Baltic J. Modern Computing, Vol. 8 (2020), No. 2, pp. 213–240
https://doi.org/10.22364/bjmc.2020.8.2.02

Security Risk Management in E-commerce Systems: A Threat-driven Approach

Abasi-amefon O. AFFIA[1], Raimundas MATULEVIČIUS[1], Alexander NOLTE[1,2]

[1] Institute of Computer Science, University of Tartu, Tartu, Estonia
[2] Institute for Software Research, Carnegie Mellon University, Pittsburgh, PA, USA
{amefon.affia, raimundas matulevicius, alexander.nolte}@ut.ee

Abstract. E-commerce has transformed the commerce industry as we know it, introducing better purchasing, shipping, and customer services. These business services generate and utilise sensitive information such as customer purchases, financial and personal information which are of high value to attackers. Securing e-commerce systems demands security risk management conscious of evolving security threats. This research work proposes and analyses a threat-driven approach that explores the use of a security threat analysis method – STRIDE to support a selected security risk management method – ISSRM (Information System Security Risk Management) in managing security risk in an e-commerce system. Results of this approach present e-commerce asset identification, threat analysis, and risk identification, with security risk treatment decisions. We discuss these results presenting the benefits of the STRIDE and ISSRM combination.

Keywords: E-commerce, Security Risk Management, Information System Security Risk Management, ISSRM, STRIDE.

1 Introduction

E-commerce refers to all types of electronic transactions between parties whether they are financial transactions or non-financial exchanges of information or other services (Chaffey et al., 2019). Such information exchange occurs between the customer, business and/or government depending on the e-commerce type (Korper and Ellis, 2000), (Chaffey et al., 2019). The e-commerce system consists of components (software, hardware, processes, services, and interactions with third-party systems) that effect the generation, dissemination and manipulation of financial information to provide commercial transactions and services over the internet. Such information includes financial, product, customer or order information enabling core processes of the system (Korper and Ellis, 2000), (Chaffey et al., 2019).

The e-commerce industry has suffered a number of major security breaches in recent years as seen in attacks such as the Target attack in 2013 (2013) and Ebay attack (2014) where millions of accounts were affected making it the biggest cyber-crime incidents in both years. In 2018, a number of e-commerce sites including large retailers Adidas (2018) and Macy's Inc.(2018) suffered security breaches of their e-commerce sites (Green and Hanbury, 2018). Impacts of these security breaches included identity theft as a result of the loss of customer personal and financial information, monetary loss for both the business owner and customer, loss of customer trust in e-commerce usage and loss of company reputation (Breach Level Index, 2019). To prevent such security breaches, security threat analysis, and security risk management is performed (Matulevičius, 2017). Security threat analysis targets threats to systems that take advantage of existing vulnerabilities to cause malicious impact. These security threats cause security risks in a system and require management.

We thus focus on the following research question: *How can we support security risk management with a targeted approach for security threat analysis*? To answer this question, a threat-driven approach is proposed. This approach uses a security threat analysis method (MSDN, 2009) to support a selected security risk management method (Dubois et al., 2010). This combination creates an iterative threat-driven approach producing (assets, risks, risk treatment, and risk estimation) components important for security risk management in e-commerce systems.

The remainder of the paper is structured as follows: in Section 2 we provide an overview of security methods used, the proposed threat-driven approach and other related approaches in research. In Section 3 we present the research design. Section 4 illustrates the results of the threat-driven approach. Section 5 discusses the application and results of the threat-driven approach. Finally, section 6 provides summary of the research work, answer to research questions and directions for future work.

2 Background

In this section we provide an overview of security risk methods, security threat analysis methods, providing the rationale behind the combination of the security risk management method and security threat analysis approach.

2.1 Approaches for security risk management

Security risk management approaches are developed from a range of general standards (Radack, 2011, Stoneburner et al., 2002) and methods in literature (Janulevičius, 2016), (Chancellery, 2004), (Li and Horkof2014), (Fredriksen et al.,2002), (Alberts et al., 2003), (Farquhar, 1991), (DCSSI Advisory Office, 2004), (De Risques, 2007). Table 1 lists popular security risk management methods that have been analysed in research. Other security risk management methods are analysed in (Janulevičius, 2016).

We select four (4) methods (Lund et al., 2011), (Alberts et al., 2003), (Dubois et al., 2010), and (Dalpiaz et al., 2016) because these have illustrative examples to solve security risk management questions within the e-commerce domain.

Table 1. Security risk management methods

ID	Method	Sources
1	Information Systems Security Risk Management (ISSRM)	(Dubois et al., 2010)
2	Austrian IT Security Handbook	(Chancellery, 2004)
3	IT- Grundschutz	(BSI Standard, 2008)
4	Socio-Technical Systems (STS) Method	(Dalpiaz et al., 2016), (Li and Horkoff, 2014), (Paja et al., 2013)
5	CORAS	(Fredriksen et al., 2002)
6	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)	(Alberts et al., 2003)
7	CCTA Risk Analysis and Management Method (CRAMM)	(Farquhar, 1991)
8	Expression of Needs and Identification of Security Objectives (EBIOS)	(DCSSI Advisory Office, 2004)
9	MEthod for Harmonised Analysis of RIsk (MEHARI)	(De Risques, 2007)

1. **CORAS** is a model-driven method for defensive risk analysis of security critical systems using a tool-supported modelling language to model risks (Lund et al., 2011). The CORAS method contains eight steps; (1) preparation for the analysis, (2) customer presentation of the targets, (3) refining of the target description using asset diagrams, (4) approval of the target description, (5) risk identification using threat diagrams, (6) risk estimation using threat diagrams, (7) risk evaluation using risk diagrams and (8) risk treatment using treatment diagrams. CORAS is considered relevant to manage cyber-security risks in e-commerce domain (Stølen, 2001), (Raptis et al., 2002).
2. **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation Method)** is a risk-based strategic assessment and planning technique for security risk management (Alberts et al., 2003). The method aims at examining organisational and technological issues as well as defining an organisation's security strategy and plan. The risk management approach follows three components: (1) identification of asset and threat scenarios, (2) identification of vulnerabilities of major assets, and (3) risk assessment and developing security strategies. OCTAVE has been used to manage security risks in the e-commerce domain specifically related to e-procurement solutions (Stephens and Valverde, 2013).
3. **ISSRM (Information System Security Risk Management)** and its domain model is a practitioner-oriented methodological tool, focused on supporting organisations to make decisions related to the security of Information Systems (Dubois et al., 2010). An application of the ISSRM method comprises of following six steps; (1) organisational context and assets identification; (2) determination of security objectives (confidentiality, integrity and availability); (3) risk analysis and assessment; (4) risk treatment decision which results to, (5) security requirements definition to implement, and (6) security controls. The *domain model* is an important artifact of the ISSRM method that introduces asset, risk, and risk treatment related concepts.

ISSRM can be used to manage security risks in the e-commerce domain (Affia, 2018) as well as other domains such as aviation (Matulevičius et al., 2016).

4. **STS (Socio-technical Systems) Method** (Dalpiaz et al., 2016), (Li and Horkoff, 2014), (Paja et al., 2013) for security analysis seeks to tackle security risks by proposing a three-layer security analysis framework of business processes, applications and physical infrastructure based on the following steps; (1) business layer security analysis of stakeholder high-level security needs, (2) application layer security analysis of security-enhanced business goals, and (3) physical layer security analysis of security-enhanced application goals. The approach defines, refines and propagates high-level security requirements into the different layers of socio-technical systems. This has been used in an e-commerce use-case to analyse security risks (Paja et al., 2012).

The described security risk management methods are compared in Table 2 to select a method suitable for the analysis of the threat-driven approach. The comparison follows a set of criteria forming important components in a security risk management process – asset, risk, risk treatment, and risk estimation.

1. **Asset**: An asset is anything that is valuable and contributes to accomplishing the organisation's goals. Critical assets of a system are to be identified and protected within the security risk management process. The ISSRM method recognises the need for asset identification (following its domain model) and illustration using security risk-oriented secure modelling languages (e.g., (Bresciani et al., 2004), (OMG, 2011), (Sindre, 2007), (Sindre and Opdahl, 2005)). OCTAVE recognises this need as well (Alberts et al., 2003), but gives less guidance on this process than ISSRM. The CORAS method also includes asset identification and illustration after prior preparations including customer targets. Finally, the STS method recognises asset identification, focusing on deriving high-level security needs of the stakeholders (Dalpiaz et al., 2016).
2. **Risk**: Identifying risk is a key aspect of any security risk management procedure. The ISSRM method supports risk analysis using its domain model. The domain model analyses vulnerabilities to deduce threats and produce an impact analysis of the resulting risks represented as risk statements and models. OCTAVE identifies threat scenarios and asset vulnerabilities before assessing risks, representing risks in risk statements (Alberts et al., 2003). CORAS identifies threats using threat diagrams and derives risk evaluations from risk diagrams. The STS method supports modelling of threats based on derived security needs, with the assumption that threats exploit a (social or technical) vulnerability (Dalpiaz et al., 2016).
3. **Risk Treatment**: For risk management, each identified risk has to go through a risk treatment procedure. This procedure is recognised by all four aforementioned risk management methods but to varying degrees. The ISSRM method not only considers the risk decision to be taken but also considers the implementation of countermeasures to mitigate risks (Dubois et al., 2010). CORAS uses treatment diagrams to illustrate risk treatment activities. OCTAVE introduces security strategies to deal with the security risks (Alberts et al., 2003). STS method analyses security requirements and control/countermeasure selections for risk mitigation (Dalpiaz et al., 2016).

4. **Risk Estimations**: Risk estimations in risk management allows for stakeholders to make decisions on risk mitigation. As the resources available may not be sufficient to treat risk simultaneously, a cost-benefit estimation is useful to decide which risks to treat first. ISSRM method provides an avenue for estimations on cost benefits for risk treatment (Dubois et al., 2010). CORAS provides some cost-benefit analysis and estimations from these risk diagrams for risk treatment. OCTAVE and the STS method does not provide concrete estimations as regard risk treatment (Alberts et al., 2003), (Dalpiaz et al., 2016).

Table 2. Criteria for comparing different security risk management methods.

Criteria	ISSRM	OCTAVE	CORAS	STS
Asset	+ +	+ +	+ +	+ -
Risk	+ +	+ -	+ -	+ -
Risk Treatment	+ +	+ -	+ +	+ -
Risk Estimations	+ +	- -	+ +	- -

*++ denotes full fulfillment, +- denotes partial fulfillment, and - - denotes no fulfillment of the respective criterion

Table 2 summarises the method comparison with varying degrees of the fulfillment of each criterion. Based on this analysis we consider ISSRM to meet all considered criteria with full satisfaction and will thus use it as a basis for our case study.

2.2 Information Systems Security Risk Management (ISSRM)

The domain model (Dubois et al., 2010) (Figure 1) for information security risk management consists of three major concept groups: asset-related concepts, risk-related concepts, and risk treatment-related concepts.

1. **Asset-related** concepts describe system assets and business assets to protect and security criteria to guarantee a certain level of asset security. The *business asset* is defined as information, data, and processes that bring value to an organisation. *System/IS assets* are assets that support *business assets*. *Security criteria* (of confidentiality, integrity, and availability) are constraints on business assets that define the security needs presented by stakeholders.
2. **Risk-related** concepts present risk definitions and their components (threats, vulnerability, event and impact). A security *risk* is a combination of a security *event* and its *impact* (negation of the security criterion) harming business and IS assets. An event occurs when *threat* exploits an existing *vulnerability*. A *vulnerability* is a characteristic of system assets, constituting its weakness. A *threat* targets system assets by exploiting their vulnerability.
3. **Risk-treatment** related concepts depict concepts to treat risk. Risk treatment decisions might include risk reduction, risk avoidance, risk transfer, or risk acceptance. *Security requirements* define conditions to be reached by mitigating identified security risks and *controls* implement the defined security requirements. ISSRM also

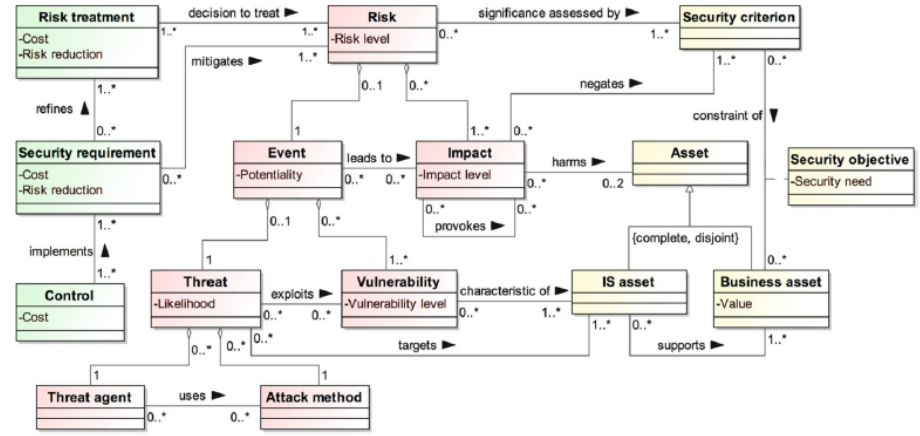

Fig. 1. ISSRM Domain Model, adapted from (Dubois et al., 2010), (Matulevičius, 2017)

proposes the use of metrics in *risk estimation* for risk treatment decisions. Risk estimations can be derived from business assets, threat and vulnerability values, risk reduction, and countermeasure cost (Dubois et al., 2010).

Although ISSRM does not define a concrete language to be applied on its process (see Figure 2), it presents an advantage of being flexible to security-oriented modelling languages (Bresciani et al., 2004), (OMG, 2011), (Sindre, 2007), (Sindre and Opdahl, 2005).

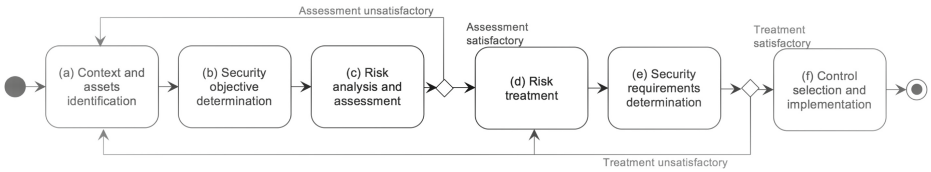

Fig. 2. ISSRM process (Dubois et al., 2010), (Matulevičius, 2017)

2.3 Security threat analysis methods

In the following we will provide an overview of various security threat analysis methods (Shostack, 2014), (CAPEC, 2019), (Wichers, 2013), (Uzunov and Fernandez, 2014), (Ahmed and Matulevičius, 2014), (Sindre and Opdahl, 2001).

1. **STRIDE** stands for **S**poofing – pretending to be something you are not or someone you are not, **T**ampering – modifying something that you are not supposed to modify, **R**epudiation – claiming you didn't do something (regardless of if this is true or

not), **I**nformation disclosure – exposing information to those who are not authorised to view it, **D**enial of service – attacks that are designed to prevent a system from providing its intended service, and **E**levation of privilege – when a program or user can to do things (technically) that they're not supposed to be able to do. These are designed to help software builders identify software attacks. Each of the aforementioned threat-specific section provides a deeper explanation of threats including its violated security requirement.

2. **Misuse cases** or abuse cases(Sindre and Opdahl, 2001) are use cases with a focus on the attacker's actions. Misuse cases have textual representations and diagram representations, to elicit security threats but they do not provide methodological guidance to discover additional threats and focus more on user-level and organisational threats (Deng et al., 2011), (Sindre and Opdahl, 2001).
3. **Attack trees** provide a formal and methodical way of describing the security of systems based on various attacks that could possibly occur. A tree structure is used to represent attacks against a system. First, the attack goals are identified. Each goal forms a tree and is represented in the root node. Then all possible attacks against each goal are formed and repeatedly added down the tree as sub-goals represented as leaf nodes. Children of each leaf nodes represent ways to achieve a superseding sub-goal. A technique to model potential attack paths is the use of Bayesian networks (Liu and Man, 2005). This approach allows the construction of attack trees by enumerating all potential attack paths thereby providing a more compact representation of attack paths than the conventional methods (Liu and Man, 2005).
4. **Attack Libraries** provide a more detailed list of common problems. A library can be created by collecting sets of attack tools; either proof of concept code of fully developed and/or weaponised exploit code that helps to understand attacks. In such collections, there are no modelling or abstraction considerations. Any security expert using an attack library needs to spend resources to create a model from the attacks for analysis. Attack libraries thus provide a lower abstraction to threats and more details for threat analysis. Two common attack libraries are MITRE's CAPEC (CAPEC, 2019) (Common Attack Pattern Enumeration and Classification) – a highly structured set of attack patterns organised into groups, and OWASP Top Ten (Wichers, 2013) – offering top ten risks specific to web applications covering threat agents, attack vectors, security weaknesses, technical and business impacts.
5. **Security Threat Patterns** follow security patterns (Schumacher et al., 2013) to describe particular recurring security threats within a specific security context to classify a wide variety of threats. Two security threat pattern examples are the taxonomy of security threats for distributed systems (Uzunov and Fernandez, 2014) and security risk-oriented patterns (SRP) (Ahmed and Matulevičius, 2014). The security threat taxonomy for distributed systems consists of eight classes of system threats (identity attacks, network communication attacks, network protocol attacks, passing illegal data attacks, stored data attacks, remote information inference, loss of accountability, and uncontrolled operations) and four classes of threats to the security of the system infrastructure (cryptographic attacks, countermeasure attacks, configuration/administration attacks, and network protocol attacks) (Uzunov and Fernandez, 2014). Security risk-oriented patterns (SRP) are based on the understanding of security risks (i.e., recurring security problems) that arise within busi-

ness processes (i.e., specific security context) (Ahmed and Matulevičius, 2014). SRPs are characterised into 5 patterns that secures data from unauthorised access, data transmission between business entities, business activity after data submission, business services against distributed denial of service (DDoS) attacks, and storage of data and data retrieval from storage.

We compared the described security threat analysis methods to select the method suitable for the threat-driven approach. The comparison follows a set of criteria needed to fully support risk management process – threat categorisation, security need, and countermeasure suggestion.

Attack libraries are a collection of attack types with each library offering some countermeasure suggestion to treat the identified threat but with no abstraction/ categorisation or security need considerations. Attack trees build attacks based on goals illustrating the security need of the assets in analysis but do not consider threat categorisation or countermeasure suggestions for the threat. Security patterns provide recurring patterns, expresses the security need of the assets during analysis, and provides some countermeasure suggestions for the identified security threat but do not provide categorisation for security threats. However, STRIDE allows for a defined threat categorisation within its mnemonic, illustrates the security need of assets during its analysis, and can propose countermeasures within an analysis of its mnemonic.

STRIDE fulfilled these requirements with the possibility to be complemented with the strengths of other security threat analysis.

2.4 STRIDE

STRIDE is an industrial-level method used for threat scenario elicitation and analysis (Howard and Lipner, 2006). For this research, STRIDE was selected as the security threat analysis method to be used further in this paper due to its industry usage, its maturity as well as its high research concentration and use within the security community, making it beneficial for security risk management. STRIDE allows model and abstraction considerations to analyse system elements such as data flows, data stores, processes, and external entities (users, external services, etc). The STRIDE threat taxonomy identifies security threat types within represented elements. STRIDE's acronym for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege forms its taxonomy. These threats are the negation of the main security properties a system should have. These are;

- Spoofing - *Authentication*
- Tampering - *Integrity*
- Repudiation - *Non-repudiation*
- Information Disclosure - *Confidentiality*
- Denial of Service - *Availability*
- Elevation of privilege - *Authorisation*

Each element within the system representation is assigned to a set of susceptible threat within the STRIDE taxonomy. A deeper analysis is required to identify which threats within STRIDE are applicable to a specific system. Alongside its benefits in

industrial practice, STRIDE comes with the main advantage of an extensive, reusable knowledge base within its taxonomy.

2.5 Threat-driven Approach

The threat-driven approach (McFarlane and Hills, 2014) centers around the identification of security threats, allocating efforts to protect assets against security threats and their resulting risks, and understand techniques to support these efforts. Threats can damage information systems and organisational assets, and thus should be the primary driver for a well-designed and adequately defended information system (McFarlane and Hills, 2014). Threat-driven approaches have been used in research (Xu and Nygard, 2005), (Xu and Pauli, 2006), (Xu and Nygard,2006) to model, verify and secure software applications. The threat-driven approach proposed in this research work advocates the use of STRIDE in supporting ISSRM efforts, to thus provide a comprehensive view of the threat landscape while managing the resulting risks. We provide reasons for this combination.

1. **Threat modelling**: The application of STRIDE supports the identification of threats to asset-related concepts. For example, the study of a BPMN model of a system (illustrating its assets) can allow analysts to identify instances where spoofing occurs to carry out a malicious action, or where data or code can be modified (tampering) to thwart business goals. The application of STRIDE for threat identification is reported to be easy to use, produce a significant number of threats for analysis (Yanyan, 2014). The identification of threats does not contradict with threat definitions of the ISSRM method as these threats can be linked to a potential attacker capability, motive and threat action as well as a vulnerability within that system that makes a viable threat. This method is iterative and can be repeated to produce correctly determined security threats.
2. **Threat Categorisation**: STRIDE allows the categorisation of identified threats under each part of its mnemonic. This categorisation is made possible by its distinct parts, properly distinguishing one category from another by definition and by it's mnemonic characters.
3. **Expressing security needs**: Each STRIDE construct represents the opposite of some security properties types a system should have, namely *confidentiality, integrity, availability, authentication, authorisation,* and *non-repudiation*. When considering the impact of the resulting risks, these impacts negate security criteria, a direct constraint of the security needs of the organisation. The identification and mitigation of risks within the STRIDE constructs is one step closer to achieving the security needs of the system. For example, resolving an Information disclosure risk brings the organisation one step closer to achieving the confidentiality of its assets.
4. **Expressing security requirements**: Security requirements enlists the conditions to fulfill to mitigate the risks and secure the system and it's business assets. STRIDE allows the elicitation of security requirements of authentication, integrity, non-repudiation, confidentiality, availability and authorisation, all within the STRIDE constructs. For example, non-repudiation threats can guide the elicitation of authorisation security requirements such as *"the application shall make and store tamper-proof records of information"*.

5. **Countermeasure Suggestion**: As each STRIDE scenario provides security requirements in a system, these requirements can be used to suggest possible countermeasures to mitigate risks. For example, in an elevation of privilege threat where authorisation is the security property concerned, countermeasure suggestions such as the implementation of RBAC (Role-based access control), DAC (Discretionary access control), MAC (Media Access Control), UAC (User Account Control), and privileged account protections (Crowell, 2011) can be proffered to mitigate the security risk.

2.6 Related Approaches

Related approaches exist in research, for the use of threat analysis and risk management methods to secure information systems (Xin and Xiaofang, 2014), (Abomhara et al., 2015), (Guan et al., 2011), (Samarütel et al., 2016). We now review research on single use of threat analysis method, combination of threat analysis methods and the combination of a threat analysis method with a security risk management method.

Researchers have leveraged STRIDE for threat analysis on Telehealth systems (Abomhara et al., 2015) and generic cloud web applications (Guan et al., 2011) to analyse potential threats and secure these information systems. Xin and Xiaofang (2014) use STRIDE combined with threat tree analysis for security analysis and evaluation on online banking system. However, these studies do not consider how to manage the discovered security threats.

Combining threat analysis with security risk management methods ensures an iterative identification and mitigation of security risks for information systems. One example is the combination of security risk oriented patterns (SRP) threat analysis method and ISSRM security risk management (Samarütel et al., 2016) for secure system development in an aviation-turnaround system. These patterns find security risk occurrences in the business process of a system and presents mitigation suggestions for risk patterns. However, the use of SRPs are not without limitations. SRPs are constrained to system business process. As such, system assets that are not represented in the business process are not considered for potential threat and risk analysis. Also, security threats that can be derived from the business process might not be covered by these 5 patterns.

The proposed combination of STRIDE and ISSRM will provide more security threat analysis support benefits including asset and threat coverage using STRIDE. It also caters for the management of the resulting risks using ISSRM. So far there is limited insight into how STRIDE and ISSRM can be combined to carry out a security risk management procedure. In this paper, the combination of these methods is applied to an e-commerce case study.

3 Case Study Design

This section discusses the research questions, research method and a case used to analyse the combination of STRIDE and ISSRM.

3.1 Research Questions

For the purpose of this research work, we propose the following research question: ***How can we support security risk management with a targeted approach for security threat analysis?***

Our efforts to answering this research question will follow ISSRM asset-related, risk-related and risk treatment-related concepts to produce the following sub-research questions:

RQ$_1$. *How can we identify relevant assets for an e-commerce system?*

RQ$_2$. *How can we identify security risks to an e-commerce system?*

RQ$_3$. *How can we carry out risk treatment procedures for an e-commerce system?*

RQ$_4$. *How can we make risk mitigation decisions for the risks discovered?*

3.2 Research method

The research method in Figure 3 illustrates the STRIDE and ISSRM combination through the process of iterative asset identification, risk determination, risk treatment and risk treatment trade-off procedures. The output of each activity is expert evaluated when the activity is complete to determine if the output of each step is satisfactory. Expert evaluation assessments are discussed in Section 3.4.

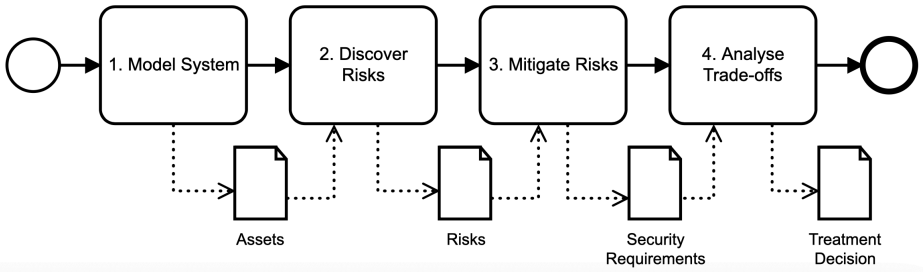

Fig. 3. Applied Threat-driven Approach.

1. **Model System**: This activity defines the system context as the first step in identifying and defining the scope of the risk management process. The outcome of this activity are *Assets* identified and illustrated using an appropriate modelling language.
2. **Discover Risks**: This activity focuses on the discovery of security risks to the e-commerce system payment process. It involves the use of STRIDE to carry out threat analysis on the identified assets in the *Model System* activity. The outcome of this activity are *Risks* developed following ISSRM risk-related concepts.

3. **Mitigate Risks**: This activity demonstrates actions to mitigate the risk scenarios identified in the *Discover Risks* activity. The outcome of this activity are *Security Requirements* to secure the system against the discovered risks.
4. **Analyse Trade-offs**: The required effort for response to risk will likely exceed available resources. Hence, risk trade-off analysis is required. A security metric procedure and the trade-off analysis procedure is introduced to tackle resource management for security risk treatment. This uses metric values of assets from the *Model System* activity, risk reduction levels from the *Discover Risks* activity and cost of implementing countermeasures from the *Mitigate Risks* activity are collected to analyse the trade-offs. The outcome of this activity are *Risk Decisions* to treat risk.

3.3 Case Selection

An e-commerce system comprises of a number of complex processes and interactions which are challenging to completely analyse within this paper. Thus, we have made a targeted selection of the process at the core of e-commerce systems – the order-fulfillment process. The order fulfillment process in Figure 4 consists of a number of

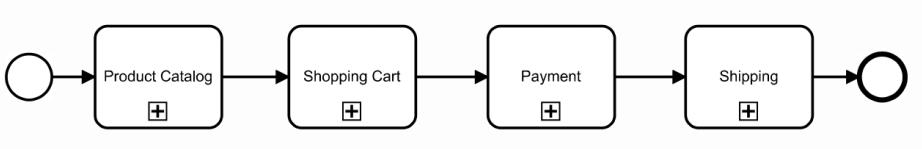

Fig. 4. Value Chain of the Order Fulfillment Process

processes beginning with the *Product Catalog process* to view product, the *Shopping Cart* process to prepare for checkout, the *Payment process* to allow purchase for selected product and the *Shipping process* that delivers product to the Customer, thus, completing the *order*.

The *Payment process* illustrated in Figure 5 is a particularly interesting process in this value chain where sensitive customer, merchant and business information is required to complete transactions. The assets within this process require high security need of confidentiality, integrity and availability. This process provides a substantial attack surface for security threat analysis and risk management and a reasonably complex case study.

3.4 Expert Evaluation

Expert evaluation of the STRIDE and ISSRM combination is carried out as soon as each activity within the threat-driven approach is completed. The experts chosen consists of seven (7) expert participants, purposefully selected based on their experience with software development and management, security risk management, and business process. These experts were IT professionals (2) and those with Business Information technology (5) background (see Table 3).

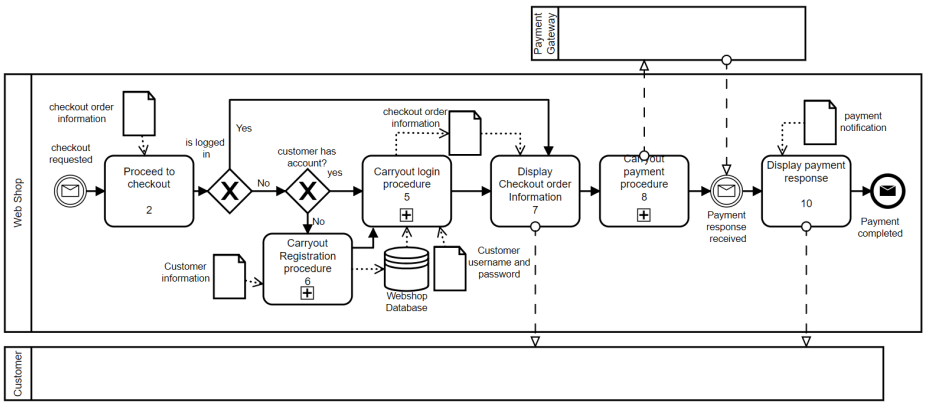

Fig. 5. E-commerce Webshop Payment Process

The experts were invited for a targeted discussion after each activity of the research method was completed to evaluate the process and the results. The evaluation is based on the correctness of model illustrations, relevance of the research method activities and the benefit of the STRIDE and ISSRM combination. At the end of each evaluation iteration, the results of each activity were found to be satisfactory.

4 Results

This section describes the results of our analysis, demonstrating the viability of combining STRIDE and ISSRM on the Payment process of an e-commerce Webshop to discover and mitigate threats.

4.1 RQ1 Assets

The payment process in Figure 5 is supported by a number of system assets and processes. This support includes the *Webshop* e-commerce application. This application consists of a *Server* that processes requests i.e login or checkout requests. For login requests, the Webshop uses its *Carryout login process* (see Figure 6) where *Customer username and password* as a business asset is provided to the Webshop (system asset) through its Login Interface(system asset) to authenticate and authorise the Customer before continuing the payment process.

Table 3. Expert Background

ID	Position	Background	Field experience
1	QA Team Lead	10+ years Software development and Testing (including 2years experience with e-commerce related software development)	IT professional
2	Development Team Lead	10+ years experience in Software development (including 3years experience with e-commerce related software development)	IT professional
3	Director of Cyber-security	26+ years in IT governance and business IT related roles	IT professional and Business Information Technology
4	Team Lead for Security Operations Centre	20+ years experience in IT governance and business IT related roles	IT professional and Business Information Technology
5	Cyber-security engineer	7+ years experience including Business IT governance and e-commerce related software development	IT professional and Business Information Technology
6	Cyber-security engineer	7+ years experience including Business IT and IT Infrastructure management	IT professional and Business Information Technology
7	Technical product specialist	4+ years IT experience including business process management research	IT professional and Business Information Technology

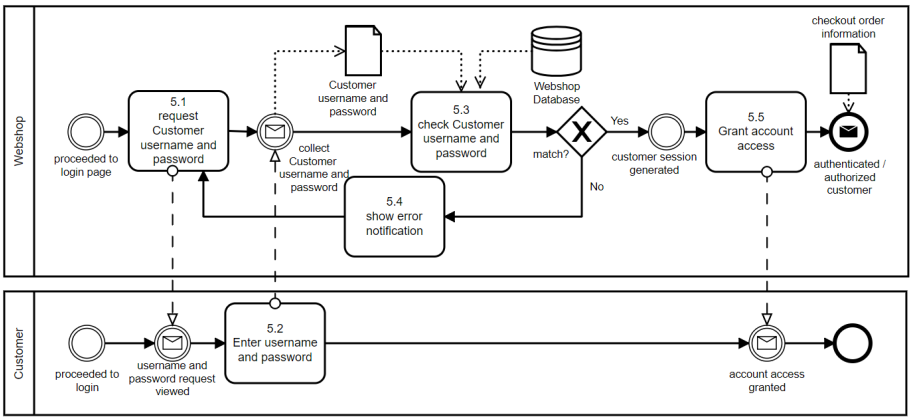

Fig. 6. E-commerce Webshop Carryout login process

Following the above description, the business assets and their supporting system assets for the case study is elicited from its business process and described in Table 4. After this activity was completed, experts evaluated the correctness of the BPMN models used to represent the assets and the quality of the assets discovered. The experts found BPMN to be an appropriate modelling language for the elicitation of assets for the payment process.The final outputs of this activity are the business and system assets as illustrated in Table 4.

Table 4. Assets in Payment Process.

System Assets	Supported Business Assets
Webshop Login Interface, Customer, Webshop Database	Carryout login procedure, Username and Password, Customer Information
Webshop Server, Webshop, Customer	Webshop Checkout Service, Checkout Order Information
Webshop Server, Customer	Customer SessionID
Webshop Database, Webshop Server	Webshop Server Logs

4.2 RQ2 Risks

The carryout login process within the payment process is used for security risk analysis. Security threats result from the existence of threat agents, and vulnerabilities in system assets. Some system assets are selected to be analysed. This includes the Webshop Login Interface, Webshop Server and Webshop to demonstrate the threat-driven approach. We used the CWE vulnerability database (CWE, 2020) to identify potential vulnerabilities of the considered system assets (see Table 4). These vulnerabilities are described in Table 5.

Table 5. Vulnerabilities of identified System Assets.

System Asset	Potential Vulnerabilities	CWE2020
Webshop Login Interface	Lack of Input Validation of Webshop Login Interface	CWE-20
Webshop Server	Improper Output Neutralisation for Webshop server logs	CWE-117
	Improper Order-checking Logic of the WebShop Server	CWE-285
	Allocation of Resources Without Limits or Throttling in Webshop Server	CWE-770
Webshop	Weak password based authentication on Webshop	CWE-521

To scope our risk analysis, we do not analyse all possible threats to an e-commerce system, but elicit one threat per STRIDE category for the vulnerable system assets in Table 6. Here, ST is Spoofing threat, TT is Tampering threat, RT is Repudiation threat, IT is Information disclosure threat, DT is Denial of service threat, and ET is Elevation of privilege threat.

Each STRIDE threat developed, and its corresponding vulnerability (V) from Table 5, follows the ISSRM risk-related concepts to derive the threat impact, in the event of a successful vulnerability exploitation (see Table 6 – column 2). From this impact analysis, we develop the security risk scenario. Table 6 – column 3 illustrates security risks where SR is Spoofing Risk, TR is Tampering Risk, RR is Repudiation Risk, IR is Information disclosure Risk, DR is Denial of service Risk, and ER is Elevation of privilege Risk. This risk analysis follows the ISSRM domain model (see Figure 1) where a security *threat* triggers 0..1 security *event* (instantiated in an impact analysis), and a security *event* triggers 0..1 security *risk* leading to a one-to-one relationship between

threats in the “Impact analysis” column and security risks in the “Security risk” column in Table 6[1].

Table 6: Risk Impact analysis of STRIDE elicited threats and its Security Requirements.

Threat type	Impact Analysis	Security Risk	Security Requirements
S	ST1: An attacker compares valid sessionIDs provided by Webshop and brute forces to access a valid Customer session. V: Weak sessionID generation of Webshop Server. Impact: Loss of Confidentiality of Customer sessionID.	SR1: An attacker compares valid sessionIDs and brute forces to access a valid Customer session, exploiting the weak sessionID generated by Webshop Server leading to loss of confidentiality of Customer sessionID.	SR1.SReq1: The Webshop Server sessionID generation algorithm should be brute proof. SR1.SReq2: The Webshop shall not permit duplicate con-current user sessions, originating from different machines.
T	TT1: An attacker modifies Webshop JavaScript code to modify Checkout Order Information by exploiting the Improper Order-checking Logic of the WebShop Server. V: Improper Order-checking Logic of the WebShop Server. Impact: Loss of Integrity of Checkout order Information.	TR1: An attacker modifies Webshop JavaScript code to modify Checkout Order Information by exploiting the Improper Order-checking Logic of the WebShop Server leading to a loss of Integrity of Checkout order Information	TR1.SReq1: The Webshop shall reject changes to check-out order information once Customer proceeds to Checkout. TR2.SReq2: Webshop shall prevent unauthorised corruption of checkout order information during payment process.
R	RT1: An attacker adds entries to Webshop server logs to obfuscate illegal transactions on Webshop. V: Improper Output Neutralisation for Webshop server logs. Impact: Loss of Integrity of Webshop server logs.	RR1: An attacker adds entries to Web-shop server logs to obfuscate illegal transactions on Webshop, exploiting the Improper Output Neutralisation to Webshop server logs, leading to loss of integrity of Webshop server logs.	RR1.SReq1: The Webshop shall verify that logs are protected from unauthorised access and modification. RR1.SReq2: The Webshop shall verify that log output is properly neutralised in log entries.

[1] It is possible that a combination of threats may lead to an event and a security risk. However, this combination is considered as one security threat in analysis, because part of the combining threats may not necessarily generate a security risk until there is a combination.

I	IT1: An attacker extracts sensitive customer information from Webshop storage by sending crafted SQL injection statements through Webshop login interface to the Webshop Database. V: Lack of Input Validation in Webshop Login Interface. Impact: Loss of Confidentiality of Customer information.	IR1: An attacker extracts Customer in-formation from Webshop storage by sending crafted SQL injection statements through Webshop Login interface, exploiting the lack of input validation of Webshop login interface leading to loss of confidentiality of Customer information.	IR1.SReq1: The Webshop shall verify that input data is canonicalised before validation. IR1.SReq2: The Webshop Login interface should re-validate input data in the parameterised stored procedures. IR1.SReq3: The Webshop shall verify that it does not output error messages containing sensitive data. IR1.SReq4: The Webshop shall only use parameterised stored procedures to query the Webshop Database.
D	DT1: An attacker exhausts Webshop checkout service with multiple checkout requests. V: Allocation of Resources Without Limits or Throttling in Webshop Server. Impact: Loss of Availability of Webshop checkout service.	DR1: An attacker floods the Webshop server with multiple checkout requests and exhaust Webshop checkout service by exploiting the Webshop server's allocation of resources Without Limits or Throttling leading to the loss of availability of Webshop checkout service.	DR1.SReq1: The Webshop components shall have limits of scale configured. DR1.SReq2: The Webshop shall have acceptable behaviors specified for when resource allocation reaches limits.
E	ET1: Attacker exploits the weak password based authentication configured in Webshop to gain full privileges to Custom-er Information. V: Weak password based authentication configured in Webshop. Impact: Loss of Confidentiality of Customer Information, Loss of Integrity of Customer Information.	ER1: An attacker exploits the weak password based authentication configured in Webshop to gain full privileges to Customer Information leading to the loss of Confidentiality and Integrity of Customer Information.	ER1.SReq1: The Webshop shall have a strong password policy configured. ER1.SReq2: The Webshop shall limit the number of detected attempted accesses that fail authentication requirements to 5 trys.

The experts evaluated this activity based on the quality of the risk scenarios and adherence to the ISSRM domain model to develop the risk scenarios. This resulted in an iterative update of repudiation and elevation of privilege security risk scenarios. Experts also commended the benefits of using STRIDE for threat analysis to support risk identification including the demonstrated STRIDE traceability, linking identified security threats to security risks.

4.3 RQ_3 Security Requirements

To treat the risks discovered, security requirements (SReq) were elicited in Table 6 for each risk scenario to secure the system against each risk. These requirements are labelled following thier security risk structure with the added security requirement (SReq) identifier. Figure 7 illustrates the application of security requirements activity on the carryout login process, with a summarised application of all security requirements on the e-commerce payment process in Figure 8. The application of security requirements on the business process also resulted in countermeasure implementations on the system (see Figure 7). Such countermeasures include mechanisms to *check input* (5.3), *Block customer account* (5.6), *Terminate other customer sessions*(5.10). The security requirements elicited for the mitigation of security risks were evaluated following quality characteristics that a good requirements specification should respect (Alexander and Stevens, 2002), (Davis et al., 1993). Special attention was given to the BPMN illustration of the security requirements on the business process considering not only its syntactic correctness but also its ability to illustrate requirement constraints on particular assets.

4.4 RQ_4 Risk Decision

For this case study we apply the security *risk reduction* treatment decision. For this treatment decision, resource management in form of a trade-off analysis is carried out in order to treat risk. The trade-off analysis uses the metric values of business assets(BV), security criterion (SC) on the business assets, potential risk reduction levels (RRL) and countermeasure cost (CC). We represent metric values for business assets and the security criterion on these assets on a scale of 1 - 3 (Matulevičius, 2017). The risk reduction levels are estimated following calculations of the risk event potentiality, risk impact level and risk level metrics (Mayer et al., 2018):
Risk event = *threat likelihood* + *vulnerability level* - 1
Impact = *maximum value of the security criterion*
Risk level = *risk event* * *impact*
Risk reduction level = *Risk level 1* - *Risk level 2*

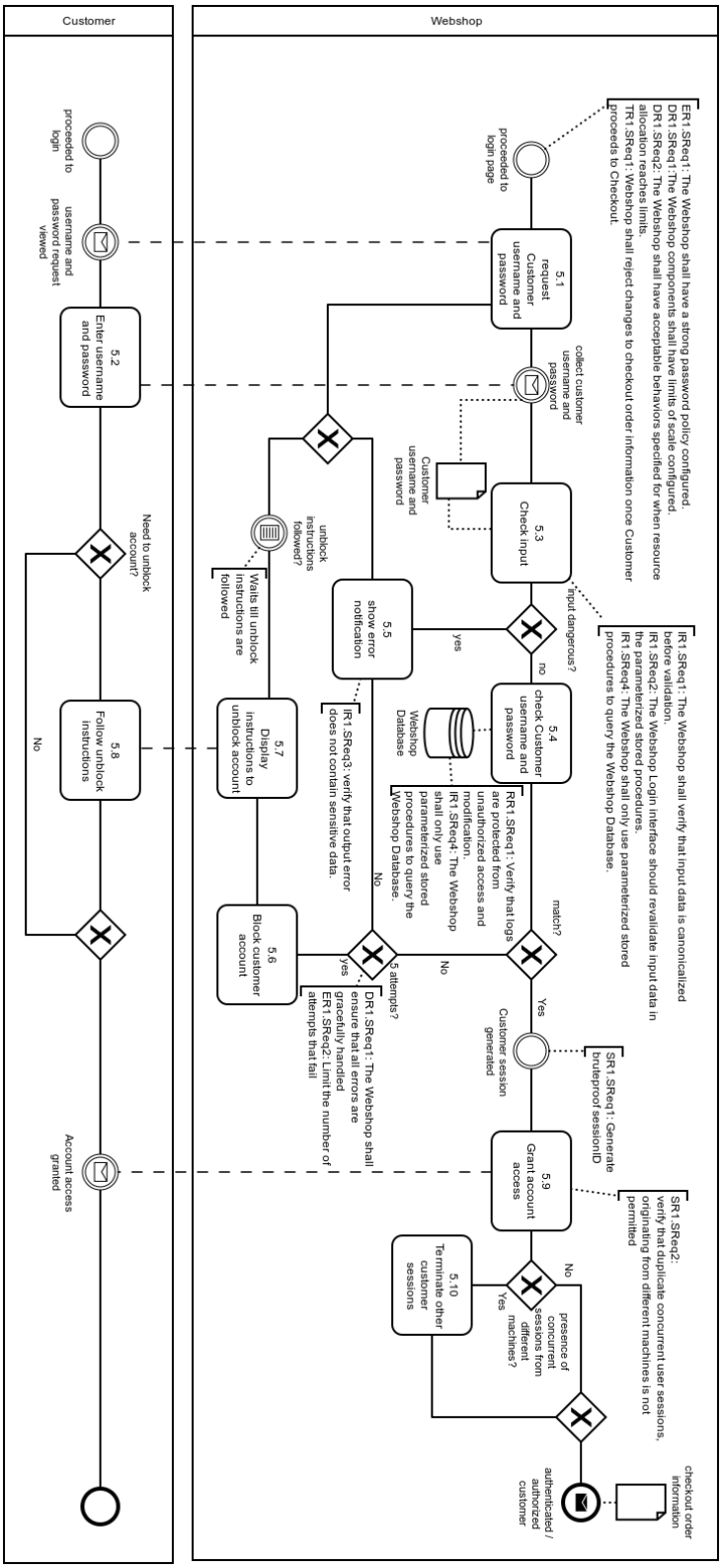

Fig. 7. Countermeasure Implementation on Carryout Login Process.

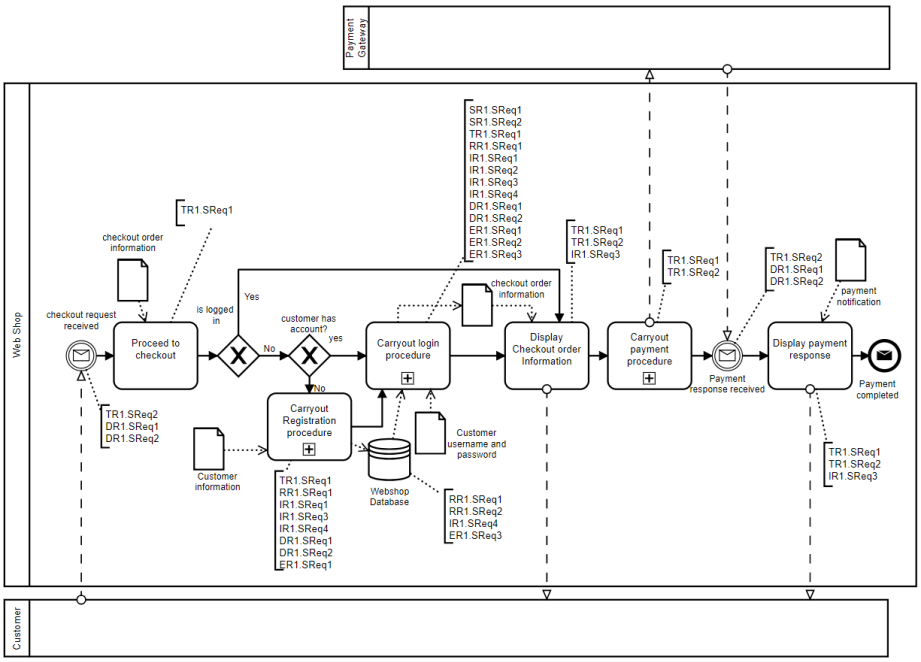

Fig. 8. Payment Process Countermeasure Diagram.

Values for vulnerability level (VL) and threat likelihood (TL) are decided with information from CWE (2020) and OWASP (Wichers, 2013) about these scenarios. Estimates for the cost of implementing countermeasures followed informed decisions based on the proposed controls and security requirement (see Section 4.3 for the risk scenarios.

The threat level (TL1) and vulnerability levels (VL1) for each risk scenario before risk treatment is derived. Estimations are also made for the threat level (TL2) and vulnerability level (VL2) after risk treatment. We then derived estimates for risk impact and the potential risk reduction levels (RRL).

Table 7. Risk Metrics Before and After Risk Treatment.

Risk ID	BV	SC	TL1	VL1	TL2	VL2	RRL	CC
SR1	3	3	2	3	1	1	9	2
TR1	3	3	3	3	2	1	9	3
RR1	2	3	2	2	1	1	6	3
IR1	3	3	3	3	1	1	12	2
DR1	3	3	3	3	1	1	12	2
ER1	3	3	3	3	2	1	9	2

Next, we place risks to be treated in graph quadrants offering three possible options labeled as **high** - 3 (optimal responses to risks), **medium** - 2 (more difficult responses to lower risk), and **low** - 1 (costly responses to lower risks) based on their derived metrics.

1. **Risk reduction level (RRL) vs Business asset value (BV)**: A desired situation is one where an asset of high business value, has a high risk reduction level value (IR1 and DR1) representing high priority. Medium priority risks represent high business

asset value and low risk-reduction level, and high risk reduction level and low business asset value (SR1, TR1, and ER1). The least desired situation is risk with low business asset value and low risk reduction level(RR1). These are illustrated in Figure 9.

2. **Risk reduction level (RRL) vs Countermeasure cost (CC)**: A desired situation is one with low countermeasure cost and a high risk reduction value, (RR1) representing high priority. Medium priority is found in quadrants having high cost of countermeasure value with high risk reduction levels (TR1) and a low countermeasure cost with low risk reduction value. The low priority risks are in the quadrant having a high countermeasure cost and a low risk reduction level value (SR1, IR1, DR1, and ER1). This is illustrated in Figure 10.

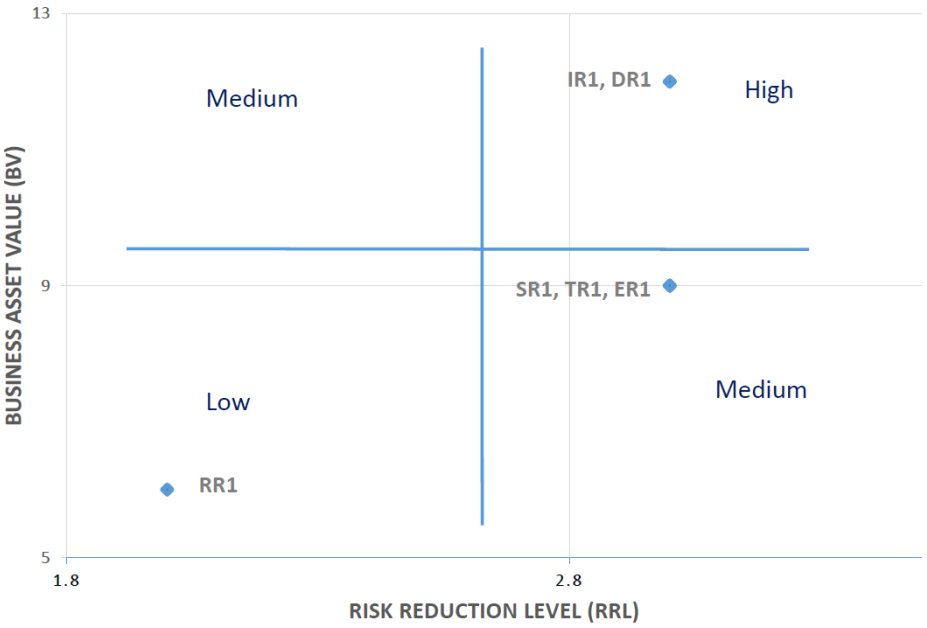

Fig. 9. Risk reduction level (RRL) vs Business asset value (BV).

3. **Countermeasure cost (CC) vs Business asset value (BV)**: The risks of high priority are found in the quadrant having low cost of countermeasure with high business asset value (SR1, IR1, DR1 and ER1). Medium priority are in quadrants having high value business assets with a high cost of countermeasure (TR1) and a low-value business asset combination with low countermeasure cost. The least desired situation is one of low business asset value with a high countermeasure cost (RR1). This is illustrated in Figure 11.

Consequently, a priority list (see Table 8) is derived from the graphs (Figures 9, 10 and 11) showing risks that can be treated with optimal responses as high priority. The

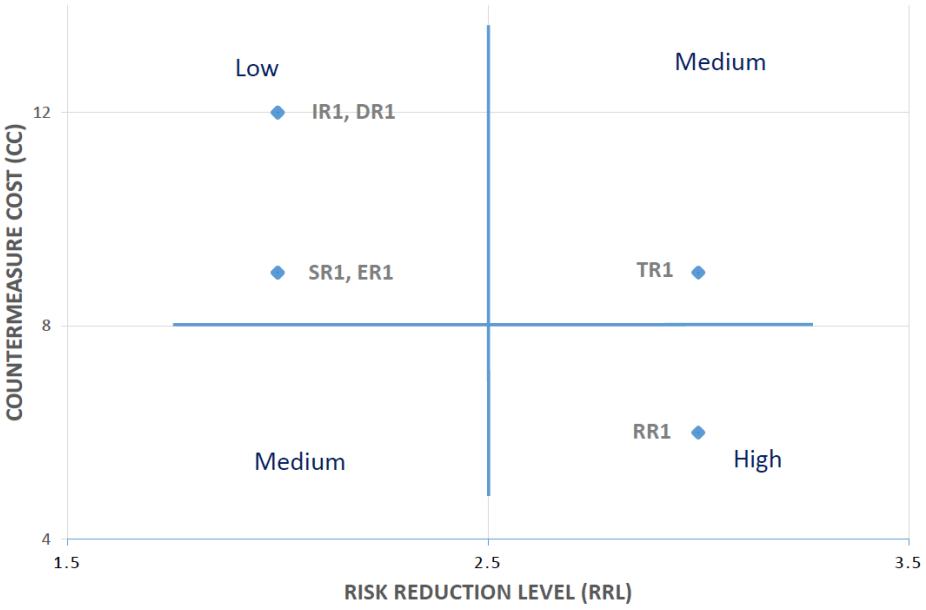

Fig. 10. Risk reduction level (RRL) vs Countermeasure cost (CC).

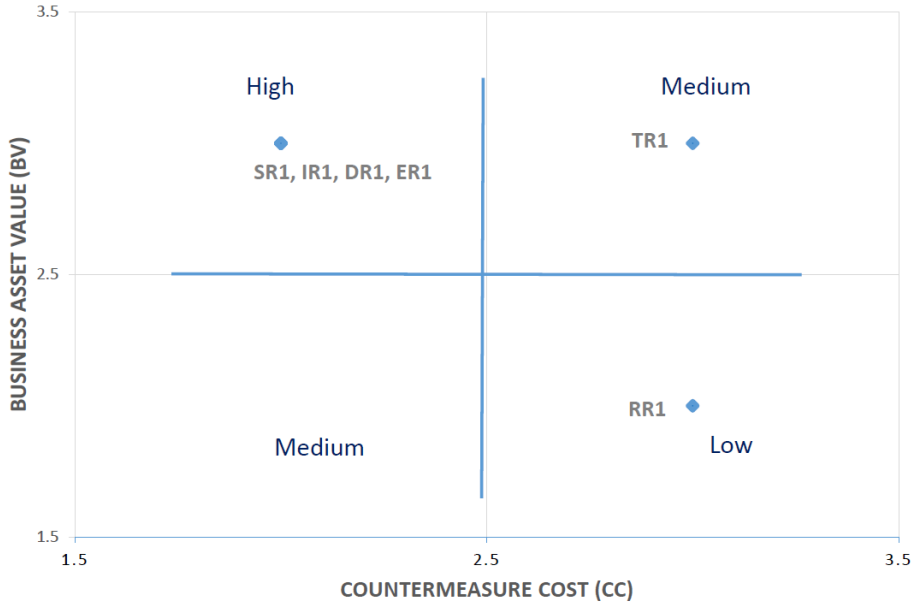

Fig. 11. Countermeasure cost (CC) vs Business asset value (BV).

derived metrics and trade-off analysis were expert evaluated and reported to be satisfactory.

Table 8. Results of Security Risk Trade-off Analysis

Risk ID	RRL vs BV	RRL vs CC	CC vs BV		Priority
IR1	3	1	3	7	High Priority
DR1	3	1	3	7	High Priority
SR1	2	1	3	6	Medium Priority
TR1	2	2	2	6	Medium Priority
ER1	2	1	3	6	Medium Priority
RR1	1	3	1	5	Low Priority

5 Discussion

The results of the use of STRIDE to support ISSRM in threat analysis has been illustrated in Section 4. This section discusses the lessons from the STRIDE and ISSRM combination, using analysis based on the threat-driven approach selection (see Section 2.5) and other related approaches (see Section 2.6).

5.1 Analysis based on Threat-driven Approach Selection

In Section 2.5, we proposed the use of STRIDE in supporting ISSRM efforts forming the threat-driven approach. Here, we reflect on how well the STRIDE and ISSRM combination satisfied the provided reasons for the combination.

- **Threat modelling**: STRIDE's constructs provided a basis for threat identification as illustrated in Table 6. Threats as a result of each STRIDE construct were easily identified and defined for the specified system assets. This technique of threat modelling followed the ISSRM domain model, allowing risk-related concepts to be instantiated. System asset vulnerabilities were augmented using Vulnerability catalogs/database (e.g. National vulnerability database (NVD, a), Common Weakness Enumeration (CWE, 2020), as well as threat agent attack methods and risk impacts, to form the security risk statement. The process of threat modelling within the *Discover Risks* activity of the research method, was done in iterative considering expert inputs and analysis to produce the risk table (see Table 6).
- **Threat Categorisation**: The security threats were elicited and classified according to STRIDE categories. However, with categorisation, there were some considerations. When analysing the threats, the assets are portrayed as the victim. For Spoofing threat (see Table 6), *the attacker compares valid sessionIDs provided by Webshop and brute-forces to access a valid Customer Session*, here the attacker uses information disclosed by the Webshop by observing issued sessionIDs, to generate valid sessionIDs. Although there is some information disclosure leading to enabling the spoofing attack, the system does not undergo an attack unless the disclosed information is used for spoofing or other purposes. The information disclosed is only a vulnerability at this point and not yet a threat.

Another perspective considered, is what happens after an attacker gains access to a customer session and now has higher privileges than the customer. This can be categorised as an elevation of privilege (**E**) threat. However, for this research, threats at this stage are classified based on first impact. Hence, this threat was eventually classified as a spoofing (**S**) threat.

- **Expressing security requirements**: The security requirements expressed within the STRIDE constructs aided in security requirement elicitation and definition. Although it did not provide the full list of security requirements for the particular security risk scenario, it served as a great starting point to security requirement definition. Each security requirements elicited are represented in the business process. This illustration depicts to stakeholders and system architects alike, where security requirements can be enforced and security controls implemented in order to ensure security.
- **Traceability**: Within the ISSRM process of risk analysis and assessment (including threat identification to classification), traceability was discovered with the use of STRIDE. It was seen that it is not enough to list the elicited security risks, but allow traceability to its associated threat. For example, all risks as a result of a spoofing threat are labeled SRx, where x is the risk number. Now within the next process of risk treatment and security requirements determination (and definition), the security requirements developed were made to be traceable to the security risk and as such the threat classification that originated the requirement. For example, security requirements generated as a result of a spoofing risk is given the label $SRx.SReqx'$, where x is the risk number and x' is the security requirement number.
- **Countermeasure Suggestion**: Countermeasure suggestion was a derivative of the security requirements for the security risk scenarios. In Figure 7, it can be seen that the application of security requirements on the carryout login process resulted in the implementation of security countermeasures such as blocking account access after 5 attempts, input checks to validate user input and presence of concurrent customer sessions check.
- **Expressing security needs**: The security needs of the e-commerce system is evaluated during the security risk analysis scenario (see Table 6) and with the spoofing risk being an authentication related risk to the e-commerce system, tampering risk being an integrity related risk as well as the rest of the security risk scenarios following the STRIDE security properties. These were helpful to identify and define the security needs of the business assets within that scenario.

5.2 Analysis based on Related approaches

The related approaches discussed in Section 2.6, showed security analysis research on information systems using STRIDE, a combination of STRIDE and other security methods and the combination of the security threat analysis method – Security-Risk Oriented Patterns (SRP) and ISSRM.

Single use of a security threat analysis method or a combination of threat analysis methods (Xin and Xiaofang, 2014), (Abomhara et al., 2015), (Guan et al., 2011) did not allow for effective management of the resulting security risks. The combination

of STRIDE and ISSRM uses STRIDE to analyse security threats and ISSRM to manage the resulting risks from the STRIDE analysed threats. This management involves the elicitation of security requirements to protect the system from the analysed threats, countermeasure suggestion, and trade-off analysis for resource management when treating risk.

Research also exists where a security threat analysis method is combined with a security risk management method (Samarütel et al., 2016). Here, the ISSRM method was combined with security risk-oriented patterns to secure the Airline Turnaround process. Although security risk-oriented patterns is a good tool for security threat analysis, it has limitations. SRPs are constrained to system business process. On the other hand, STRIDE analysis of security threats in a system is not constrained to a business process representation. STRIDE is open to other representations such as Data flow diagrams (DFD) not constrained by a business process. In this work, the use of business modelling techniques (i.e BPMN) is used to consider the asset, risk, and risk treatment scenarios is used in enabling enhanced security risk communication between IT and business stakeholders involved in the security risk management procedure. However, the analysis was not constrained only to assets illustrated in the models (see Section 4.1). SRPs contain 5 patterns for security threat analysis and these patterns do not cover as much security need for a system as opposed to STRIDE. STRIDE does not use patterns but contains security properties expressing (in its opposites) the security needs of the system (see Section 5.1).

Following the discussions, the combination of STRIDE and ISSRM provided a benefit against single use of STRIDE and combinations between other security threat analysis methods. This is the same for other security threat analysis method combinations with ISSRM. The approach utilised the benefits of STRIDE and ISSRM, producing expert evaluated analysis on system threats, risk, risk mitigation and trade-off analysis for security risk management.

6 Conclusion

Analysis on the combination of STRIDE and ISSRM on the payment process, come together in providing an answer to the research question of this paper: *How can we support security risk management with a targeted approach for security threat analysis?* A threat-driven approach, evaluated by security experts for security risk management is proposed and analysed. This analyses the use of the security threat analysis method – STRIDE to demonstrate an intensive security threat analysis that supports ISSRM, a security risk management method. STRIDE supports ISSRM with threat modelling, categorisation, traceability, expressing of security need, expressing of security requirements and countermeasure suggestion efforts for security risk management.

Assets for an e-commerce system can be identified from business process models of the system. Using this model, both business assets and system assets are illustrated implicitly or explicitly fulfilling the asset-related requirements of ISSRM. STRIDE is used to identify system asset threats, following the ISSRM domain model to derive impact and risk assessments. Risk treatment procedure of the STRIDE risks results in security requirements elicitation. The STRIDE labeled security requirements elicited

can be applied to the business process to show processes in need of optimisations and security countermeasures to treat risks. These security requirements introduce actions and countermeasure implementations that lead to security risk mitigation. Finally, a cost-benefit analysis aided risk mitigation decisions as resources may not be available to treat all discovered risks.

An adaptation of this approach to other domains will be beneficial in security risk management research and implementation.

References

Abomhara, M., Gerdes, M., and Køien, G. M. (2015). A stride-based threat model for telehealth systems. *Norsk informasjonssikkerhetskonferanse (NISK)*, **8**(1), 82–96.

Adidas.(2018). Adidas alerts certain consumers of potential data security incident. https://www.adidas-group.com/en/media/news-archive/press-releases/2018/adidas-alerts-certain-consumers-potential-data-security-incident/.

Affia, A. A. O. (2018). *Security Risk Management of E-commerce Systems*.(Masters dissertation).

Ahmed, N., Matulevičius, R. (2014). Securing business processes using security risk-oriented patterns. Computer Standards & Interfaces, **36**(4), 723-733.

Alberts, C., Dorofee, A., Stevens, J., Woody, C. (2003). *Introduction to the OCTAVE Approach*. Carnegie-mellon University Pittsburgh PA Software Engineering Institute.

Alexander, I. F., Stevens, R. (2002). *Writing better requirements*. Pearson Education.

Breach Level Index. (2019). Data Breach Database - Breach Level Index. http://breachlevelindex.com/data-breach-database.

Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F., Mylopoulos, J. (2004). Tropos: An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, **8**(3), 203-236.

BSI Standard. (2008) 100-3, 2005. *Risk Analysis Based On It-grundschutz-version*, **2**

CAPEC. (2019). Common Attack Pattern Enumeration Classification. https://capec.mitre.org.

Chaffey, D., Hemphill, T., Edmundson-Bird, D. (2019). *Digital business and e-commerce management*. Pearson UK.

Chancellery, A. F. (2004). *Austrian IT Security Handbook*.

CWE. (2020). Common Weakness Enumeration. A community-developed dictionary of software weakness types. https://cwe.mitre.org/index.html.

Crowell, A. (2011). A Survey of Access Control Policies. *University of Maryland*.

Dalpiaz, F., Paja, E., Giorgini, P. (2016). *Security requirements engineering: designing secure socio-technical systems*. MIT Press.

Davis, A., Overmyer, S., Jordan, K., Caruso, J., D, Ashi, F., Dinh, A., Kincaid, G., Ledeboer, G., Reynolds, P., Sitaram, P., and others. Identifying and measuring quality in a software requirements specification. In:*Proceedings First International Software Metrics Symposium*, IEEE, 141–152.

Deng, M., Wuyts, K., Sc, Ariato, R., Preneel, B., Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*. **16**, 3–32.

De Risques, M. H. D. A. (2007). MEHARI. *Clusif, France*.

DCSSI Advisory Office. (2010). EBIOS: Expression of Needs and Identification of Security Objectives. Technical Report, Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information

Dubois, É., Heymans, P., Mayer, N., Matulevičius, R., (2010). A Systematic Approach to Define the Domain of Information System Security Risk Management. In: *Intentional Perspectives On Information Systems Engineering*, Springer, 289–306.

eBay Inc.. (2014). Frequently Asked Questions on eBay Password Change. https://www.ebayinc.com/stories/news/faq-ebay-password-change/.

Farquhar, B. (1991). One approach to risk assessment. In: *Computers & Security* **10**(1), 21–23.

Fredriksen, R., Kristiansen, M., Gran, B., Stølen, K., Opperud, T., Dimitrakos, T. (2002). The CORAS framework for a model-based risk management process. In:*International Conference on Computer Safety, Reliability, and Security*, Springer, 94–105.

Green, D., and Hanbury, M. (2018). If you shopped at these 14 stores in the last year, your data might have been stolen. *Business Insider*, 6. https://www.businessinsider.com/data-breaches-2018-4.

Guan, H., Chen, W. R., Li, H., and Wang, J. (2011). STRIDE–Based Risk Assessment for Web Application. In Applied Mechanics and Materials (Vol. 58, pp. 1323–1328). Trans Tech Publications Ltd.

Howard, M., Lipner, S. (2006). *The security development lifecycle*.(Vol. 8). Redmond: Microsoft Press.

Janulevičius, J. (2016). *Method of Information Security Risk Analysis for Virtualized System* (Doctoral dissertation, VGTU leidykla Technika).

Korper, S., Ellis, J. (2000). The E-commerce Book: Building the E-empire. Elsevier.

Li, T., and Horkoff, J. (2014). Dealing with security requirements for socio-technical systems: A holistic approach. In *International Conference on Advanced Information Systems Engineering*. Springer, Cham, 285–300).

Liu, Y., and Man, H. (2005). Network vulnerability assessment using Bayesian networks. In *Data mining, intrusion detection, information assurance, and data networks security 2005* (Vol. 5812, pp. 61-71). International Society for Optics and Photonics.

Lund, M. S., Solhaug, B., Stølen, K. (2011). The CORAS approach.

Macy's. (2018). Macy's warns customers of online data breach https://eu.freep.com/story/money/business/2018/07/06/macys-data-breach-online/763074002/.

Matulevičius, R. (2017). *Fundamentals of secure system modelling*. Springer.

Matulevičius, R., Norta, A., Udokwu, C., Nõukas, R. (2016). Security risk management in the aviation turnaround sector. In *International Conference on Future Data and Security Engineering*. Springer, Cham, 119–140.

Mayer, N., Dubois, E., Matulevičius, R., Heymans, P. (2008). Towards a Measurement Framework for Security Risk Management. In *MODSEC@ MoDELS*. http://ceur-ws.org/vol-413/paper17.pdf.

Muckin, M., and Fitch, S. C. (2014). A threat-driven approach to cyber security. *Lockheed Martin Corporation*.

MSDN. (2009). STRIDE Threat Model. https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

NVD.(a). National vulnerability database. National Institute of Standards and Technology. https://nvd.nist.gov.

OMG (2011). Notation (bpmn) version 2.0. *OMG Specification, Object Management Group*, 22–31.

Paja, E., Dalpiaz, F., Giorgini, P. Managing security requirements conflicts in socio-technical systems. In:*International Conference on Conceptual Modeling*, Springer, 270–283.

Paja, E., Dalpiaz, F., Poggianella, M., Roberti, P., Giorgini, P. (2012). STS-Tool: Using commitments to specify socio-technical security requirements. In: *International Conference on Conceptual Modeling*. Springer, Berlin, Heidelberg, 396–399.

Radack, S. (2011). *Managing information security risk: organization, mission and information system view* (No. ITL Bulletin March 2011). National Institute of Standards and Technology.

Raptis, D., Dimitrakos, T., Gran, B., Stølen, K. (2002). The CORAS approach for model-based risk management applied to e-commerce domain. In:*Advanced Communications and Multimedia Security.* Springer, 169–181.

Samarütel, S. Matulevičius, R., Norta, A., Nõukas, R. (2016). Securing airline-turnaround processes using security risk-oriented patterns. In: *IFIP Working Conference on The Practice of Enterprise Modeling*. Springer, Cham. 209–224.

Shostack, A. (2014). *Threat modeling: Designing for security. John Wiley & Sons.*

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerlad, P. (2013). *Security Patterns: Integrating security and systems engineering*. John Wiley & Sons.

Sindre, G., Opdahl, A. L. (2001). Templates for misuse case description. *In Proceedings of the 7th International Workshop on Requirements Engineering, Foundation for Software Quality (REFSQ'2001), Switzerland.*

Sindre, G., Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. *Requirements engineering*, **10**(1), 34–44.

Sindre, G. (2007). Mal-activity diagrams for capturing attacks on business processes. In: *International working conference on requirements engineering: foundation for software quality*. Springer, Berlin, Heidelberg, 355–366.

Stephens, J., Valverde, R. (2013). Security of e-procurement transactions in supply chain reengineering. *Computer and Information Science*, **6**(3).

Stoneburner, G., Goguen, A., Feringa, A. (2002). Risk management guide for information technology systems. *NIST special publication, 800*(30), 800-30.

Stølen, K. (2001). CORAS A Framework for Risk Analysis of Security Critical Systems. In: *Supplement of the 2001 International Conference on Dependable Systems and Networks, pages D4-D11*.

Target. (2013). Data breach FAQ. `https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car`.

Uzunov, A. V., and Fernandez, E. B. (2014). An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces*, **36**(4), 734–747.

Wichers, D.(2013). Owasp top-10 2013. *OWASP Foundation*.

Xin, T., Xiaofang, B. (2014). Online Banking Security Analysis based on STRIDE Threat Model. *International Journal of Security and Its Applications*, **8**(2), 271-282.

Xu, D., and Nygard, K. E. (2005). A threat-driven approach to modeling and verifying secure software. In *Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering*, 342–346.

Xu, D., and Nygard, K. E. (2006). Threat-driven modeling and verification of secure software using aspect-oriented Petri nets. IEEE transactions on software engineering, **32**(4), 265–278.

Xu, D., and Pauli, J. (2006). Threat-driven design and analysis of secure software architectures. Journal of Information Assurance and Security, **1**(3), 171–180.

Yanyan, W. (2014). Research on e-commerce Security based on Risk Management Perspective. *International Journal of Security and Its Applications*, **8**(3), 153-162.

Received January 15, 2020 , revised March 20, 2020, accepted March 27, 2020