Irmina Chmielowska

Kamil Kwiatkowski

Krzysztof Pochrebiennik

Jakub Wrzodek

Przemysław Gradziński

Information Security Management System

Report

Task 4:

Prepare an Information Security Management System for a health insurance company. The company processes a large volume of medical transactions of their clients and must distinguish fake transactions from the genuine ones. Moreover, the company stores an archive of the transactions for the purpose of calculating future insurance rates.

1. Context establishment

Information security is important for the business, however, its importance is generally underestimated. Main reason is that the profits of high developed information security management system are not easily palpable – their point rely on preventing loss, of any kind. As figures speak louder than words, resulting business losses should be quantified as a consequence of actual, simulated, and hypothetical security breaches. However, we understand ISMS necessity, especially in insurance industry, therefore we put effort into implementing system in our company.

Following document covers necessary points of Information Security Management System, according to ISO/IEC 27005:2008.

* 1. Scope and boundaries
     1. The organization’s main purpose
* provide health insurance services
* providing around the clock information and help via call center
  + 1. The organization's business:
* developing an algorithm for calculating future insurance rates, based on past transactions archives
* storing and processing a large volume of medical transactions data
* monitoring signed contracts and reacting to risk calculations changes (reinsurance etc.)
* observing market prices in order to ensure competitive offers
* constant growth towards gaining new customers and sustain current ones
* investing in employee competences
  + 1. Organization motto

Better health, better life.

* + 1. Organization’s values:
* attention to details
* respect for privacy
* ability to adapt to changing conditions
* quick response to client’s requests
  + 1. Structure of the organization:
* call center department – receiving calls from clients - x people
* sales department - sustain customers, get new ones – x people
* compensation department – claims settlement – x people
* analytic section – group engineers and economists developing an algorithm and analyzing data in order to create profitable contract data – x people
* system administrators - company’s infrastructure maintenance – x people
* accountancy – keeping pay records, archive company’s turnover data – x people
* financial section – making investment decisions – x people
* legal section – taking care of legal side of business – x people
* public relations and marketing – creating positive company image and brand recognition – x people
* human resources - recruiting new workers – x people
* guards receptionists and cleaning staff – x people
* management of the company – making decisions about the company’s operations based upon reports and analyzes provided from departments - x people
  + 1. List of the constraints affecting the organization

* HR constraint: shortage of skilled computer security employees
* Financial: investment priority of stakeholders is mainly focused on visible income, information security is less important matter
* Technical: Large volume of medical transactions and customer data, moreover company uses Libre Office as main office suite
* Legal: General Data Protection Regulation sets additional restrictions on handling customer data
* Environmental: SARS-CoV-2 spread, managers have to work remotely
  + 1. List of the legislative and regulatory references applicable to the organization

The main legal acts related to information security are:

* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation )(Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych))
* Consolidated text of the EP and Council Regulation (Skonsolidowany tekst rozporządzenia PE i Rady (UE) 2016/679 z 27 kwietnia 2016 r.)
* Corrigendum to European Parliament and Council regulation (Sprostowanie do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.)
* Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June

2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem).

* Act of 16 April 1993 on combating unfair competition. (Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji.)
  1. Basic Criteria

As health insurance company we process large volume of medical transactions of our clients and store an archive of the transactions for the purpose of calculating future insurance rates. This directly influences types of criteria we want to adopt, and way we approach them.

* + 1. Risk evaluation criteria

Since we are health insurance company, information safety is crucial for us. Not only because of the company’s prosperity, but also our clients safety and privacy, and numerous legal regulations regarding handling of personal data. We divided risk evaluation criteria in following way:

|  |  |  |
| --- | --- | --- |
| Probability of occurence criteria | Point value | Case |
| Neglible | 0 | An event can occur only in exceptional circumstances (event that occurs once in 5 years), it concerns individual cases. |
| Low | 1 | It is unlikely that this event will occur (event that occurs once per 2 years), it applies to a few cases. |
| Medium | 2 | The event is likely to occur in the near future (event that occurs once per year), it applies to some matters |
| High | 3 | The occurrence of the event is very likely (event that occurs at least once per year). It is expected that such an event may occur several times a year. |

* + 1. Impact criteria

|  |  |  |
| --- | --- | --- |
| Level of impact | Point value | Case |
| Insignificant | 0 | Negligible effect on the objectives and tasks of the organization, no legal effect; slight financial effect, no impact on employee safety, no impact on the image of the organization.  Less than 0,1% of annual income |
| Low | 1 | Little impact on the achievement of goals and tasks, without legal effects, little financial effect; no impact on employee safety, little impact on the image of the organization.  0,1 – 1% of annual income |
| Medium | 2 | The average impact on the implementation of objectives and tasks, potential threats may lead to the failure to perform basic tasks within a specified scope, moderate legal consequences, average financial effect, no impact on employee safety, medium risk of losing good image.  1 – 5% of annual income |
| High | 3 | Serious impact on the implementation of the task, including a serious threat to the date of its implementation and achievement of the goal; extensive legal consequences; threat to employee safety; high financial losses; loss of a good image of the organization in the environment and in public opinion.  More than 5% of annual income |

* + 1. Risk table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk | | Impact | | | |
| 0 | 1 | 2 | 3 |
| Probability | 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 3 | 4 | 5 |
| 3 | 3 | 4 | 5 | 6 |

* + 1. Risk assessment criteria:

• The strategic value of the business information process -> business information process is shaped by future insurance rates, so it is an offer and the opportunity to acquire new customers. Its absence results in a lack of customers.

Impact(2), Probability(2), Risk(4)

• The criticality of the information assets involved -> assessment of the reliability of up-to-date information stored in the company database. Falsification and manipulation of the information could be used to steal goods and collect large amounts of financial money from the company.

Impact(2), Probability(2), Risk(4)

• Legal and regulatory requirements and contractual obligations -> Are the company’s main base, because when they are not strict enough, the potential customer will abuse them by using the company's finances wrongly. When you take into account the criterions on the scale of many customers with potential bad intentions, this can result in the collapse of the company.

Impact(2), Probability(2), Risk(4)

• Operational and business importance of availability, confidentiality and integrity -> build trust with the customer. As an insurance company, health is the key point provide a steady income. Customers will be willing to spend more money by their own will to take out insurance. Otherwise, this will limit the company's revenue to some extent.

Impact(1), Probability(1), Risk(2)

• confidentiality and honesty -> in this case, there are many insurance companies that do not meet these conditions. So the risk margin is remote, however it is good to stand out as a reliable and honest company.

Impact(0), Probability(0), Risk(0)

• Expectations and perceptions of stakeholders and negative consequences for goodwill and reputation ->perception of stakeholders is important, although insurance companies are famous of. If the company is aspiring to reach the richest customers negative reviews will not allow it. However, for most leads, this will not significantly affect.

Impact(0), Probability(1), Risk(1)

Qualitative estimate - scales and attributes eligible to describe the magnitude of potential consequences:

- low; Impact(0), Probability(0), Risk(0)

+medium; ; Impact(1), Probability of occurrence(1), Risk(1-2)

++high;; Impact(2), Probability(2), Risk(3-4)

generally: Impact(7), Probability(8), Risk(15)

• Breaches of information security (e.g. loss of confidentiality, integrity and availability) -> risk of claiming financial compensation by a company client. When security breaches are high, the company is spleened by lawsuits. 5%

• (Reduced quality actions) Impaired operations (internal or third parties) -> Reduced-quality internal activities can bring big losses and put the company at high risk. An example is an error in calculating future insurance rates. Even a small difference can cause the company to collapse. On the other hand, external works of reduced quality, such as marketing, advertising – it will not be as significant and the company will still have a chance to generate profits. 5%

• Loss of business and financial value -> It is worth having these criteria under constant analysis, as it can indicate the reason for the generation of losses by the company and be a good clue to finding mistakes made when managing your business. This will help to minimize the losses generated. 3%

• Disruption of plans and deadlines -> This is noticeable in any larger enterprise and should usually be minimized such distortions, but are inevitable. When paying insurance rates, a margin of several weeks can be adopted so that the company has a constant financial potential, at the expense of a minor reputational downgrade. 2%

• Damage of reputation -> inhibits the growth of future, potential customers and thus limits the possibility of business development. This are important points, however into building the company's reputation. It is difficult to sharply sway the reputation of the company, so this criterion can be considered low risk. 0.5%

• (exception) Breaches of legal, regulatory or contractual requirements -> with high risk and a case of state-owned government shutdown. 15%

impact criteria:

-low; less than 1% of annual income

+medium; 1% to 5% of annual income

++high; more than 5% of the annual

Initial output: 3,1%(5,08%)

* + 1. Risk acceptance criteria

• Business criteria 2,2,4 | 1,1,2|0,1,1|5%, 3%, 2%, 0,5%

Risk acceptance level: 5%

Risk status: 4,725%

• Legal and regulatory aspects 2,2,4|5%, 15%

Risk acceptance level: 30% for infringement of legislation up to 3months

Risk status: 40%

• Operations |5%, 5%, 3%, 2%

Risk acceptance level: 15%

Risk status: 20%

• Technology 2,2,4 | 5%, 2%

Risk acceptance level: 8,75%

Risk status: 10%

• Finance 2,2,4|5%, 3%

Risk acceptance level: 10%

Risk status: 8%

• Social and humanitarian factors 2,2,4| 1,1,2|0,0,0|0,1,1|5%, 2%, 0,5%

Risk acceptance level: 5,62% for infringement of legislation up to 6months

Risk status: 8%

((ΣImpact + ΣRisk)/ ΣProbability) \* impact criteria

* 1. Development of the information security risk:

The appropriate information security risk management process should be tailored to the nature of the organization. For the health insurance company should be established assessing the reality of transactions system. To manage risk, must be develop a plan to assess the severity of the hazards and identify potential hazards.

* + 1. Archiving of important records:

The specification of records that should be kept is the basis of any risk assessment system. Records should contain relevant information from the point of view of the health insurance company, such as:

* date of recording (date of transaction execution)
* transaction process
* transaction result (if it was found to be false or true)
* parties involved in the transaction
  + 1. Establishment of important relations between the parties

It is extremely important for the proper functioning of the organization to determine the relationship between this organization and the units with which it cooperates under the system being developed. For the health insurance company, it is crucial to establish the relationship between it and private clients as well as entire companies.

* + 1. Definition of decision escalation paths

Inadequately designed decision escalation paths can destroy entire projects by complicating the production and development process. Regardless of the company's sector, decision escalation paths should be:

* easy to read and understand
* uncomplicated (minimizing the number of paths)
* flexible (easy to update)
  + 1. Definition of the responsibilities of internal and external parties

Establishing internal obligations is a requirement for the functioning of each organization. Creating an appropriate hierarchy of responsibility and controlling positions allows ensuring the proper functioning of the organization. Determining the liability of external parties is part of the contract. Therefore, they are obliged to fulfill specific responsibilities.

* + 1. The hierarchy of persons responsible for ISMS

Four important roles make up the Information Security Section. The Information Security Section is in cooperation with the legal department. Main person in the responsible for ISMS hierarchy is the Information Security Officer. He has to coordinate all activities related to the ISMS and communication of information relating to ISMS in the Organization. Information Security Officer appoints three deputies focused on a specific sector of responsibility:

* network and software security
* organizational procedures and updates of ISMS
* physical security and surveillance systems

1. Risk assessment

TU WKLEIĆ

2.1.1.3 Identification of existing controls

To identify and evaluate state of existing controls, following activities have been carried out:

* Reviewing documents containing information about the controls: risk-related documents, risk treatment plans
* Interviews with the people responsible for information security and the users as to which controls are really implemented
* Comparing implemented physical controls with the list of what controls should be there, and checking for correctness and efficiency.
* Reviewing results of previous internal audits

Existing organizational and legal controls:

* Security awareness trainings for new employees
* Every employee has to sign NDA
* Agreement with security company - if alarm is raised, armed employees have to arrive within 5 minutes

Existing physical controls:

* Alarm system
* Doors and windows have anti-burglar reinforcements

Existing IT controls:

* All data about clients and transactions are securely encrypted
* Emails are sent signed and encrypted
* Regular checking for software updates
* Company is using Kaspersky Internet Security on every computer
* Fake transaction distinguishing algorithms
* Users have limited access rights to company computers
* USB ports are monitored