data affect the reputation of the organization, which are "Unapproved Consulting Fee" and "Approved Consulting Fee", both identified from "Consulting fees" business process, 2) Two security data affect the closure of the organization, which are "Received Medical Information" and "Submitted Medical Information", both extracted from "Payment of medical expenses" business process 3) Damaging any security data does not affect the bankruptcy of the organization, 4) Two of the data, which are "Unapproved Consulting Fee" and "Approved Consulting Fee", are having an impact on customers. If customer orientation is one of the key factors for our organization to compete in the market, this information can be very important, 5) Damage to any of the security data is affecting the health of the organization.

Figure 14 shows the sensitivity of business processes to security indicators in one perspective. As can be seen in the two processes of delivering and receiving goods to/from the warehouse, only data integrity is important. In the process of consulting fees, it is important not to disclose information. In other processes, both confidentiality and integrity indicators are important.

Figures 15 and 16 represent the result of calculating the value of data confidentiality and integrity. If we look at the confidentiality result, four data have the highest value: 1) "Received Medical Information", 2) "Submitted Medical Information", 3) "Unapproved Consulting Fee", and 4) "Approved Consulting Fee". The reason is that these four data influence the reputation and closure of an organization (see Table 9). The other two data, called "Blocked Person Information" and "New Card Information", have the lowest value because confidentiality only relates to one's own concerns. In integrity criteria, two data have no integrity meaning: "Unapproved Consulting Fee" and "Approved Consulting Fee". The value of the other data is about five. This is because compromising integrity does not affect important organizational metrics, which are bankruptcy, closure, and reputation.

As can be seen in figure 17, the payment of the medical expenses process is of the highest importance among the processes. This figure will be of great importance to senior executives in organizations. They find out which processes contain high security data. Therefore, if the payment of the medical expenses process is of high importance to the organization, we should evaluate the status of the vulnerabilities in the assets against the data contained in the process.

One of the important outputs of our model is the relationship between the asset and the security data state. This relationship shows what roles the asset has in data states. In other words, which asset's vulnerabilities can affect security data states. As Figure 18 shows, 14 assets are involved in generating 15 security data: 1) seven human assets which are seven users in three departments and 2) seven logical assets which are seven front-end of different software on seven computers. The same assets can also edit the security data. As can be seen in the transfer situation, human assets do not play a role in security data transmission. There are 28 logical assets involved in data transfer (see patterns in Tables 4-6), which are: 1) seven front-end of different software, seven Chrome web browser, and seven operating systems in client-side, 2) one operating system, one web service, and five back-ends of different software in server-side. Note that these software are *Automation System*, *Financial System*, *Warehouse System*, *E-card System*, *Insurance System*. In the physical part, 30 physical assets are involved in the transmission, which are seven computers in client-side, one server in server-side, one firewall, and 21 switches/access points.

The display state indicates which assets can view or display the data. As shown in the Figure, in the human assets section, seven users can view the data. In the logical part, seven web platforms which are Chrome web browsers and seven front-end of different software can display security data. The same logical assets can also process the security data. We have only one physical asset, one firewall, which processes security data. Regarding store status, a logical asset called a server-side database and a physical asset that is server are involved in storing security data.

Figure 19 shows the value of assets in the defined scope. The weight values of the security data states are as follows: *create= 0.3, edit= 0.2, transfer= 0.05, display= 0.05, process= 0.15,* and *store= 0.25*. Three most important assets are: 1) Application Server (value 32.4), 2) Database (value 27), and 3) PC-F1: Financial System (front-end) and PC-I1: Insurance System (front-end) (value 19.5). The application server holds the most value among human, logical, and physical assets. Based on the predefined patterns for the server-side (see 6), this server involves two states of security data life-cycle: *transfer* and *store*. Since all security data are stored in this server, this asset plays a critical role between all assets. The database which is in second place, is responsible for storing all the data. Note that the database has only one correlation with the store state. In the second place, two assets have the same value: front-end of two applications, insurance and financial system. The insurance system on PC-I1 involves two security data: 1) "Submitted Medial Information" and 2) "Received Medical Information". Each of these data has a value of 13. While the financial system on PC-F1 involves four security data: 1) "Patient Card Number", 2) "Disabled Patient Card Number", 3) "Disabled Confirmed", 4) "Approved Consulting Fee". The value of these data are 5, 5, 8, and 8, respectively (see Table 10). Among human assets, Matthew has a higher value. The reason is that Matthew works with computer PC-F2. He works with two software: *financial system* and *insurance system*. As mentioned, the financial system on this computer involves four security data. Moreover, the insurance system involves another data which is "Unapproved Consulting Fee". The question may come to mind as to why the value of Matthew dealing with five data is less than the value of either the financial system or

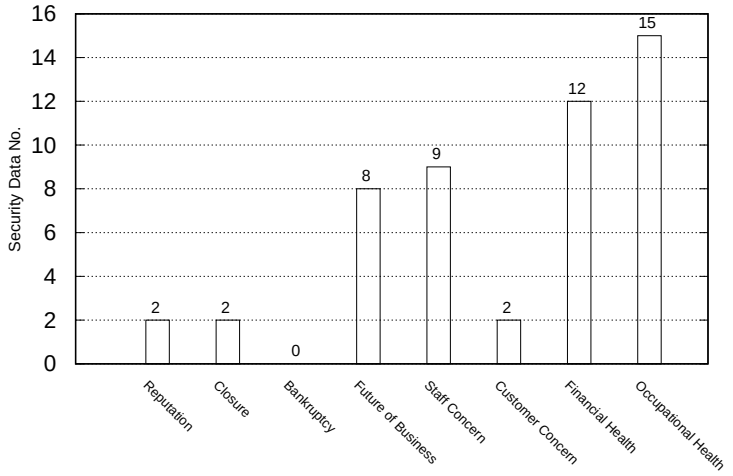

Fig. 13: Relationship between organizational indicators for data valuation within project scope

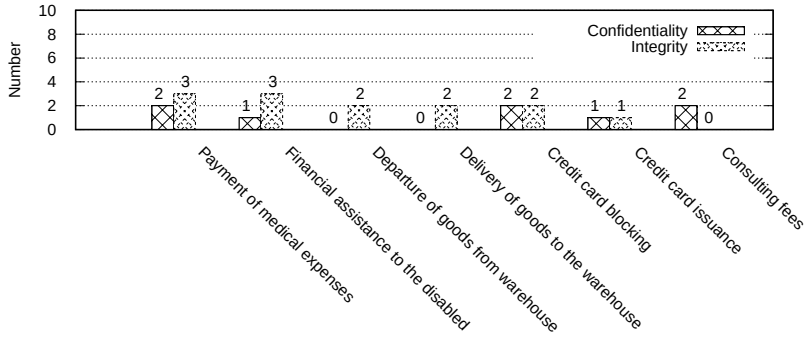

Fig. 14: Distribution of security data types based on security indicators to business processes

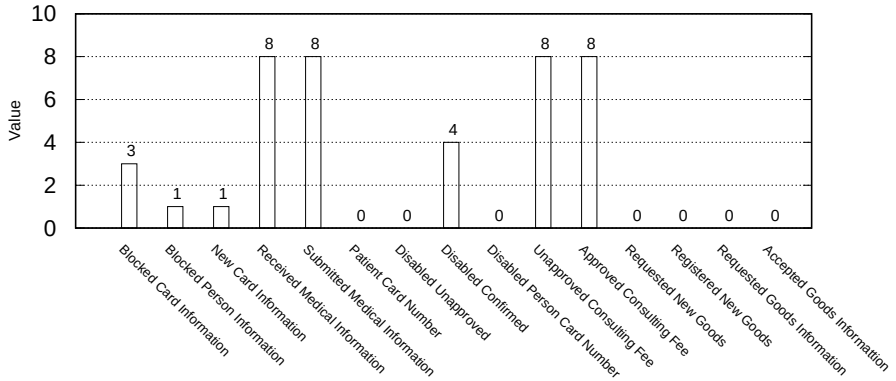

Fig. 15: Confidentiality value of security data

insurance system. If we look at the formula given in the asset value calculation and also the predefined patterns in client-side (Table 4), we will notice that the front-end of software plays a key role in all states except storage. Whereas a user is involved in three state: *create*, *edit*, and *display*.

As mentioned in Section 3.5, the proposed method in this paper can improve the well-known methods of risk severity calculation, CVSS and OWASP. For this purpose, we consider the calculation of two risks in the case study presented. In order to understand the accuracy of the improvement in CVSS and OWASP methods, three security experts were asked to perform the severity calculation and then the mean results are shown. Three experts were first asked to calculate the risk using CVSS and OWASP methods without the knowledge of the information chain that our idea provides. Secondly, they were asked to recalculate the same risks using the knowledge that our model provides.

As described in our case study, the welfare office had seven

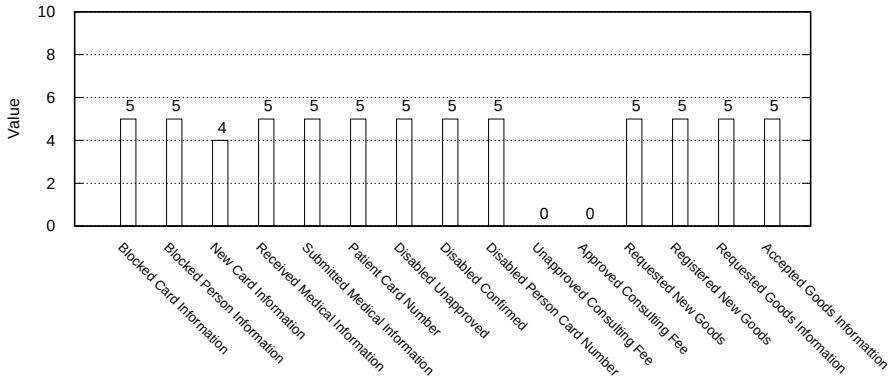

Fig. 16: Integrity value of security data

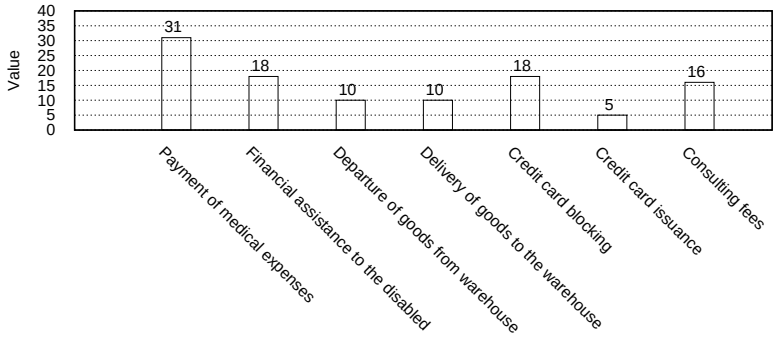

Fig. 17: Value of business processes based on the value of security data contains

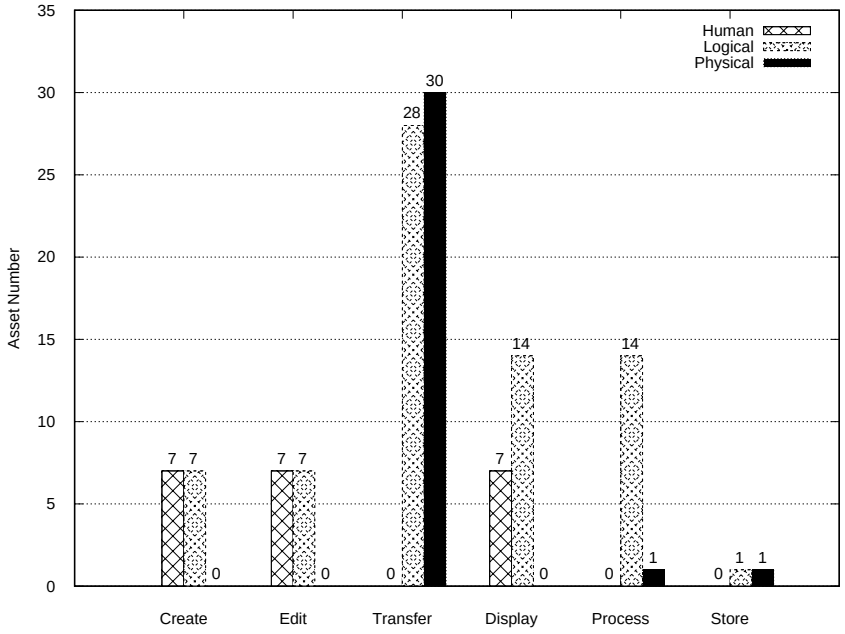

Fig. 18: The Relationship between assets and the security data life cycle

computer users. We considered a vulnerability called ”lack of awareness of the basics of security” that would lead to the disclosure of information. Figure 20 shows the results of the risk severity assessment for seven computer users. As can be seen, for Matthew, Julien, and Jack, the risk intensified as evaluators realized what sensitive data was available to the three users. In the case of Benjamin and Lucas, evaluators found that the two users did not have any sensitive data that

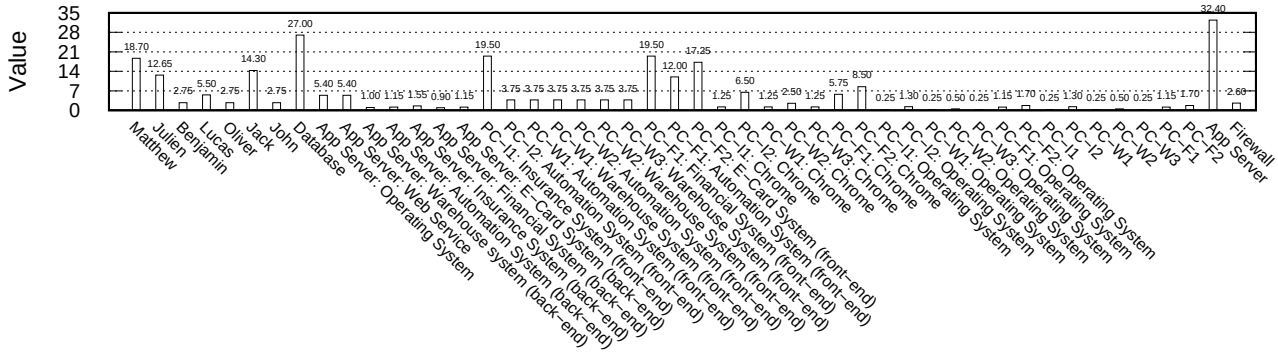

Fig. 19: The value of the assets within the defined scope based on the security data life cycle and their values

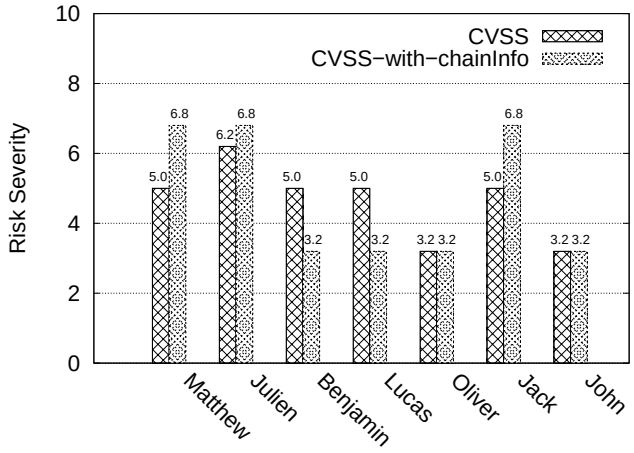

Fig. 20: Comparison of risk severity calculation with CVSS method in two cases 1) without knowledge of the security data of the organization, and 2) with knowledge of the security data available to users

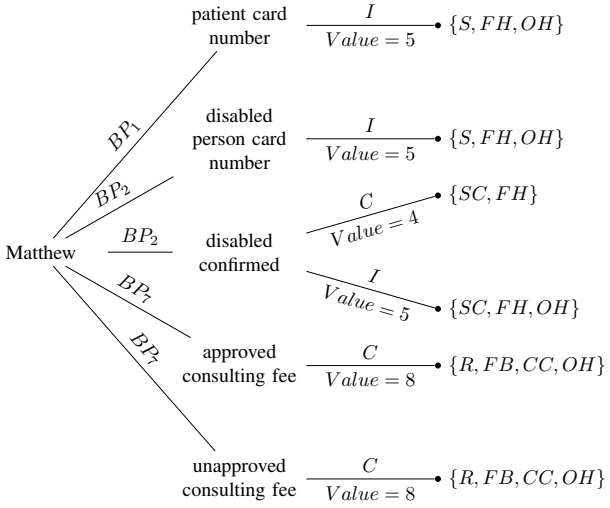

Fig. 21: The information chain under Matthew's authority, along with the value of the data and its effect on organizational indicators (Reputation (R), Closure (C), Bankruptcy (B), Future of Business (FB), Staff Concern (SC), Customer Concern (CC), Financial Health (FH), Occupational Health (OH))

was important from the confidentiality perspective, and so the risk severity was reduced. For the other two users, the risk severity was the same after providing the information. Table 11 shows the security data owned by each user.

Let us take a look at calculating the risk severity for Matthew in two evaluation modes. The details of the first security expert's assessment are presented below:

```
Asset: Matthew
Vulnerability: Lack of awareness of the basics of security
Threat: Disclosure of information
Risk Severity: 5

Setting the parameters of CVSS v3 method
========================================

Attack Vector/Modified Attack Vector: LOCAL
Attack Complexity/Modified Attack Complexity: LOW
Privileges Required/Modified Privileges Required: LOW
User Interaction/Modified User Interaction: REQUIRED
Scope/Modified Scope: UNCHANGED
Confidentiality/Modified Confidentiality: HIGH
Integrity/Modified Integrity: LOW
Availability/Modified Availability: LOW
Exploit Code Maturity: NOT-DEFINED
Remediation Level: NOT-DEFINED
Report Confidence: NOT-DEFINED
Confidentiality Requirement: MEDIUM
Integrity Requirement: NOT-DEFINED
Availability Requirement: NOT-DEFINED
```

The expert did ask questions, for example, what software Matthew works with, to quantify the *Confidentiality Requirement* parameter (see Table 8), and the result of CVSS score was calculated as 5.

In the second evaluation, we gave the evaluators the information chain, along with the value of the data and its effect on organizational indicators, as shown in Figure 21. As mentioned, Matthew works with two software: *financial system* and *insurance system*. The financial system on this computer involves four security data. Moreover, the insurance system involves other data. As seen in Figure 21, he can expose three data. Disclosure of information can damage many of the indicators, especially the reputation of the organization. Based on this information, the first evaluator changed their decision to set confidentiality parameter:

```
Confidentiality Requirement: HIGH
```

The value of risk severity changed from 5 to 6.8.

In the following, we illustrate the calculation of the risk

TABLE 11: Security data owned by each user

User	Data
Matthew	Patient Card Number (I) — Disabled Person Card Number (I) Disabled Confirmed (C,I) — Approved Consulting Fee (C) Unapproved Consulting Fee (C)
Julien	Blocked Person Information (C,I) — Blocked Card Information (C,I) New Card Information (C,I)
Benjamin	Requested Goods Information (I)
Lucas	Requested New Goods (I) — Registered New Goods (I)
Oliver	Accepted Goods Information (I)
Jack	Submitted Medical Information (C,I) — Received Medical Information (C,I)
John	Disabled Unapproved (I)

severity based on OWASP method for "Session Fixation" vulnerability in the financial system. Session fixation is a web attack technique where an attacker is able to trick a victim into using a Session ID which is previously known to him. Let us see how the first evaluator quantifies the parameters of OWASP method without knowledge of the security data available in the financial system:

```
Asset: Financial System
Vulnerability: Session Fixation
Threat: Hijacking the user-validated session
Risk Severity: 2.7

Setting the parameters of OWASP method
=====================================

Threat Agent Factors:
---------------------
Skills required: NETWORK AND PROGRAMMING SKILLS
Motive: HIGH REWARD
Opportunity: SOME ACCESS OR RESOURCES REQUIRED
Population Size: AUTHENTICATED USERS

Vulnerability Factors:
----------------------
Easy of Discovery: EASY
Ease of Exploit: EASY
Awareness: PUBLIC KNOWLEDGE
Intrusion Detection: NOT LOGGED

Technical Impact Factors:
-------------------------
Loss of Confidentiality: EXTENSIVE NON-SENSITIVE DATA DISCLOSED
Loss of Integrity: MINIMAL SLIGHTLY CORRUPT DATA
Loss of Availability: NOT APPLICABLE
Loss of Accountability: ATTACK COMPLETELY ANONYMOUS

Business Impact Factors:
------------------------
Financial Damage: SIGNIFICANT EFFECT ON ANNUAL PROFIT
Reputation Damage: MINIMAL DAMAGE
Non-Compliance: MINOR VIOLATION
Privacy violation: HUNDREDS OF PEOPLE
```

Matthew is a user who works in the financial department with the financial system. If an attacker gets access to it, he can access important security data, as shown in Figure 21. The integrity of three data can be compromised and three data can be disclosed. As discussed in the extraction of fear stories of the organization, the non-disclosure of the organization's consultations and even the personal information of the consultant was one of the security concerns. On the other hand, the lack of disclosure of the illnesses of the employees of the organization was also a major concern. Knowing these, the first evaluator quantified the following two parameters in a different way:

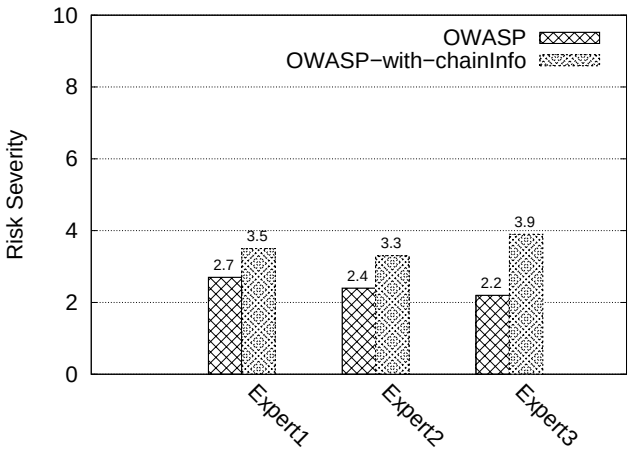

Fig. 22: Comparison of risk severity calculation with OWASP method in two cases 1) without knowledge of the security data of the organization, and 2) with knowledge of the security data available in the financial system

```
Loss of Confidentiality: EXTENSIVE CRITICAL DATA DISCLOSED
Loss of Integrity: EXTENSIVE SLIGHTLY CORRUPT DATA
```

Although the evaluator could better quantify the financial damage parameter by knowing this information, but since the financial system is being evaluated, the evaluator initially considered it almost the highest option and did not change it. In terms of the organizational reputation degradation parameter, since two security data (see Figure 21) influenced the reputation of the organization, a better option was chosen:

```
Reputation Damage: LOSS OF GOODWILL
```

The value of risk severity changed from 2.7 to 3.5 after changing the value of three parameters. Figure 22 shows the results of three security experts' assessment of financial system risk in two ways, without the knowledge and knowledge of the organization's security data available in the financial system.

5 Conclusion

Analyzing security risks and selecting the right security controls in organizations is one of the most important security challenges. Risk assessment can be done at various levels, including assets or business processes. We believe that we need to go beyond the business processes and extract the hidden security data in the process activities. In fact, our assets, which we need to focus on, are the organization's security data, which separates one organization from others. We mean that assets are not the primary wealth of organizations, but the content of business processes, which are security data, should be the primary focus of security professionals.

The main purpose of this paper is to extract the security data and then connect them to logical, physical and human assets according to the concept of data life cycle. The data life cycle means where the data is created, where it is edited, processed, where it is transmitted, where it is displayed, and where it will eventually be stored. The model presented in this paper will improve the accuracy of well-known risk assessment methods such as CVSS, OWASP, and DREAD.

REFERENCES

[1] M. Gerber and R. von Solms, "From Risk Analysis to Security Requirements," Computers & Security, vol. 20, no. 7, pp. 577-584, 2001.

[2] M. Weske, "Business Process Management - Concepts, Languages, Architectures, 2nd Edition," Springer Berlin Heidelberg, 2012.

[3] ISO, "ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management," Online: https://www.iso.org/standard/75281.html, 2018.

[4] W. C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," 2003.

[5] S. Taubenberger and J. Jurjens, "IT Security Risk Analysis based on Business Process Models enhanced with Security Requirements," pp. 1-10, 2008.

[6] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," Computers & Security, vol. 88, p.101640, 2020.

[7] Trend Micro, "Business Process Compromise (BPC)," 2017.

[8] T. Peltier, "Information security fundamentals," 2013.

[9] T. Peltier, "Information security risk analysis," 2010.

[10] K. Khanmohammadi and S. H. Houmb, "Business process-based information security risk assessment," In 2010 Fourth international conference on network and system security, pp. 199-206, 2010.

[11] W. Labda, N. Mehandjiev, and P. Sampaio, "Modeling of privacy-aware business processes in BPMN to protect personal data," In Proceedings of the 29th Annual ACM Symposium on Applied Computing, pp. 1399-1405, 2014.

[12] P. T. Figueira, C. L. Bravo, and J. L. R. López, "Improving information security risk analysis by including threat-occurrence predictive models," Computers & Security, vol. 88, p.101609, 2020.

[13] M. Eckhart, B. Brenner, A. Ekelhart, and E. Weippl, "Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges," Journal of Internet Services and Information Security (JISIS), vol. 9, no. 3, pp.52-73, 2019.

[14] R. Bojanc and B. Jerman-Blazic, "Towards a standard approach for quantifying an ICT security investment," Comput. Stand. Interfaces, vol. 30, no. 4, pp. 216-222, 2008.

[15] B. B. Madan, K. Gogeva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "Modeling and quantification of security attributes of software systems," In Proceedings International Conference on Dependable Systems and Networks, pp. 505-514, 2002.

[16] S. H. Houmb and K. Sallhammar, "Modeling System Integrity Of A Security CriticalSystem Using Colored Petri Nets," WIT Trans. Built Environ., vol. 82, 2005.

[17] P. Shedden, W. Smith, and A. Ahmad, "Information Security Risk Assessment: Towards a Business Practice Perspective," 8th Aust. Inf. Secur. Manag. Conf. Proc., pp. 555-590, 2010.

[18] C. Schmitz and S. Pape, "LiSRA: Lightweight Security Risk Assessment for decision support in information security," Computers & Security, vol. 90, p.101656, 2020.

[19] Y. Peng, K. Huang, W. Tu, and C. Zhou, "A model-data integrated cyber security risk assessment method for industrial control systems," In 2018 IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS), pp. 344-349, 2018.

[20] G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives," Inf. Syst. J., vol. 11, no. 2, pp. 127-153, 2001.

[21] P. Klempt, H. Schmidpeter, S. Sowa, and L. Tsinas, "Business Oriented Information Security Management–A Layered Approach," In OTM Confederated International Conferences - On the Move to Meaningful Internet Systems, pp. 1835-1852, 2007.

[22] J. Wang, M. Neil, and N. Fenton, "A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model," Computers & Security, vol. 89, p.101659, 2020.

[23] S. C. Cha and K.H. Yeh, "A data-driven security risk assessment scheme for personal data protection," IEEE Access, pp.50510-50517, 2018.

[24] J. H. Eom, S. H. Park, Y. J. Han, and T. M. Chung, "Risk Assessment Method Based on Business Process-Oriented Asset Evaluation for Information System Security," In International Conference on Computational Science, pp. 1024-1031, 2007.

[25] V. M. Belov, A. I. Pestunov, and T. M. Pestunova, "On the Issue of Information Security Risks Assessment of Business Processes," In 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), pp. 136-139, 2018.

[26] X. Su, D. Bolson, and P. van Eck, "A Business Goal Driven Approach for Information Security Requirements," in Proceedings of the 13th Workshop on Exploring Modeling Methods for Systems Analysis and Design (EMMSAD 2007), held in conjunction with the Held in conjunction with CAiSE'08 The 20th International Conference on Advanced Information Systems Engineering, pp. 465-472, 2008.

[27] E. W. Cope, J. M. Kuster, D. Etzweiler, L. A. Deleris, and B. Ray, "Incorporating risk into business process models," IBM Journal of Research and Development, vol. 54, no. 3, pp. 1-13, 2010.

[28] G. Michael, A. Pfitzmann, and K. Rannenberg, "Information Technology Security Evaluation Criteria (ITSEC)-a Contribution to Vulnerability?," In IFIP Congress (2), pp. 579-587, 1992.

[29] A. Rodríguez, A. Caro, C. Cappiello, and I. Caballero, "A BPMN extension for including data quality requirements in business process modeling," In International Workshop on Business Process Modeling Notation, pp. 116-125, 2012.

[30] O. Altuhhov, R. Matulevičius, and N. Ahmed, "An Extension of Business Process Model and Notation for Security Risk Management," International Journal of Information System Modeling and Design (IJISMD), vol. 4, no. 4, pp. 93-113, 2013.

[31] J. H. Lambert, R. K. Jennings, and N. N. Joshi, "Integration of risk identification with business process models," Syst. Eng., vol. 9, no. 3, pp. 187-198, 2006.

[32] P. Herrmann and G. Herrmann, "Security requirement analysis of business processes," Electronic Commerce Research, vol. 6, no. 3-4, pp. 305-335, 2006.

[33] D. Olifer, N. Goranin, J. Janulevicius, A. Kaceniauskas, and A. Cenys, "Improvement of security costs evaluation process by using data automatically captured from BPMN and EPC models," In International Conference on Business Process Management, pp. 698-709, 2017.

[34] J. Jurjens, "Umlsec: Extending uml for secure systems development," in UML 2002 - The Unified Modeling Language (J.-M. Jézéquel, H. Hussmann, and S. Cook, eds.), (Berlin, Heidelberg), pp. 412-425, 2002.

[35] I. Soomro and N. Ahmed, "Towards security risk-oriented misuse cases," International Conference on Business Process Management, vol. 132, pp. 689-700, 2013.

[36] A. Manna, A. Sengupta, and C. Mazumdar, "A Quantitative Methodology for Business Process-Based Data Privacy Risk Computation," In Advanced Computing and Systems for Security, pp. 17-33, 2020.

[37] N. Nagaratnam, A. Nadalin, M. Hondo, M. McIntosh, and P. Austel, "Business-driven application security: From Modeling to Managing Secure Applications," IBM Systems Journal, vol. 44, no. 4, 2005.

[38] M. Menzel, I. Thomas, and C. Meinel, "Security requirements specification in service-oriented business process management," International Conference on Availability, Reliability and Security, pp. 41-48, 2009.

[39] B. Xue, R. Krishnan, R. Padman, and H. J. Wang, "On risk management with information flows in business processes," Information Systems Research, pp. 1-19, 2012.

[40] A. J. Varela-Vaca, L. Parody, R. M. Gasca, and M. T. Gomez-Lopez, "Automatic Verification and Diagnosis of Security Risk Assessments in Business Process Models," IEEE Access, vol. 7, pp. 26448-26465, 2019.

[41] C. L. Maines, D. Llewellyn-Jones, S. Tang, and B. Zhou, "A cyber security ontology for BPMN-security extensions," In 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 1756-1763, 2015.

[42] R. Saluja, S. K. Singh, and A. K. Chaturvedi, "Security checking in ABPMN," In 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 449-454, 2016.

[43] C. C. Lo and W. J. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls," Expert Systems with Applications, vol. 39, no. 1, pp. 247-257, 2012.

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

[45] P. Shedden, A. Ahmad, W. Smith, H. Tscherning, and R. Scheepers, "Asset identification in information security risk assessment: A business practice approach," Communications of the Association for Information Systems, vol. 39, no. 1, p.15, 2016.

[46] O. Altuhhova, R. Matulevicius, and N. Ahmed, "Towards definition of secure business processes," Lect. Notes Bus. Inf. Process., vol. 112, pp. 1-15, 2012.

[47] A. Shameli-Sendi, M. Jabbarifar, M. Shajari, and M. Dagenais, "FEMRA: Fuzzy Expert Model for Risk Assessment," in 2010 Fifth International Conference on Internet Monitoring and Protection, pp. 48-53, 2010.

[48] B. Karabacak and I. Sogukpinar, "ISRAM: Information security risk analysis method," Computers & Security, vol. 24, no. 2, pp. 147-159, 2005.

[49] S. A. Kokolakis, A. J. Demopoulos, and E. A. Kiountouzis, "The use of business process modelling in information systems security analysis and design," Inf. Manag. Computers & Security, vol. 8, no. 3, pp. 107-116, 2000.
[50] N. Ahmed and R. Matulevicius, "Securing business processes using security risk-oriented patterns," Computer Standards & Interfaces, vol. 36, no. 4, pp. 723-733, 2014.
[51] S. Taubenberger, J. Jurjens, Y. Yu, and B. Nuseibeh, "Resolving vulnerability identification errors using security requirements on business process models," Information Management & Computer Security, vol. 21, no. 3, pp. 202-223, 2013.

Alireza Shameli-Sendi is currently an Assistant Professor at Shahid Beheshti University. Before joining SBU, he was a Postdoctoral Fellow at Ericsson, Canada and Postdoctoral at ETS and McGill universities in collaboration with Ericsson. He received his Ph.D. degree in computer engineering from Ecole Polytechnique de Montreal, Canada. He obtained his B.Sc. and M.Sc. from Amirkabir University of Technology. His primary research interests include information security, intrusion response system, and cloud computing. He is a recipient of the Postdoctoral Research Fellowship Award and Industrial Postdoctoral Fellowship Award from Canada. In addition, he received the best researcher award, in industrial track, at SBU, in 2018.