Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Introducing OSSF: A framework for online service cybersecurity risk management

Jan Meszaros [*], *Alena Buchalcevova*

Department of Information Technologies, University of Economics, W. Churchill Sq. 4, 130 67 Prague 3, Czech Republic

ARTICLE INFO

Article history:
Received 19 May 2016
Received in revised form 1 October 2016
Accepted 14 December 2016
Available online 19 December 2016

Keywords:
Security
Cybersecurity
Security risks
Risk management
Online service
Threats
Vulnerabilities
Measures
Risk analysis
Threat analysis

ABSTRACT

This paper proposes a new framework for online services security risk management which can be used by both service providers and service consumers. The proposed framework was validated through a case study performed in a large enterprise environment. The key components of the proposed framework are Threat model and Risk model. These models are designed to fit specific features of online services and the surrounding cyberspace environment. A risk management process is an integral part of the framework. The process is suitable for frequent and recurrent risk assessments. The process execution results in identification and performance of proper tasks which contribute to treatment of identified security risks and deficiencies. Online services risk score could be continuously documented and reported if the process is executed on a regular basis.

1. Introduction

Securing information processed and stored by information and communication technologies is increasingly important task due to increasing ingenuity and quantity of attacks detected in the cyberspace. Therefore, this paper focuses on online services security covering generally any services which are provided and consumed within the public Internet environment. Authors of this paper are confident that a fundamental precondition for assuring that an online service is provided or consumed securely is an adoption of a proper risk management framework. No such framework has been identified which focuses specifically on online services and therefore, this paper's aim is to fill this gap and to propose a novel framework for online service cybersecurity risk management.

This paper is organized as follows. Section 2 describes research methods applied, Section 3 is dedicated to terminology and related work. Section 4 represents the main contribution proposing the cybersecurity risk management framework for on-line services. Section 5 describes the evaluation of the proposed framework. Lastly, the discussion and conclusion sections are included.

[*] *Corresponding author.*
E-mail addresses: jan@meszaros.cz (J. Meszaros), alena.buchalcevova@vse.cz (A. Buchalcevova).

http://dx.doi.org/10.1016/j.cose.2016.12.008
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

2. Research methods

The proposed framework was developed using the Design Science Research methodology (DSR) published by Peffers et al. (2007). This method defines a process of six activities which result in an artifact (Peffers et al., 2007):

1. The "Problem identification and motivation" activity defines the specific research problem and justifies the value of a solution (see Sections 1, 3.3 and 3.4).
2. The "Define the objectives for a solution" activity goal is to infer the objectives of a solution from the problem definition and knowledge what is possible and feasible (see Section 4.1).
3. The "Design and development" activity is focused on creating the artifact, which can be constructs, models, methods or instantiations (see Sections 4.2 up to 4.8).
4. The "Demonstration" activity comprises illustration of the artifact usage within solving one or more instances of the problem. Although this activity was performed by the authors, it is not documented within this paper.
5. The "Evaluation" activity is dedicated to observe and measure how well the artifact supports a solution to the problem (see Section 5).
6. The last activity is "Communication", it is represented by this paper itself which communicates the problem, its importance and the proposed artifact.

The artifact is a quite broad term representing "any designed object in which a research contribution is embedded in the design" (Peffers et al., 2007). Peffers et al. (2007) mention constructs, models, methods or instantiations as examples of particular artifact types. From this perspective, the proposed framework is considered as an artifact.

For the evaluation of the proposed framework, the Case study method was utilized according to Yin (2009).

3. Background and related work

This section summarizes key terms used in the subsequent paragraphs, briefly describes similar artifacts and depicts a motivation for creating a new artifact.

3.1. *Terminology used*

In this paper, terms related to information security and cybersecurity are adopted from the ISO/IEC 27000 family of standards.

The following fundamental terms are defined according to the overview and vocabulary standard (ISO/IEC, 2014): *Information security* is "preservation of confidentiality, integrity and availability of information", *threat* is "potential cause of an unwanted incident, which may result in harm to a system or organization", *vulnerability* is "weakness of an asset or control that can be exploited by one or more threats", *information security event* is "identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant", *information security incident* is "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security", *risk* is "effect of uncertainty on objectives", *risk management* is defined as "coordinated activities to direct and control an organization with regard to risk", *risk assessment* is "overall process of risk identification, risk analysis and risk evaluation".

The term *cybersecurity* is defined differently in various sources, for example ITU-T (2009) or NIST (2014). In this paper, a definition based on the "information security" term is used according to ISO/IEC 27032 (2012) standard: "Cybersecurity is preservation of confidentiality, integrity and availability of information in the cyberspace." The same standard defines *the cyberspace* as "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".

Differences and relations among the *information security, cybersecurity* and *ICT* security are discussed by von Solms and van Niekerk (2013). Their conclusion is that cybersecurity discipline is not only focused on protecting information in the cyberspace but also on those that function in the cyberspace and any of their assets that can be reached via the cyberspace (von Solms and van Niekerk, 2013). They perceive the *ICT security* field as a subset of both information security and cybersecurity disciplines (von Solms and van Niekerk, 2013).

Currently, there is no common definition of *online service* and therefore, the following definition was proposed: *Online service* is provided by a service provider and used by a service consumer, both provider and consumer are present in the cyberspace.

3.2. *Overview of similar artifacts*

Total seven similar artifacts were identified. In the following paragraphs, only brief overviews of similar artifacts are presented instead of detailed descriptions which are contained in the corresponding author's dissertation.

The CORAS method was developed by members of Department of Informatics at the University of Oslo. The method defines a process containing eight steps, the overall goal of the process is to identify threats and risks and to decide to implement suitable security measures (Lund et al., 2011). The process execution is supported by the CORAS Tool which supports all diagram types defined by the method.

The Harmonized Threat and Risk Assessment Methodology (HTRA) was developed by the Government of Canada in order to unify the manner how threats and risks are assessed by the individual governmental organizations (Government of Canada, 2007). Threat and risk assessment is considered as a project by the methodology which consists of five subsequent phases. The methodology points out that the IS/ICT environment is highly dynamic and therefore new threats and vulnerabilities are emerging. Due to this fact, the methodology promotes a need to update project variables continuously (Government of Canada, 2007).

The ISO/IEC 27005 standard defines guidelines for information security risk management and relevant process with respect to requirements on information security management. The standard does not prescribe or recommend any particular risk management method and has appendices which describe common techniques and principles of risk management (ISO/IEC, 2011).

The main purpose of *the NIST Risk Management Framework* is to provide guidance for risk management application, its risk management process consists of six steps (NIST, 2010). This framework focuses mainly on management of risks related to new information systems implementation and deployment within federal organizations in the USA.

The OCTAVE Allegro is the most recent version of the OCTAVE method developed at Software Engineering Institute at Carnegie Mellon University (Caralli et al., 2007). This risk management method is focused primarily on identification of organization's information assets. For identified assets, threat scenarios and risks are identified. This is performed using a process which comprises eight steps. The method supports recurring usage and provides consistent outputs across an organization.

The Threat Agent Risk Assessment (TARA) methodology was published by Intel Corporation in 2009. The main aim of this methodology is to identify threat agents who are pursuing reachable targets and can cause losses to an organization (Rosenquist, 2009). The methodology is focused especially on prediction in a risk management process.

A framework for measuring temporal variance in computer network risks was published by Awan et al. (2016). This risk assessment framework focuses on temporal variances of risk score within networks and subnets. The applied principle of measuring risk score over time is similar to a comparable principle utilized within the proposed framework.

3.3. *Evaluation of similar artifacts*

The evaluation is focused mainly on structure of a risk management process and ease of use viewpoints with regards to online services. The artifacts listed in the previous section are in the evaluation scope except for the TARA methodology and the framework published by Awan et al. (2016) because they are focused only on risk assessment discipline.

Risk management processes of the CORAS, HTRA, ISO/IEC 27005 and OCTAVE Allegro artifacts consist of the common phases described by the ISO/IEC 31000 standard (ISO/IEC, 2009): scope specification, risk identification, analysis, evaluation and treatment. The risk identification phase is based on asset identification. In the online service context, the scope is clearly defined as the whole online service before the risk management process starts. The asset identification activity does not seem beneficial as the asset is the online service itself. Individual online service components can be perceived as assets of course. But it is not clear what level of service decomposition is enough in order to identify important threats and risks. Decomposition to atomic level can be very time consuming and it does not seem useful. The asset valuation concept contained in HTRA, ISO/IEC 27005 and OCTAVE Allegro seems to be useless for components of on-line services, because their purchase price can be zero in case of open source software. Estimating a value can be difficult in case of in-house developed software. Moreover, making efforts to estimate a business value of online service components in terms of loss expectancy or revenue creation can be a very difficult task with regards to online service complexity.

The *NIST Risk Management Framework's* process differs in terms of its risk management process. It starts with categorization of information systems and information based on impact analysis and continues with selection and implementation of security controls based on the categorization. Selection of security controls should be based on risk assessment results, but the framework does not specify how the risks should be assessed. The subsequent steps cover assessment of security controls, authorization of information systems and security controls monitoring.

Easy usage of the artifacts can be supported by toolsets. The CORAS Tool software application is freely provided by authors of CORAS method. Various commercial and free software exist which support security risk management according to ISO 27005 standard. No supporting software applications were found for the OCTAVE Allegro and HTRA artifacts but they are provided at least with worksheets and guidance materials.

Risk identification and classification tasks are facilitated through predefined catalogues of threats and vulnerabilities which are provided by HTRA and ISO/IEC 27005. OCTAVE Allegro contains predefined threat trees which support threat scenario identification and description.

3.4. *Challenges and motivation*

One of the main challenges in the researched area is to keep the artifact as much as simple and easily understandable by its prospective users while keeping valuable outputs. These attributes may enable adoption of proper risk management of online services in practice and make risk management activities feasible not only to big enterprise environments but also to small and medium businesses.

Other challenges are to keep focus on performing suitable tasks contributing to risk treatment instead of extensive analyses or assessments. Outcomes of tasks should be measured in terms how they helped to decrease a particular risk score.

The challenges mentioned above can be apparently resolved by a consistent and structured framework or methodology fully supported and automated as much as possible by a suitable software tool.

4. The online service security framework proposal

A novel framework was proposed which is referenced using the "OSSF" abbreviation originating from the "Online Services Security Framework" naming. The OSSF is also referenced by "the Framework" expression in the following text. The Framework was designed to support online services security risk management activities better than the similar artifacts listed in Section 3.2.

4.1. *Objectives*

The Framework was developed in accordance to nine objectives derived from evaluation of similar artifacts and from the identified challenges and motivation:

O-1 Take dynamic environment of online services into consideration
O-2 Enable usage by both providers and consumers of online services
O-3 Enable usage by organizations of any size and type
O-4 Increase effectivity and user experience of risk management utilizing a supporting software tool
O-5 Enable easy identification of threats
O-6 Enable easy risk analysis
O-7 Support proper performing of the right tasks
O-8 Support recurring analyses and continuous risk management
O-9 Define and use unified taxonomy

4.2. *Characteristics of the framework*

New technologies are developed and new kinds of threats are emerging. As the nature of new threats cannot be predicted, the proposed Framework is designed in order to be continuously extensible with regards to new threats and corresponding countermeasures.

The Framework supports self-assessment. It means that an organization is able to identify threats or weaknesses without any external support.

Ability to record and monitor changes over time is crucial mainly due to a highly dynamic character of online environment. This enables prediction of a future state based on history analysis.

The proposed Framework contains predefined content which is general and should be useful for most of the users. Nevertheless, the Framework's content is customizable in order to fit specific conditions and features of a particular online service.

The Framework enables to determine severity of identified issues which is a key input for prioritization of countermeasures implementation. This help to ensure that particular tasks related to high risk issues mitigation will be performed without delays.

Instead of extensive and time-consuming analyses whose results are often valid for short time period, the Framework helps its users to focus mainly on activities related to treatment of identified risks. Therefore, the threat and risk analysis tasks are simplified as much as possible.

The Framework provides its users with an overall insight into security threats which may have impact on online services. This approach can reveal some threats which can be hidden or unnoticed.

Different viewpoints are considered within risk management activities. This approach brings better understanding of risks by various business functions and decomposition and structuring of a risk.

The Framework fulfills current and specific needs of its users. They can work with various levels of detail with the Framework. This enables to use the Framework in diverse manners which can reflect for example a current maturity of risk management practices in an organization.

A zero trust approach is utilized which means that the Framework do not suppose existence of any trusted environment and do not take trust levels into consideration. This principle helps to identify threats which are sometimes omitted or hidden, for example threats coming from business partners, contractors, subcontractors and similar.

4.3. *High-level framework architecture*

The OSSF brings its users values in terms of online service security improvements from both consumers' and providers' viewpoints. The Framework is dedicated to online services security management which is realized through a risk management process. Execution of the process is significantly supported and partially automated by a software tool.

The Framework is based on a Threat model (see Section 4.4), a Risk model (see Section 4.5) and a Meta model. Both Threat model and Risk model are considered an important autonomous parts of the Meta model which describes the whole Framework as depicted in Fig. 1.

For threat identification and description purposes, asset, vulnerability, threat and environment objects are used. Assets and security controls are present in a particular environment. They contain vulnerabilities which can be exploited by a threat.

Relevant risks are identified which are related to applicable threats. A risk description comprises threat, environment, asset, vulnerability, risk score and treatment. Risk modification and transfer involve certain types of tasks which have to be performed. Each task is further characterized by its priority, status and outcomes. In the Framework, there is a set of predefined tasks. They were identified as common tasks which can help to implement security measures defending against threat types defined by the Threat model.

4.4. *Threat model*

The main purpose of the Threat model is to facilitate awareness and identification of all possible threat scenarios which may be applicable in a specific online service context. The Threat model is capable to identify, classify and describe threats.

4.4.1. *Scope and limitations of the threat model*

The model is focused on provider's and consumer's viewpoints. Threats influencing surrounding environment are out of scope, because such threats apparently can jeopardize neither provider nor consumer of a particular online service.

Threat agents situated in third party environments can affect other third parties' assets, but such cases are not covered by the model. Therefore, in case that the model describes any threat located in a third party environment affecting assets in a third party environment, then it means always one particular third party.

The Threat model is considering only root causes of possible security violations which may result in incidents. The model also abstracts away from possibly indirect impacts of threats.

Environmental threats are not covered in detail, because they are not very specific for online services.

4.4.2. *Structure of the threat model*

The Threat model describes a threat using an asset and a threat agent characteristics based on entity type and environment type attributes (see Fig. 2). Vulnerabilities of an asset or of a

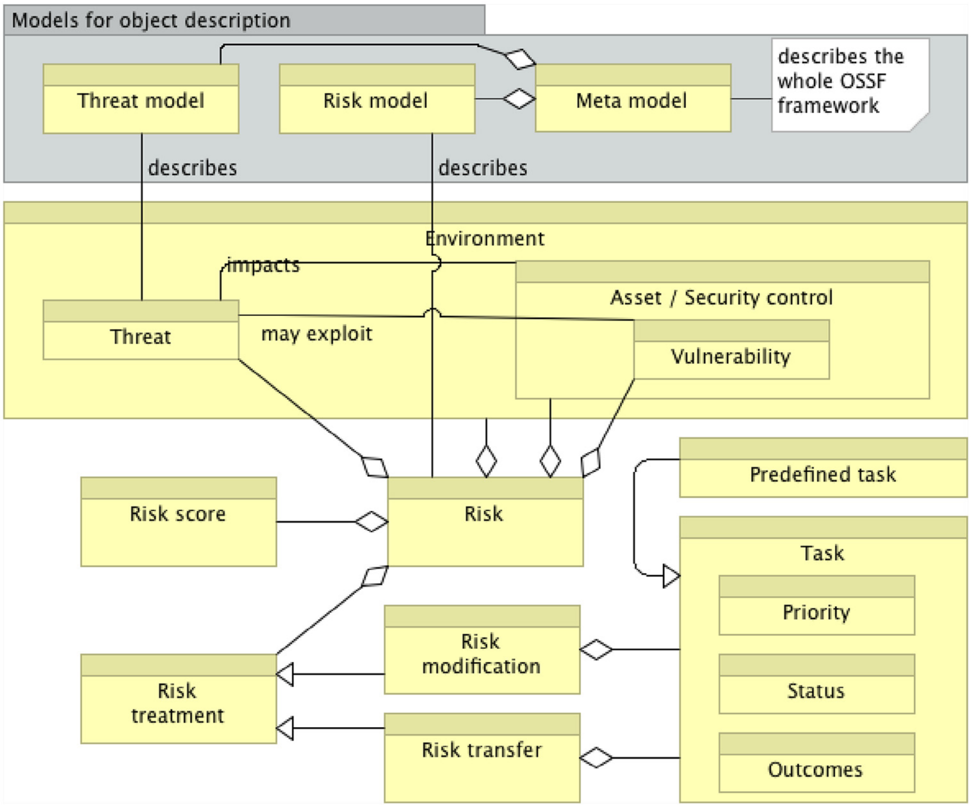

Fig. 1 – Components of the OSSF (ArchiMate notation, information structure viewpoint).

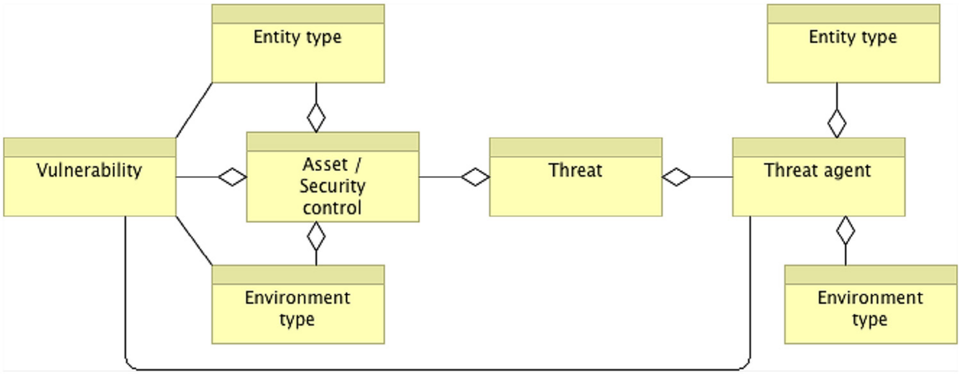

Fig. 2 – Threat model of the OSSF (ArchiMate notation, information structure viewpoint).

security control which may be exploited by a threat agent are taken into consideration as well.

4.4.3. *Assets and security controls*

A security control protecting a particular asset is perceived as an asset by the model. The following five asset types are defined for classification which was inspired by the BMIS model[1]:

- Human – this class refers to people who are participating on operations, providing and consuming of online services.
- Governance – covers governance at business and ICT levels.
- Processes and activities – this refers to various processes and activities related to online services providing and consuming.
- Technology – technical resources and principles utilized for online service providing or consuming.
- Information – this class covers information assets represented by data which are processed or stored by any technology utilized within online service.

[1] Business Model for Information Security, see http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx.

Table 1 – Examples of typical asset types present in different types of environment.

Asset type / Environment type	Provider's environment	Consumer's environment	Third parties' environment
Human	Employees, contractors, suppliers' personnel working on-site, their identity is usually known and verified	Users of online service, various levels of identity knowledge and verification	Similar as for provider's environment but identities are known partially at most, limited verification possibilities
Governance	Business and ICT governance and management		
Processes and activities	Business processes and functions provided within online service, supporting processes	Processes and activities which may rely on an online service	Processes and activities which may be prerequisite for both providing and consuming of online service
Technology	Network components, security facilities, servers, storage devices, endpoint devices including mobile devices, BYOD, IoT devices, software applications and systems, protocols and standards etc.		
Information	Information with various confidentiality levels owned by both providers and consumers	Information with various confidentiality levels owned by consumers	Information with various confidentiality levels owned by providers or consumers or third parties

The first four classes can contain specific vulnerabilities which are described in Section 4.4.5. Information assets do not contain any vulnerability within themselves; vulnerabilities can be contained only in security controls protecting information assets.

Assets may be located in the following three environment types:

- Provider's environment
- Consumer's environment
- Third parties' environment – this type covers any environment of third parties or subcontractors whose products or services are utilized in order to provide or consume an online service.

Examples of assets characterized by combinations of entity and environment types are summarized in Table 1.

4.4.4. *Threat agents*

The Threat agent is an entity that has an intention or an ability to negatively affect online service security. The Threat model distinguishes two threat agent types:

- Human – various people may violate security of online systems by performing unintentional activities, intentional activities or inactivity.
- Technological – this type comprises malware activity, malfunctions or failures, accidents and similar technology-related events.

Environmental threat agent type exists of course but it is not specifically considered, as stated in the scope and limitation summary in Section 4.4.1.

The Threat model defines four types of environment where a threat agent may occur from the online service viewpoint:

- Provider's environment
- Consumer's environment
- Third parties' environment
- Surroundings – entities which are present in this environment class do not have any relationship to provider or consumer; this environment may be also described generally as a cyberspace.

In Table 2, applicable threat agent types are defined for combinations of asset types and threat agent environment classes.

Assets classified as human and governance can be affected only by human threat agents according to Table 2. This reflects the root cause principle which was mentioned as a model limitation in Section 4.4.1.

4.4.5. *Vulnerabilities*

For certain asset types, the Threat model defines common vulnerabilities (see Table 3) which may be exploited by various threat agents. Vulnerability type identifiers are used for mapping between threat types and vulnerability types which is contained in Table A1.

Table 2 – Security risk management scope for different classes of assets and threat agents (except for environmental threat agents).

Asset type	Threat agent environment class			
	Provider's env.	Consumer's env.	Third parties' env.	Surroundings
Human	Human	Human	Human	Human
Governance	Human	Human	Human	Human
Processes and activities	Human, technological	Human, technological	Human, technological	Technological
Technology	Human, technological	Human, technological	Human, technological	Human, technological
Information	Human, technological	Human, technological	Human, technological	Human, technological

Table 3 – Vulnerabilities of human, governance, and processes and activities asset types.

Human	Governance	Processes and activities
VH.1 Social engineering	VG.1 Non-consistent governance	VP.1 Missing or insufficient measures
VH.2 Mistakes	VG.2 Existence of not managed areas, processes and activities	VP.2 Missing validation of inputs and outputs of processes or activities
VH.3 Errors	VG.3 Wrong or missing controls	VP.3 Workflow design errors
VH.4 Negligence	VG.4 Deficiencies and mistakes in reporting	VP.4 Process design and implementation errors
VH.5 Lack of competences	VG.5 Risk management mistakes and errors	VP.5 Process execution errors caused by missing process documentation
	VG.6 Wrong decisions	VP.6 Violation of process SLAs
	VG.7 Impossible deputizing of key personnel	

Technology	
VT.1 Physical security issues	VT.6 Software (code) issues
VT.2 Logical security issues	VT.7 Integration issues
VT.3 Issues in functional and non-functional requirements	VT.8 Communication network issues
VT.4 Design issues	VT.9 Protocols and standards issues
VT.5 Hardware issues	

4.4.6. *Threat classification*

Threat types are defined in Table 4 for combinations of threat agents and assets. Applicable combinations of threat agents and assets arose from the analysis with respect to root cause principle which is fundamental for the Threat model:

- Human threat agents may threaten human, governance, processes and activities, technology and information types of assets.
- Technological threat agents may threaten processes and activities, technologies and information.

Every threat class may exploit vulnerabilities of an applicable asset type except for information assets which do not contain vulnerabilities. Mappings between threats, vulnerabilities and predefined tasks (see Section 4.7) are documented in Tables A1 and A2.

4.5. *Risk model*

The main purpose of the Risk model is to identify, assess and treat risks in a way which takes all important risk perceptions into account. The model is composed of five elements which are described in sections below.

4.5.1. *Threat scenario component*

This component describes threats related to risks and is based on the Threat model introduced in Section 4.4. The main aim of the Threat scenario component is to support risk identification. Threat scenario is an applicable combination of threat agent types and asset types. Threat scenario enables to find out applicable threat types based on mappings among threat agent types, asset types and threat types provided by the Threat model. The applicable threat type list helps to become aware of certain risks emerging from the threats which could be previously unknown or hidden.

4.5.2. *Risk assessment component*

This component's aim is to determine severity of a particular risk based on qualitative risk analysis methodology as described by ISO/IEC 27005:2011 standard. For simplicity, this component uses a 3-level scale for describing likelihood and impact levels which result in 5 possible risk severity levels and 9 risk scores according to Table 5. The likelihood and impact levels are expressed as numbers as well in order to calculate risk score values as sum of likelihood and impact values.

The OSSF proposes using the OWASP Risk Rating Methodology (OWASP, 2015) for determining the likelihood and impact levels, nevertheless, any suitable approach may be used.

4.5.3. *Risk treatment component*

Three different viewpoints are considered for this component. The first focuses on risk treatment options and distinguishes those four defined in the ISO/IEC 27005:2011 standard: risk modification, retention, avoidance, and sharing. The second viewpoint describes objectives of security controls applied within risk treatment and uses preventive, detective, and reactive classes. The latter point of view is focused on nature of a security control which can be administrative or technical.

4.5.4. *Risk classification component*

Usage of widely-accepted OWASP Top 10 list and OWASP Top 10 Mobile Risks list is proposed. Classification scheme can be of course customized.

4.6. *Risk management process*

The process is proposed in accordance to ISO 27005:2011 standard. The process design is suitable for recurrent and frequent iterations. The whole process is documented at Fig. 3 and its individual activities are described below.

The risk management process consists of eight activities which are performed successively:

1. General threat scenarios identification – based on the Threat model, general threat scenarios are selected which may occur in a particular online service context.

Table 4 – Threat classification by different asset and threat agent types.

Asset types	Human threat agents	Technological threat agents
Human	HH.1 Phishing (as a specific social engineering technique) HH.2 Social engineering (other techniques) HH.3 Physical observation and surveillance	–
Governance	HG.1 Policy issues HG.2 Compliance issues HG.3 Failure of controls HG.4 Problem escalation issues	–
Processes and activities	HP.1 Failure to meet SLAs HP.2 Performing unauthorized activities and operations HP.3 Service usage terms violation	TP.1 Exhaustion of system resources TP.2 Issues in specification, design or integration TP.3 Unapproved or unreported technology or technological components
Technology	HT.1 Fraud HT.2 Hacking HT.3 Malware deployment (intentional) HT.4 Man in the middle (MitM) HT.5 Sabotage HT.6 System resources abuse HT.7 Theft HT.8 Vandalism HT.9 Repudiation HT.10 Denial of service (DoS, DDoS) HT.11 Elevation of privileges HT.12 Malware infection (unintentional) HT.13 Mistake HT.14 Negligence HT.15 Missing human resources HT.16 Lack of competences HT.17 Insufficient management and professional guidance	TT.1 Components containing 0-day vulnerabilities TT.2 Components containing known vulnerabilities TT.3 Configuration issues TT.4 Obsolete and/or unsupported technology TT.5 Weak cryptography
Information	HI.1 Identity theft HI.2 Spoofing HI.3 Tampering HI.4 Information leakage HI.5 Data breach	TI.1 Damage TI.2 Destruction TI.3 Information leakage TI.4 Data breach

2. Specific threats identification – based on the list of general threat scenarios, suitable threat categories are selected and the current context is considered by more detailed description of threats including threat agents and relevant assets.
3. Risks identification and assessment – risks which arise from threats are identified and briefly described, risk assessment is performed and vulnerabilities of affected assets are taken into account.
4. Risk treatment – appropriate risk treatment options are decided.
5. Identification of suitable tasks – in order to implement selected risk treatment; predefined tasks are recommended by the OSSF, recommendation is based on mappings between tasks and threat classes (see Appendix, Table A2).
6. Tasks prioritization – all tasks are ordered by their priority which is derived from related risk score. Priorities may be manually altered. Then, tasks are scheduled.
7. Tasks execution – scheduled tasks are performed; task status is tracked over time.
8. Review of results and benefits of finished tasks – whether and how much have the results contributed to decreasing of relevant risk scores. This activity compares a risk treatment plan to reality.

The last activity of the process refers to two points in time depicted at Fig. 3. The situation at point t_1 refers to identified risk with certain severity which should be somehow treated. The point t_2 refers to a moment when a treatment is

Table 5 – Likelihood, impact, risk severity levels and scores.

	High impact (value 9)	Medium impact (value 6)	Low impact (value 3)
High likelihood (value 6)	Critical risk (score 15)	High risk (score 12)	Medium risk (score 9)
Medium likelihood (value 4)	High risk (score 13)	Medium risk (score 10)	Low risk (score 7)
Low likelihood (value 2)	Medium risk (score 11)	Low risk (score 8)	Very low risk (score 5)

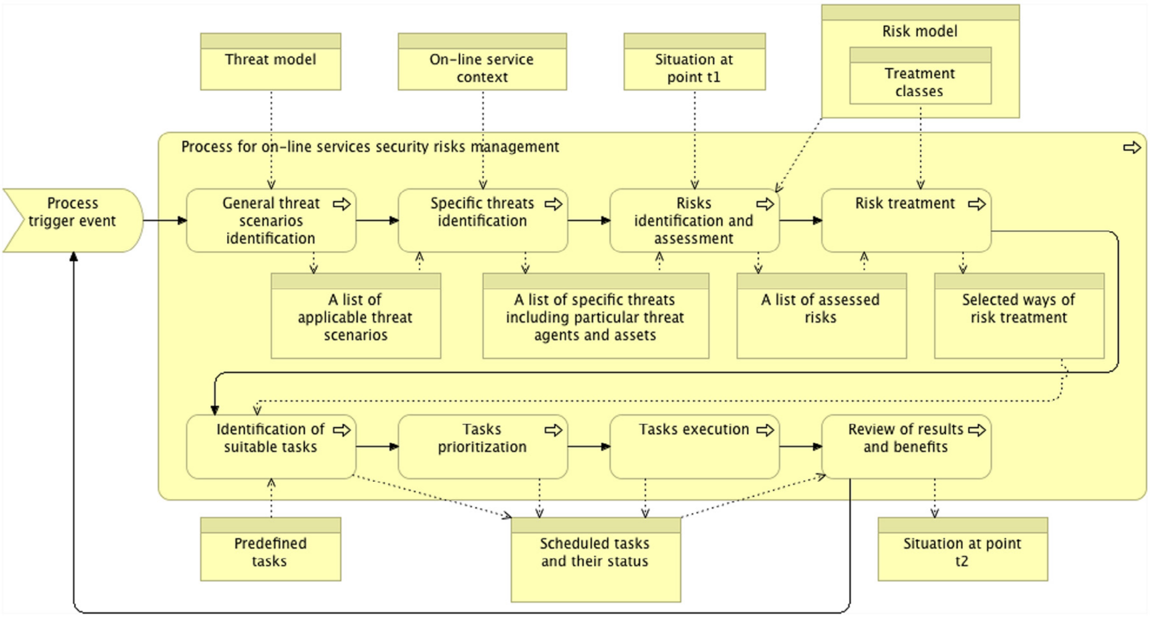
Threat model
On-line service context
Situation at point t1
Risk model
Treatment classes
Process for on-line services security risks management
Process trigger event
General threat scenarios identification
Specific threats identification
Risks identification and assessment
Risk treatment
A list of applicable threat scenarios
A list of specific threats including particular threat agents and assets
A list of assessed risks
Selected ways of risk treatment
Identification of suitable tasks
Tasks prioritization
Tasks execution
Review of results and benefits
Predefined tasks
Scheduled tasks and their status
Situation at point t2

Fig. 3 – Risk management process of the OSSF (ArchiMate notation, business process viewpoint).

completed, a review was performed and relevant risks should be assessed again. This triggers another iteration of the Risk management process. Subsequent process iteration may also be triggered by another events, for example, periodic execution according to schedule, changes were performed in online service, a new threat or vulnerability was discovered, new treatments were performed, an important security event occurred or doubts regarding effectiveness or efficiency of performed tasks were raised.

A new process iteration content is based on a previous iteration. So for the new iteration, only necessary modifications must be done which reflect changes in reality. Such approach considerably simplifies performing activities of recurring process iterations, because only previous variables must be modified. This means that all iterations of the Risk management process can be then compared and various reports may be created based on different metrics.

4.7. *Predefined tasks*

Predefined tasks contribute to treatment of risks relevant to threat classes (defined in Section 4.3.6). The tasks are suitable for the most typical situation and of course, additional custom tasks can be added to the OSSF. A list of 27 predefined tasks is contained in Table A2.

4.8. *Software tool prototype*

A supporting SW tool prototype was developed which implements all entities and relations described in this paper. The tool also consists of mappings documented in Appendix and all predefined content like classification schemes and set of predefined tasks. The prototype was utilized to perform verification of the proposed OSSF through a case study documented in the next section.

5. Case study

Verification of the proposed Framework was done through a case study that was performed in a particular organization which acts as online service provider and consumer. The organization can be classified as a large enterprise. The name of the organization is intentionally not mentioned due to anonymity preservation. Instead of the specific name, the word "Organization" is used which refers to that particular enterprise.

The following sections refer to steps of a case study described by Yin (2009).

5.1. *Plan*

The main goal of this case study is to validate quality and usability of the proposed Framework in a real-world environment. Results of the study should assess especially how much the nine objectives (see Section 4.1) were fulfilled and how beneficial was the Framework usage for the Organization.

This case study is based on data about security events related to online services which were collected in the Organization during the second half of year 2015. In the Organization, no formal security risk management was applied for the online services. Therefore, no initial information about risks and their severity could be provided by the Organization. For this situation, reactive risk management approach was applied which means that risks related to particular online services were assessed after a security event occurred. In terms of OSSF, each security event triggered a new OSSF risk management process execution. This approach enabled to create a baseline risk register from the historical data and prepared a way for switching to proactive risk management. This may be perceived as a typical OSSF adoption strategy for organizations which never performed risk management activities. As a side effect, the Organization gained deeper and structured knowledge about security events and vulnerabilities related to individual online services.

5.2. *Design and preparation*

The only reliable source of past security events in the Organization was a security incident database which was provided by the Organization for this study. Only such online services were in scope which had more than one security incident record in the incident database. This condition was fulfilled by total six different online services provided by the Organization.

According to terminology used in this paper, the most of the database records were rather security events. For example, XSS vulnerability was identified in a production environment after a vulnerability scan was performed. A real exploitation of the vulnerability was difficult and no attack exploiting this vulnerability was detected by the Organization in the past. This event was recorded as a security incident but according to ISO 27000:2014 terminology, this record described a security event instead of incident because there was no significant probability of compromising business operations and threatening information security. Furthermore, individual database records which were perceived by the Organization as security incidents contained usually information about more security events characterized as previously unknown situations that may be security relevant. For example, a known vulnerability was fixed which contributed to lowering of a relevant risk score.

The OSSF software tool prototype was utilized during this study. Data were anonymized before entering into the tool and identifiers with no meaning were used instead of particular names. Information regarding security events was kept in its original state as much as possible with respect to preserving anonymity.

Time information precision was limited to one day which was enough for data analysis. Creation date of an analyzed event was perceived as the point of time when the event incepted. It means that a simplification was made because in reality, an event record could be created even few days after it was discovered and moreover, an event might occur much earlier than detected and reported.

5.3. *Data collection*

Data about events which occurred during the 2nd half of 2015 in relation to 6 online services in scope were collected and anonymized according to the Organization's requirements.

For each online service, the first OSSF process instance was executed in the software tool prototype as soon as the first security event occurred. The first process instance was related to the context of the first event. The first process was focused especially on determining applicable threat types and performing an initial risk analysis. In some cases, selection of suitable tasks for risk treatment was performed. The subsequent processes were started after a new security event happened.

5.4. *Data analysis*

After data collection, the actual content of the OSSF software tool prototype was summarized into Table 6.

Within this case study, 34 OSSF processes related to 6 online services were executed which correspond to the total number of security events identified in the collected data. The first process execution date refers to the security event date recorded by the Organization. The initial risk severity is relevant to the first OSSF process and the ending risk severity refers to the end of the investigated time frame (i.e. end of 2015). The risk score value "-" means that no security risks were recorded in the OSSF software tool prototype in the particular point of time.

5.5. *Results*

All results documented in this section were gathered from the OSSF software tool prototype.

Fig. 4 shows how total number of risks grouped by severity was changing during the 2nd half of 2015. The Organization faced only one critical risk from the 27th of July to the 29th. Events with high risk occurred between the 21st and 26th of July and also between the 30th of July and 13th of August. Similar time frames can be read from the graph for medium, low and very low risk frequencies.

Another graph is depicted in Fig. 5 which illustrates maximum and average risk score observed for each online service during the same time frame. Maximum risk score was equal to average risk score for services labeled S1, S3, S4 and S6. Due to this fact, only one joint data series are present at Fig. 5 for those services which represent maximum as well as average risk score together. The first security event was related to the service S2 and occurred on the 15th of July. The highest risk score was found out for service S2 in a period from the 27th of July to the 29th. This finding exactly corresponds with the critical risk in Fig. 4 which was described as full denial of service caused by ongoing attack. During the covered period of time, the lowest as well as the most stable risk score was observed for services S1, S3 and S6. The lowest risk score was

Table 6 – Summary of contents of the software tool prototype.

Service ID	Security events number	First process execution date	Risk severity after the first process execution	Risk severity after the last process execution
S1	4	2015-09-10	low	–
S2	14	2015-07-15	medium	medium
S3	4	2015-11-03	low	–
S4	3	2015-08-21	medium	very low
S5	2	2015-12-11	medium	medium
S6	7	2015-10-26	low	low

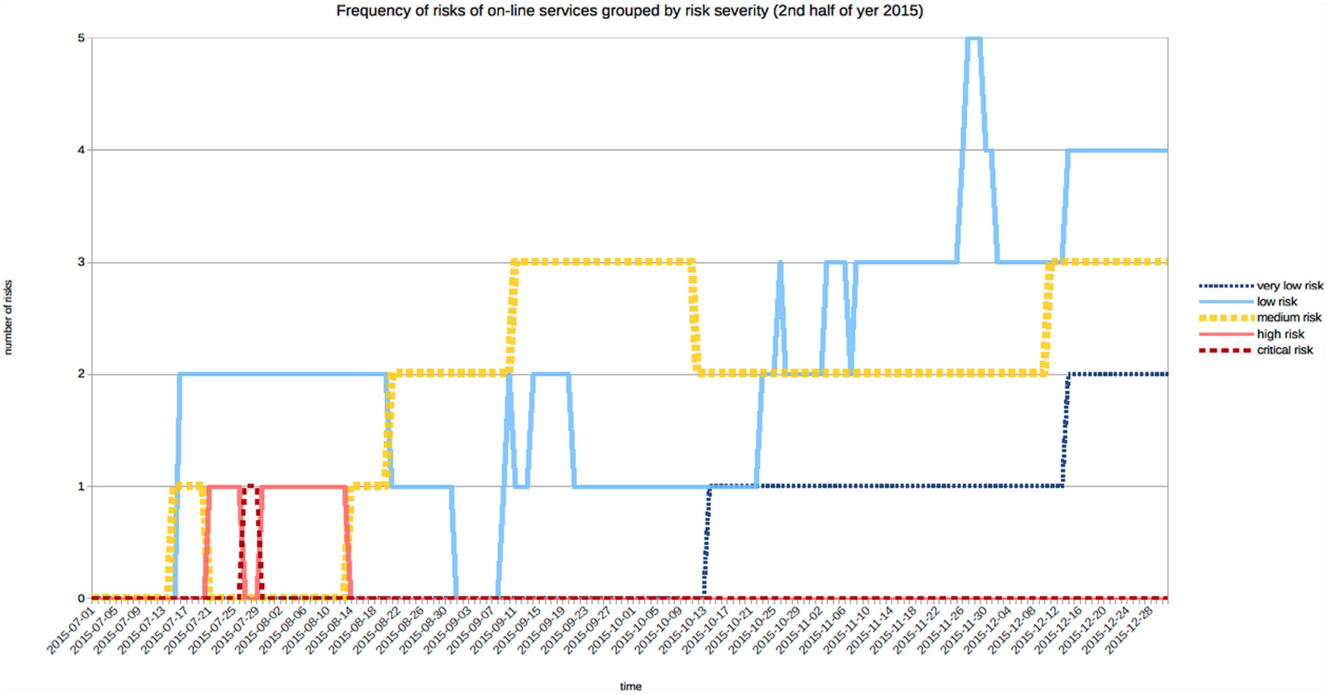

Fig. 4 – Frequency of risks grouped by severity.

reached for service S4 where the score was managed to decrease from 10 to 5 from the 14th of October.

Decreases of risk scores at Fig. 5 were caused by execution of tasks which were planned in consequences of discovered risks. There are those tasks documented in Table 7. In Table 8, numbers of risks by class are documented.

On the basis of the results above, the following action points were recommended to the Organization:

- Improve education of online service developers in areas of vulnerabilities and risks of web applications. Topics related to authentication, session management, cross-site

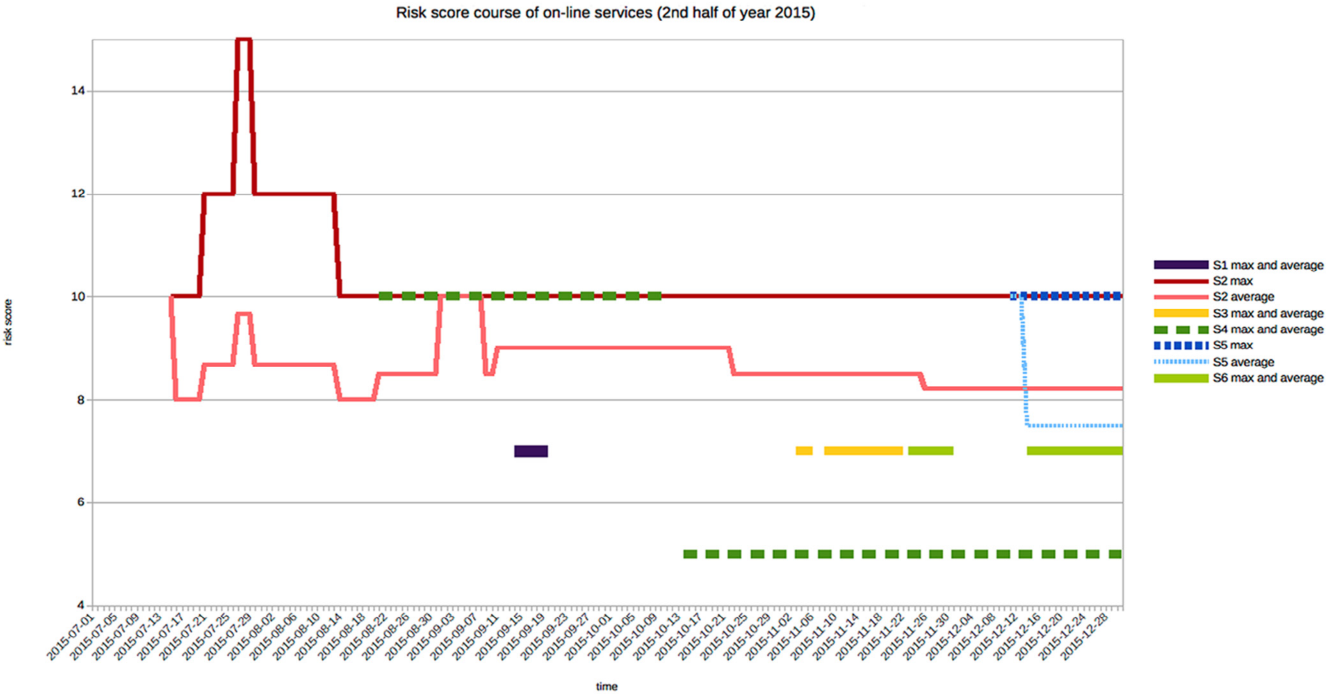

Fig. 5 – Risk score course.

Table 7 – Overview of tasks performed.

Task ID	Task name	Service IDs	Total number of realizations
T2	Code fix	S1, S2, S3, S6	10
T4	Configuration change	S2, S5, S6	4
T7	DoS/DDoS protection	S2, S4	2
T10	Forensic investigation	S2	1

Table 8 – Risk classes summary.

Risk class	Number of risks
Broken authentication and session management	4
Security misconfiguration	4
Cross-site scripting (XSS)	3
Sensitive data exposure	3
Denial of service	2
Unvalidated redirects and forwards	1
Total risks	17

scripting, sensitive data protection and security configurations should be covered in particular.

- The current scope of the web application firewall protection should be extended to more online services.
- Areas vulnerable to DDoS should be identified and DDoS protection should be strengthened.
- Reduce risk score especially for service S2 where the aggregated risk severity was identified as the highest which means between medium and critical levels.

The case study proofed that all objectives defined for the proposed Framework were fulfilled. Rationale and evidence for that conclusion are documented in the Table 9.

6. Discussion

The proposed Framework filled a gap by adding a specific risk management framework focused on online services to the current set of frameworks (see Section 3.2). Main differences and advantages of the OSSF were identified during the case study compared to the current similar frameworks listed in Section 3.4 as follows.

Asset identification and value estimation is not emphasized by the OSSF because a particular online service itself is considered as an important asset at the beginning of the OSSF risk management process.

Various components of the particular online services are of course identified as assets. Nevertheless, this does not happen in the beginning which would require time-consuming decomposition and analysis but after relevant threats are identified. After that, only those assets are considered within the risk management process which can be really affected. Then, potential impacts of exploiting vulnerabilities of assets are determined in context of the online service.

The approach described above enables identification of the weakest security points in an online service and helps to prioritize risk treatment activities.

The Framework stresses on selection and performing of proper tasks leading to successful risk treatment results instead of focusing on extensive analyses.

The OSSF is supported by a software tool which makes usage of the Framework significantly easier. The tool was designed in a way which enforces proper application of the Framework and keeps every records highly structured and consistent.

Apart from the key advantages listed above, there are some areas which require further extensions of the proposed Framework. Groups of threats which are typical to some pre-defined

Table 9 – Objective fulfillment overview.

Objective ID and name	Rationale of fulfillment
O-1 Take dynamic environment of online services into consideration	Dynamic nature is reflected by the OSSF process which is optimized for recurring and frequent iterations.
O-2 Enable usage by both providers and consumers of online services	The case study proofed that the Framework is appropriate for risk management from the provider's viewpoint. Appropriateness for consumers was validated through the Demonstration phase of the DSR process (see Section 2). The Demonstration phase is not contained in this paper.
O-3 Enable usage by organizations of any size and type	Usability was verified in a large enterprise environment. Situations typical for small and middle enterprises were passed during the Demonstration phase (not documented in this paper, see Section 2).
O-4 Increase effectivity and user experience of risk management utilizing a supporting software tool	The OSSF supporting software tool prototype was developed and validated through the Demonstration phase and this case study.
O-5 Enable easy identification of threats	The Threat model component of the Framework facilitates identification of all relevant threats applicable for the particular online service. The threat scenarios and the threat types make discovery of hidden or previously unknown threats easier.
O-6 Enable easy risk analysis	It was proved that The Risk model component of the OSSF is easy understandable and consistent.
O-7 Support proper performing of the right tasks	The OSSF contains a set of 27 predefined tasks. Some of the tasks were utilized within the case study.
O-8 Support recurring analyses and continuous risk management	Even though the first execution of the OSSF process for the particular service may be exacting, the further iterations are based on changes performed in the previous one. During the case study, it was proofed that the changes triggered by various security events can be performed quickly in the software tool prototype.
O-9 Define and use unified taxonomy	Various classification schemes were defined which were utilized within the case study.

cases may be created which would speed up the initial identification of applicable threats. The predefined tasks discussed in Section 4.7 may be described in detail and relevant methodologies, standards, techniques and tools may be recommended.

Further research and development of the OSSF can be focused on metrics and reporting topics. The Framework must be definitely continuously updated in the future, because new kinds of threats and vulnerabilities will arise along with evolution of technologies.

7. Conclusions

In this paper, the novel Online Services Security Framework (OSSF) was proposed. Its main aim is to facilitate security risk management of online services from both provider's and consumer's viewpoints. The Framework was designed in accordance to widely-accepted risk management practices standardized by the ISO/IEC 31000:2009.

The following components comprise the proposed Framework: Threat model, Risk model, Risk management process, Predefined tasks and Software tool. Compared to similar artifacts, the OSSF differs in the initial activities of the security risk management process. Instead of scope definition, asset identification and asset valuation, the Framework's process starts with applicable threat scenarios identification based on the predefined threat scenarios. The process continues with naming of specific threats and linking them to assets (i.e. components of online service) which may be affected. Then, particular risks are assessed and their treatment is performed based on the predefined task set. This approach enables more effective risk management of complex online services through focusing only at the most possible causes of unwanted incidents and at tasks contributing to treatment of risks.

The proposed Framework including all its components was successfully validated by a case study performed in a real environment of a large enterprise. All objectives defined for the Framework in the beginning were fulfilled.

Appendix

Table A1 – Mapping between threats and vulnerabilities.

Threat ID	Threat name	Applicable vulnerabilities
HH.1	Phishing (as a specific social engineering technique)	VH.1, VH.2, VH.3, VH.4
HH.2	Social engineering (other techniques)	VH.1, VH.2, VH.3, VH.4, VH.5
HH.3	Physical observation and surveillance	VH.2
HG.1	Policy issues	VG.1, VG.2
HG.2	Compliance issues	VG.3, VG.5, VG.6
HG.3	Failure of controls	VG.3, VG.4, VG.7
HG.4	Problem escalation issues	VG.5, VG.6
HP.1	Failure to meet SLAs	VP.3, VP.4, VP.5, VP.6
HP.2	Performing unauthorized activities and operations	VP.1, VP.2, VP.4, VP.4
HP.3	Service usage terms violation	VP.1, VP.2, VP.4
HT.1	Fraud	VT.2, VT.3, VT.4, VT.6, VT.8
HT.2	Hacking	VT.2, VT.3, VT.4, VT.6, VT.7, VT.8, VT.9
HT.3	Malware deployment (intentional)	VT.2, VT.6
HT.4	Man in the middle (MitM)	VT.1, VT.2, VT.7, VT.8, VT.9
HT.5	Sabotage	VT.1, VT.2
HT.6	System resources abuse	VT.2, VT.3, VT.4, VT.6, VT.7
HT.7	Theft	VT.1, VT.2, VT.6, VT.8, VT.9
HT.8	Vandalism	VT.1, VT.2, VT.8, VT.9
HT.9	Repudiation	VT.2, VT.3, VT.4
HT.10	Denial of service (DoS, DDoS)	VT.4, VT.5, VT.6, VT.8, VT.9
HT.11	Elevation of privileges	VT.2, VT.4, VT.6
HT.12	Malware infection (unintentional)	VT.2, VT.6, VT.8
HT.13	Mistake	VT.1, VT.2, VT.3, VT.4, VT.5, VT.6, VT.7, VT.8, VT.9
HT.14	Negligence	VT.1, VT.2, VT.3, VT.4, VT.5, VT.6, VT.7, VT.8, VT.9
HT.15	Missing human resources	VT.1, VT.2, VT.3, VT.4, VT.5, VT.6, VT.7, VT.8, VT.9
HT.16	Lack of competences	VT.1, VT.2, VT.3, VT.4, VT.5, VT.6, VT.7, VT.8, VT.9
HT.17	Insufficient management and professional guidance	VT.1, VT.2, VT.3, VT.4, VT.5, VT.6, VT.7, VT.8, VT.9
TP.1	Exhaustion of system resources	VP.1, VP.2, VP.4
TP.2	Issues in specification, design or integration	VP.1, VP.2, VP.3, VP.4, VP.5, VP.6
TP.3	Unapproved or unreported technology or technological components	VP.1
TT.1	Components containing 0-day vulnerabilities	VT.2, VT.4, VT.6, VT.8, VT.9
TT.2	Components containing known vulnerabilities	VT.3, VT.6
TT.3	Configuration issues	VT.2, VT.6
TT.4	Obsolete and/or unsupported technology	VT.1, VT.2, VT.3, VT.4, VT.5, VT.6, VT.7, VT.8, VT.9
TT.5	Weak cryptography	VT.1, VT.3, VT.6, VT.9

Table A2 – Predefined tasks mapped to relevant threats.

Task ID	Task name	Threat ID
T1	Audit logging of users	HI.3, HP.2, HT.5, HT.6, HT.8, HT.9, HT.11, HT.13, HT.14
T2	Code fix	HI.2, HI.3, HI.4, HG.3, HP.2, HT.1, HT.2, HT.4, HT.10, HT.11, HT.13, TI.4, TT.5
T3	Code review	HT.5, HT.6, HT.13, HT.14, HT.16, HT.17, TP.1, TT.1, TT.5
T4	Configuration change	HI.4, HI.5, HG.1, HG.2, HG.3, HP.2, HP.3, HT.2, HT.10, TI.3, TI.4, TT.3
T5	Cybersecurity assurance	HI.4, HG.2, HG.3, HT.7, TP.3
T6	DDoS protection	HT.10
T7	DoS/DDoS simulation	HP.1, HT.10, TP.1
T8	Endpoint devices protection	HH.1, HT.2, HT.3, HT.4, HT.12
T9	Fallback planning	HT.10, TI.1, TI.2
T10	Forensic investigation	all
T11	Fraud detection and prevention	HP.2, HP.3, HT.1
T12	Installation of security patches/updates	HI.1, HI.2, HI.3, HI.4, HI.5, HP.2, HT.2, HT.8, HT.10, HT.11, HT.12, TI.1, TI.2, TI.3, TI.4, TP.1, TT.2
T13	Intrusion detection and prevention	HI.1, HI.2, HI.4, HG.1, HG.2, HH.1, HT.2, HT.3, HT.10, HT.12, TP.3, TT.2, TT.4, TT.5
T14	Monitoring and logging	HI.2, HI.3, HI.4, HI.5, HG.2, HG.3, HP.1, HP.2, HP.3, HT.6, HT.11, HT.13, HT.14, TP.1, TP.3
T15	Non-disclosure agreement arrangement	HI.4, TI.3
T16	Penetration testing	HP.2, TT.1, TT.2, TT.3, TT.4, TT.5
T17	Policy creation / update	all
T18	Privileged access management	HP.2, HT.5, HT.8, HT.9
T19	Security awareness improvement	all
T20	Security configuration review	TT.3
T21	Security controls creation / update	all
T22	Security guidelines creation / update	all
T23	Security requirements specification	HG.2, HG.3, TP.2, TT.3
T24	Social engineering testing	HH.1, HH.2
T25	Threat analysis and modeling	HG.3
T26	Vulnerability scanning	HT.2, TP.3, TT.2, TT.3, TT.4, TT.5
T27	Web application firewall (WAF) deployment	HT.2, TT.2, TT.3, TT.4, TT.5

REFERENCES

Awan MSK, Burnap P, Rana O. Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk. Comput Secur 2016;57:31–46. http://dx.doi.org/10.1016/j.cose.2015.11.003.

Caralli RA, Stevens JF, Young LR, Wilson WR. Introducing OCTAVE Allegro: improving the Information Security Risk Assessment Process. Software Engineering Institute, Carnegie Mellon University; 2007. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419.

Government of Canada. Harmonized Threat and Risk Assessment Methodology. Ottawa; 2007. https://www.cse-cst.gc.ca/en/system/files/pdf_documents/tra-emr-1-e.pdf.

ISO/IEC. ISO/IEC 31000:2009. Risk management – principles and guidelines. 2009.

ISO/IEC. ISO/IEC 27005:2011. Information technology – security techniques – information security risk management. 2011.

ISO/IEC. ISO/IEC 27032:2012. Information technology – security techniques – guidelines for cybersecurity. 2012.

ISO/IEC. ISO/IEC 27000. Information technology – security techniques – information security management systems – overview and vocabulary. 2014.

ITU-T. X.1205: Overview of cybersecurity. 2009. Available from: https://www.itu.int/rec/T-REC-X.1205-200804-I.

Lund MS, Solhaug B, Stølen K. Model-driven risk analysis: The CORAS approach. Springer-Verlag Berlin Heidelberg; 2011. Available from: http://dx.doi.org/10.1007/978-3-642-12323-8.

NIST. Guide for applying the risk management framework to federal information systems: a security life cycle approach. Gaithersburg; 2010. Available from: http://dx.doi.org/10.6028/NIST.SP.800-37r1.

NIST. Framework for improving critical infrastructure cybersecurity. Gaithersburg; 2014. Available from: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

OWASP. OWASP risk rating methodology. 2015. Available from: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S. A design science research methodology for information systems research. J Manag Inf Syst 2007;24(3):45–77. Available from: http://dx.doi.org/10.2753/MIS0742-1222240302.

Rosenquist M. Prioritizing information security risks with threat agent risk assessment. Intel. 2009. Available from: http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf.

von Solms R, van Niekerk J. From information security to cyber security. Comput Secur 2013;38:97–102. Available from: http://dx.doi.org/10.1016/j.cose.2013.04.004.

Yin RK. Case study research: design and methods. 4th ed. Los Angeles, CA: Sage; 2009.

Jan Meszaros is a member of faculty in the Department of Information Technology at the University of Economics in Prague. He is postdoctoral researcher in computer science field; his research focus is information, cyber and ICT security. He works as an information security architect and a security consultant for certain global firms.

Alena Buchalcevova is an associate professor at the Department of Information Technologies, Prague University of Economics in the Czech Republic. She has been working at the faculty since 1981. Her research interest includes software development methodologies, software quality assurance, business informatics management, and enterprise architecture.