Implementation of Information Security System in Service and Trade

Aleksandra Nechai1, Elena Pavlova1*, Tatiana Batova1, Vadim Petrov1,
1ITMO University, St. Petersburg, Russian Federation
*Corresponding author: Elena Pavlova, ea_pavlova@mail.ru

Abstract. Usage of information technologies in service and trade industry is increasing daily which is accompanied by information leakage risks. Information security system can prevent threats from employee’s lack of skills and detect vulnerabilities on early stages. To implement information security system, general steps are to build conceptual model of the subject area, build a semantic network to follow decision making process, adept current situation in company to ISO 27001 requirements and choose information system to atomize business processes. EPC diagram given in this paper shows the steps that service and trade companies can follow to get ISO 27001 certificate. The article describes such security information and event management systems as IBM QRadar security intelligence platform, Splunk Enterprise Security and RSA NetWitness Suite. The results of the research show how implementation of information security policy impact company’s indicators and reputation. Cyber security system’s implementation can lead to low expenses caused by interruption in service or data leakage, increased reliability and security of systems and improved business processes’ optimization.

1. Introduction
In modern society it is hard to imagine a company that does not have a website or at least social media accounts. They are connected with databases of orders, customers information and payment process data such as clients’ credit cards information [1]. It certainly gathers interest from competitors and hackers who can use data in their own purposes. Unauthorized access to employee’ computers, social media accounts or databases can result in leakage of critical information. From the Board of Directors and the CEO to all levels of the team, information security should be everyone's concern and responsibility [2].

Almost every trade and service company has its own mobile app in order to reach the majority of potential customers who make online-orders on the phone. However, most of traditional methods for data protection are not suitable for mobile apps and the risk of information loss is higher than through PC. John Atkinson showed that mobile device apps can inadvertently broadcast personal information through their use of wireless networks despite the correct use of encryption [3]. If a company has an app but does not have a proper information security system applied, it can lead to major problems confidential information and, as a result, a blow to the reputation.

Studies show that one of the main threats to information security comes from within a company itself. Major causes of data losses occur because of employee’s lack of skills related to information security or ignorance of information security policy [4]. Many data breaches continue to result from accidental, intentional or malicious human factors, leading to financial or reputational loss [5].
information security policy, implementing ISO 27001 and atomizing processes with the help of special software not only reduces risks associated with missing vulnerabilities but also increase working team’s awareness of existing problem.

Reasons to implement information security systems are well-known and are mention in most of the article. The aim of the research is to show general method to implement information security management system in service and trade to minimize data leakage risks. The objectives are to define the subject area that need to be taken into the consideration while implementing the system, to build workflow of ISO 27001 standard’s application and to analyse Security Information and Event Management systems’ market to find the most suitable one for Internet trade companies.

2. Methods
In order to implement information security system, it is necessary to formulate certain requirements: who will be using the system, what needs to be analyzed and what business purposes must be fulfilled. First of all, we should acknowledge the subject area of the following implementation and draw up a its conceptual model. The scheme (Figure A) is Entity-Relationship Diagram that illustrates relations between multiple entities such as software, password, host and other [6]. Secondly, semantic network should be built. Semantic networks represent decision making processes in selected subject area [7]. Notes of the graph shows objects in the area and arcs represent relationship between those objects. This network helps to represent data that needs to be stored in future information security system. After building these types of schemes, we should analyze ISO 27001 requirements and plan how to follow them. With requirements formulated and the subject area analyzed, we can compare information systems for information security and choose one to implement in service and trade.

2.1. Conceptual model
The computer security specialist in the organization is most often responsible for information security. An information security specialist monitors host security. A host is any computer or server connected to a local or global network. Each computer has an operating system. The operating system is a complex of interconnected programs designed to manage computer resources and organize user interaction. The computer stores files that are prone to threats. A threat is usually understood as a potential event, action, process or phenomenon that may have an undesirable effect on the system and the information that is stored and processed in it. Threats using vulnerabilities can lead to the destruction, distortion, copying, unauthorized distribution of information, to restrict or block access to it.

Vulnerabilities in service and trade companies can be created by payment transactions which are created by company’s customers. Customers usually use internet shops and pay their orders by credit cards. Client’s credit cards’ information is the most important asset that needs to be protected by information security department.

An information security specialist creates passwords to protect files on workstations. Passwords restrict access to files. In addition to password protection methods, the organization also uses other technical methods of ensuring computer security aimed at restricting access to files. For example, an information security specialist downloads all software updates. Vulnerabilities are mitigated through timely software updates installed on computers. To protect the network ports used in the operation of the software, firewalls are installed. A firewall is a software or hardware-software element of a computer network that monitors and filters the network traffic passing through it in accordance with the specified rules. The firewall blocks and intercepts incoming packets. In computer networks, a packet is a block of data in a certain way that is transmitted over the network in packet mode.

The key business entities are:
- Information security specialist. Entity attributes are ‘name’, ‘e-mail’, ‘phone number’.
- Password. Entity attributes: ‘creation date’, ‘number of characters’, ‘hash function’.
- Software. Entity attributes: ‘name’, ‘installation date’, ‘size’, ‘developer’.
- Network port. Entity attributes: ‘number’, ‘availability’ (available / not available).
2.2. Semantic network

To build a semantic network we will use the objects selected at 2.1. The key concepts of the subject area are the information security specialist and the hosts they monitor. All employees of the company have common properties (including a specialist in information security), so we highlight the general abstract concept – an employee. An information security specialist identifies vulnerabilities by scanning hosts and the software installed on them. Based on this, the notes of the graph will be as follows: “Host”, “Employee”, “Information Security Specialist”, “Software”, “Host Scanning”. The software has vulnerabilities. For this reason, we add the “Vulnerability” to the graph. The main cause of vulnerabilities in service and trade is “Payment transaction” which is another note of the graph. Transactions are initiated by customers, so we add “Customers” and “Credit Card” to the graph as well.

We define relations and their types for the available notes. Let there be an HP Computer host. When a threat message is received, an information security specialist detects the attacked host, determines the source of the vulnerability, tests the software, and in case a software failure is detected, downloads its update.

Based on this, we add the corresponding notes to the graph and connect them with functional relations and relations such as “for example” or “be an instance”. The resulting graph is shown in Figure 1.
2.3. Following ISO 27001 requirements

ISO 27001 is the most widely accepted international standard for information security [8-9]. It shows steps an organization should follow to build its own information security management system, however, none of them are universally mandatory for compliance [10]. Every company has its own regulations depending on its field of activity. In service and trade organizations must protects customers’ data and transactions’ data above all the remaining.

There are 4 phases according to the standard: Plan, Do, Check, Act [11]. First of all, companies need to plan, what will they protect and select the key entities of the subject area. We have already done this in 2.1 by building a conceptual model. In this step organizations should also identify risks and methods to deal with it. The core risks in service and trade companies are [12-13]:

- Loss of payment transactions’ data;
- Loss of client’s personal information;
- Risk of cyber-attack on the website, so customers will not be able to make an order;
- Malware instillation to gain control over corporate network.

Information security department workers should choose one of the strategies to work with risks: accept it, avoid it, reduce it or risk insurance [14-15]. ‘Do’ step means that chosen strategy should be applied and information security policy should be documented. ‘Check’ phase works with policy metrics and effectiveness of the business processes. ‘Act’ involves correcting the processes and policy if it is not as effective as it was supposed to be. EPC diagram shown in Figure 2 reflects main steps a company should follow to meet ISO 27001 requirements [16-17].
2.4. Atomizing information security management system

To make processes more effective it is necessary to implement information system and atomize business processes connected with information security. To gather all the information about potential threats, about audits of information security and atomize incident related business processes companies mostly use SIEM (Security Information and Event Management) systems. SIEM systems
are designed to investigate data to expand the extensive term usefulness and proficiency of infrastructure in information security structure [18].

To make a choice about implementing specific system, we should formulate requirements that it needs to satisfy. Information system needs to:

- Give information security specialists quick access to information about hosts, scanned files, software updates and possible vulnerabilities.
- SIEM system needs to scan all payment transactions and alarm if customer’s credit card information is not secure.
- Have information about potential and current threats to corporate network.
- Have an opportunity to export reports for top management.

According to Gartner magic quadrant for security information and event management for 2018, the leaders on SIEM market are IBM and their IBM QRadar security intelligence platform, Splunk and their Splunk Enterprise Security and Dell Technologies and their RSA NetWitness Suite [19]. They all give needed information for information security monitoring, detect threats and generate reports. Comparative characteristics of the systems are presented in table 1.

**Table 1. Comparative analysis of SIEM systems**

| System                                      | Pros                                                                 | Cons                                                                 |
|---------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|
| IBM QRadar security intelligence platform   | • Can be used either on IaaS or SaaS.                                 | • Is a very complicated tool and it takes a lot of time to learn how to use it properly. |
|                                             | • Consists of various monitoring systems such as log manager, risk manager, vulnerability manager, packet capture and incident forensics. | • Can create false alarms.                                           |
|                                             | • The system is stable and ready for high load rates.               | • Price is available only on demand.                                 |
|                                             | • Detects threats and informs about its effect on IT infrastructure. |                                                                      |
|                                             | • Can analyze users’ activity.                                      |                                                                      |
|                                             | • Has a free trial period.                                          |                                                                      |
| Splunk Enterprise Security                   | • Can work with data from any sources.                              | • Price for a perpetual license for GB daily index volume is $4,500 per GB, which is expensive for small companies. |
|                                             | • Can work with big data effectively.                              |                                                                      |
|                                             | • Gather and process machine data.                                  |                                                                      |
|                                             | • Constantly monitors and investigate activities.                   |                                                                      |
|                                             | • Is famous for its great performance.                              |                                                                      |
|                                             | • Generate reports on incidents.                                   |                                                                      |
| RSA NetWitness Suite                        | • Integrates analytic threat detection and event monitoring.       | • Prices are high - $8200 a month.                                   |
|                                             | • Investigate and analyze threats in network traffic, endpoints and other sources of security events and logs. | • Complex license modelling.                                         |
|                                             | • Uses machine learning to automate and orchestrate the entire incident response lifecycle. |                                                                      |
|                                             | • Has a PCI DSS capability.                                        |                                                                      |
|                                             | • Has a free demo version.                                         |                                                                      |

The analysis shows that *RSA NetWitness Suite* is the best choice for service and trade companies. The reasons are:

- It follows PCI DSS requirements that are essential for Internet trade as it requires total control over payment transactions’ security. Besides, meeting PCI DSS is required to work with Visa and MasterCard in order to accept client’s credit cards that is very important for service and trade.
• The system works with any size of data.
• It has a free trial that is why a company can save money in case RSA NetWitness does not suit their needs.
• The system provides useful log analysis, so it is easier to detect source of threats aimed at payment transactions' information.

3. Results
Implementation of information security system in service and trade can result both in quantitative and qualitative benefits. Benefits from standard’s implementation can also be internal and external [20-22]. Information security is usually considered as a cost with no obvious financial gain. However, we can predict what expenses can be lower if the system is implemented. The list is presented in table 2.

| Quantitative benefits                                                                 | Qualitative benefits                                                                 |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| ISMS saves money that the payment data breach can cost                                | Increased reliability and security of systems and information                        |
| The system reduces the time that it takes to detect a threat                         | Improved management processes and integration with corporate risk strategies         |
| The system makes the expenses caused by interruption in service lower                 | Preventing loss of reputation                                                       |
| The system increases a chance of vulnerability detection                              | Compliance with commercial, contractual and legal responsibilities                  |
| Reduction of time that takes information security specialist to scan files and hosts  | Competitive advantage over companies without ISO 27001 certificate                  |

4. Conclusion
The purpose of the study – form the method how to implement information security management system for service and trade companies – is achieved.

Building conceptual model and semantic network of the subject area is shown as an important part for atomizing information security related business processes. The research describes three of the most popular and suitable SIEM systems to use in service and trade.

The results of the research show that information security system implementation in service and trade can save company’s reputation on the market, gain new clients and prevent loss of critical payment data such as customers’ credit cards’ numbers. With following the steps described in this article and studying ISO 27001 every service and trade organization can implement cyber security system.
Figure A. Conceptual model of the subject area
References

[1] Long L J, Eaganathan U, Sabri N A B 2019 Adopting information system security services in online clothing marketing system using rup methodology under php Journal of Physics: Conference Series 1228 012062

[2] Reece R P, Stahl B C 2015 The professionalisation of information security Computers and Security 48 182-195

[3] Atkinson J S, Mitchell J E, Rio M, Matich G 2018 Your WiFi is leaking: What do your mobile apps gossip about you? Future Generation Computer Systems 80 546-557

[4] Alqahtani F H 2017 Developing an Information Security Policy: A Case Study Approach Procedia Computer Science 124 619-697

[5] Ki-Aries D, Faily S 2017 Persona-centered information security awareness Computers & Security 70 663-674

[6] Kino Y 2018 Conceptual Modeling supported by Text Analysis Procedia Computer Science 126 1387-1394

[7] Martin F R 2019 How Important are Semantic Networks in Artificial Intelligence Analytics India Magazine

[8] Haufe K, Colomo-Palacios R, Dzombeta S, Brandis K, Stantchev V 2016 Security Management Standards: A Mapping Procedia Computer Science 100 755-761

[9] Susanto H, Almunawar M N, Tuan Y C 2011 Information security management system standards: A comparative study of the big five Int. J. Electr. Comput. Sci. IJECSIJENS 11 23–29

[10] Watson M 2019 Requirements for achieving ISO 27001 certification IT governance

[11] Hohan A I, Olaru M, Pirnea I C 2015 Assessment and continuous improvement of information security based on TQM and business excellence principles Procedia Economics and Finance 32 2015 352-359

[12] Grishko E 2017 4 Cyber security threats all companies face and what to do about them Trade Ready

[13] Munteanu A B, Fotache D 2015 Enablers of Information Security Culture Procedia Economics and Finance 20 414-422

[14] Syreyshchikova N V, Pimenov D Y, Mikolajczyk T, Moldovan L 2019 Information Safety Process Development According to ISO 27001 for an Industrial Enterprise Procedia Manufacturing 32 278-285

[15] Kozlov O A, Rodionov D G, Guzikova L A 2018 Information security problems in educational institutions in conditions of network interaction 2018 International Conference on Information Networking 1 267-269

[16] ISO, 2013. ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements. s.l.: International Standardisation Organisation

[17] Qi L, Qingling D, Wei S, Jine Z 2012 Modeling of Risk Treatment Measurement Model under Four Clusters Standards (ISO 9001, 14001, 27001, OHSAS 18001) Procedia Engineering 37 354-358

[18] Mehta A, Abhishek M K 2016 A survey on log correlation in security information and event management with Hadoop International Journal of Advance Research and Innovative Ideas in Education 2 593-596

[19] Gartner 2019 Magic Quadrant for Security Information and Event Management retrieved September 13 2019 from Gartner: https://www.gartner.com/en/documents/3894573

[20] Cots S, Casadesus M, Marimon F 2016 Benefits of ISO 20000 IT service management certification Information Systems and e-Business Management 14 1-18

[21] Marrone M, Kolbe L M 2011 Erratum to: Uncovering ITIL claims: IT executives’ perception on benefits and Business-IT alignment Inf Syst E-Bus Manage 9 381-382

[22] Boiral O 2011 Managing with ISO Systems: Lessons from Practice Long Range Planning 44 197-220