sciendo CzOTO 2019, volume 1, issue 1, pp. 156-162

CREATING VALUE ADDED FOR AN ENTERPRISE BY MANAGING INFORMATION SECURITY INCIDENTS

doi: 10.2478/czoto-2019-0020
Date of submission of the article to the Editor: 02/12/2018
Date of acceptance of the article by the Editor: 25/01/2019

Żywiołek Justyna[1] – *orcid id:* 0000-0003-0407-0826
Alberto di Taranto[2]– *orcid id:* 0000-0001-8189-4103
[1] Czestochowa University of Technology, **Poland,** *justyna.zywiolek@wz.pcz.pl*
[2] CEO of Tyto srl

Abstract: This article presents the structure and analysis of information security incidents in a production company in 2015-2017. The purpose of the analysis is to identify incidental events and their frequencies. The analysis includes the occurrence of notifications, threatening events, employee errors and false alarms. The conducted research includes also the procedure for handling the incident in the enterprise. The enterprises very often avoid informing their contractors about the occurrence of incidents. Thanks to the analysis of incidents and a clearly defined action plan, the examined enterprise tested the incidents and actions taken with them as a method of creating the added value of the enterprise during the period under consideration. The conducted research has shown that contractors who are aware of preventive actions taken, as well as those affecting information security even after the occurrence of an incident, are more willing to provide trust and even support to the surveyed enterprise. The conducted analysis is a pilot study carried out in one large enterprise in the metallurgical industry. The aim of the conducted research is to show that the incident or negative event may have a positive impact on the company's image. The research was carried out with the use of a questionnaire and in-depth interview with representatives of enterprises that are co-operators of the examined company.
Keywords: incident service, management of information security incidents, creation of value through information security

1. INTRODUCTION

Security-threatening events can occur at any time and place, including information security. Therefore, the enterprise is a place of potential threats that may occur for many different reasons. The purpose of this analysis is to show that events potentially decreasing the value of a company (incidents) can become a driving force for action, and managing incidents in the right way can become a factor that builds trust and creates value of business among contractors. The study was conducted on the basis of data provided by the metallurgical and multi-faculty enterprise.

Man's natural aspiration is to ensure his safety and his surroundings. Every person, work or social group undertaking actions aimed at exerting influence on the environment in such a way as to eliminate any threats, ensures safety (Żywiołek, 2016). Situations threatening human safety, and which can occur at any time and in

any place, are commonly called threats. Therefore, every person lives in an environment of potential threats that may occur as a result of changes. The level of security is a component of many elements that may occur in specific situations, individually or in specific combinations (Szymonik, 2010). One of the elements influencing the security of an enterprise is the management of information security incidents. Effective management of information in crisis situations can be implemented by managing activities around incidents. The implementation of activities and procedures related to information security does not ensure full physical and IT security, because there may be events that could not be predicted during implementation. Therefore, in the interests of raising the level of security, the system ensuring safety must be improved. This is supported by implementation and post-implementation activities, which include incident management and business continuity assurance (Żywiołek, 2018).

Incident management as an element of creating a security system

The importance of risk analysis has been emphasized in literature many times. The risk measure is estimated, developed on the basis of partial assessments, defining the possibility of adverse events (Peltier, 2002). Such estimates require confrontation in real conditions in the enterprise. The basic tool used for this purpose is the management of incidents, which consists in the permanent collection and analysis of all types of events related to breaches of the security system.

Incident management supports risk analysis, verifies the estimated results obtained in the course of risk analysis and facilitates their use while introducing necessary improvements in the enterprise security system. In each enterprise, a procedure should be developed and implemented for the occurrence of an incident whose main element is the IAS incident analysis scheme. As part of these activities, the incident management process consists of (Osborn, 2006):

- collecting information about events that may turn out to be incidents according to the criteria set by the company ,
- ongoing analysis of the results of the risk analysis,
- applying recommendations regarding correct incident response methods.

These activities support the process of safety management and are carried out on a regular basis during the operation of systems (Axelrod, C.Wet al., 2009). In addition, there are carried out general actions for which reaction and threat factors are not at a critical level. Conclusions from threat analysis and incident analysis should be reflected in training materials and those distributed among employees.

Training of incidents, not necessarily registered in an enterprise, may be an excellent training material. Such behaviour corresponds to the implementation promoted in the security policy, it also supports the principles of learning from own mistakes or those committed by others.

Proper management of incidents not only reduces the risk of incidents in the enterprise, but also (Wołowski, Zawiła-Niedźwiecki, 2015):

- enhances the effectiveness of the process of risk analysis and reviews accompanying the security management,
- supports preventive activities, as it improves the staff’s alertness and general knowledge level,
- raises the level of security awareness, because each incident carries the hallmarks of warnings,

- provides warning information for partners and the company.

Incident management in creating enterprise added value

Incident management is carried out according to a fixed action plan, clearly defined in the incident analysis scheme. Table 1 presents the framework for such a plan, and there are seven aspects distinguished in it.

It is known that the company as a system is subject to constant changes also in the field of security. Improvement of the system requires knowledge about the properties and safety parameters before and after changes in the security system, therefore it should be possible to assess their impact on the overall security of the company.

Table 1

Elements of incident management plan

Lp.	Contents of the plan
1	preparatory actions to achieve readiness to detect and respond to incidents
	preparation of procedures, training for employees
	establishing general rules of conduct
	gathering documentation of the security system, directly related to incidents
	correlation with the business continuity plan
	detailed rules on registers and journals
	training
2	detection of events indicating the possibility of an incident and the first reaction
	detection of symptoms, anomalies
	notification according to the notification scheme
	handling and responding to the incident
	reporting
3	event assessment procedures
	explanation of the causes of the incident
	determination of seriousness
	selection of remedies
4	reacting, reducing consequences and notifying management
	repel the attack
	limiting damages
	notifying management
5	replay after the incident
	restoration of the condition from before the incident
6	drawing conclusions from incidents
	determination of the causes
	estimation of the amount of incurred damages
	confrontation of the incident with forecasts
	applying the principle of learning from mistakes
	implementation of corrective actions
7	improvement of incident management system
	analysis of incidence trends
	review of procedures
	exchange of information and analysis of incidents with partners
	cooperation with partners in the area of mutual warning

In an illustrative way, the actions improving the security system are presented in Figure 1.

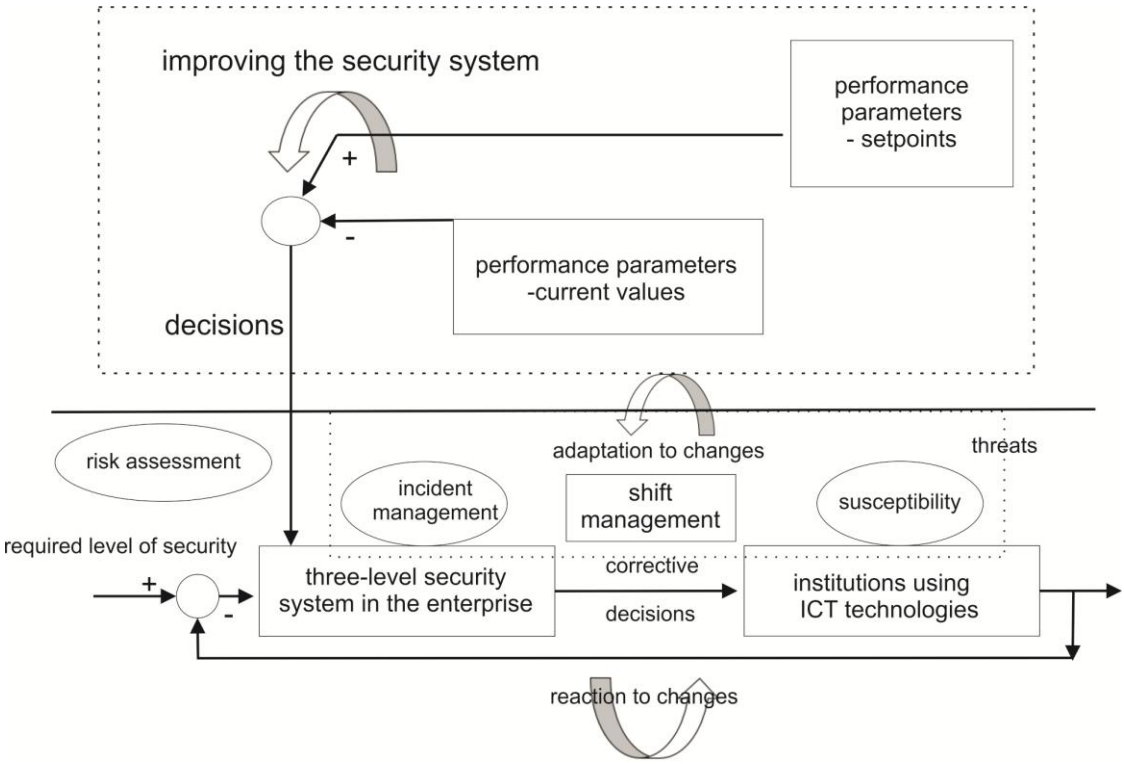

Fig. 1. Improving the company's security system

The lower part of Figure 1 shows the security system that keeps the risk as low as possible and has the ability to adapt to changes taking place in the company's systems. The upper part represents an additional, superior feedback loop responsible for improving the company's security system.

Incident management process is the main source of information on the effectiveness of the security system. They are collected and analyzed, carefully observed trends of different types of threats are tracked. On this basis, corrective decisions are made.

There is also a possibility of improving the efficiency of the security system. For this purpose, enterprises can organize mutual exchange of warnings and information gathered from the analysis of incidents. This may be a source of additional benefits (Grodzki and Piech, 2017):

- a more efficient incident response process,
- smooth transfer of warnings,
- comprehensive trend analysis, when the company owns a larger collection of cases for analysis,
- better prevention, thanks to the use of the experience of others.

In order to ensure information security, there has been created a hierarchy of events that appears in the global and internal environment of the company. They can also threaten a man, his surroundings and even the whole company. The structure of the occurrence of individual types of events divided into months is shown on Figure 2.

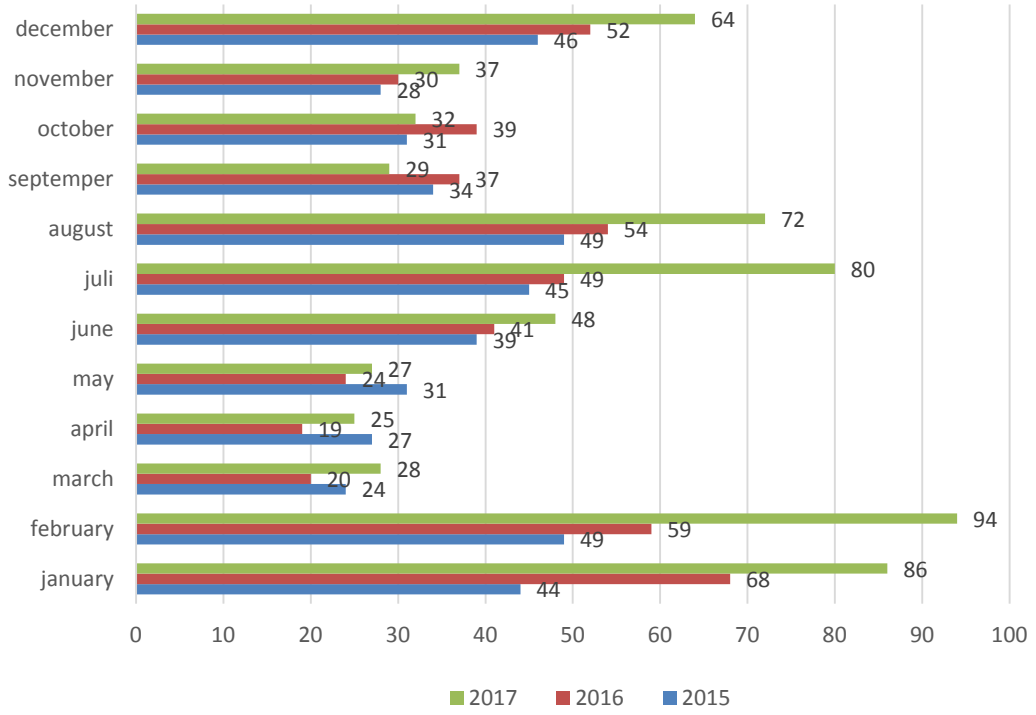

Fig. 2 Reporting events that threaten information security

The next figure (Figure 3) shows the actions taken by the surveyed company to prevent incidents.

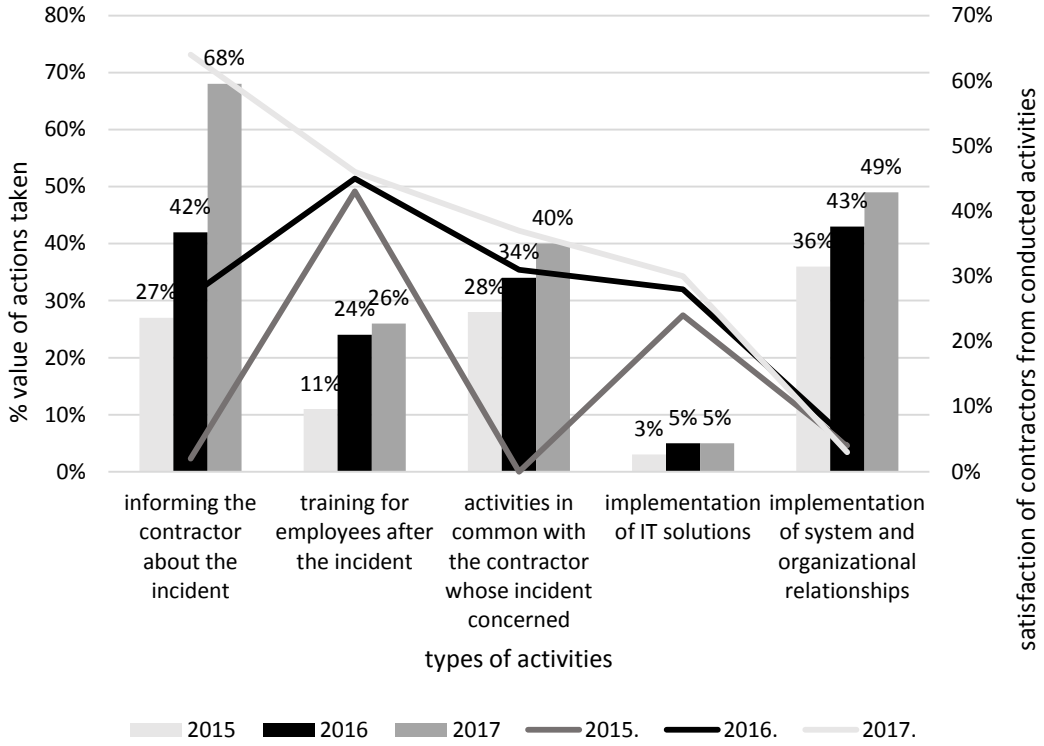

Fig. 3. Actions taken to prevent incidents with indication of contractors' satisfaction with the actions taken

The columns of the chart represent real actions taken by the company in individual years. There is a noticeable increase in awareness and, consequently, an increase in the number of undertaken activities, only an imperceptible increase takes place in the implementation of IT solutions, the barrier of which is the issue of finance. The auxiliary lines illustrate the satisfaction of the contractors of the actions taken. It is easy to notice that understanding the activities undertaken by the surveyed company required time. The contractors believed that the normal operation is the use of training and subsequent system implementations for the examined enterprise. However, at the beginning they did not accept informing them about incidents, they treated it as a mistake of a co-operator and not as its honesty and willingness to care for the value of the contractor's company.

2. ADDED VALUE - INCIDENT MANAGEMENT

Added value is a competitive advantage that has a big impact on creating the company's popularity and its image. This effect is desired by specialists dealing in many different fields, but none of the marketing companies recommend bragging about incidents. They recommend innovation, transport, warranty, that is everything that the competition in the given industry cares for. Nobody boasts of the mistakes made, the companies try to hide them from contractors, mask their mistake, deny it, which can result in customer loss. Each company should focus not only on the needs of customers, but also be able to use their activities in their favour. It is inevitable that the contractor will learn about the occurrence of the incident. Therefore, a better solution is to learn from us, know what actions have been taken, provide support to prevent further incidents. The created added value is shown in Figure 4.

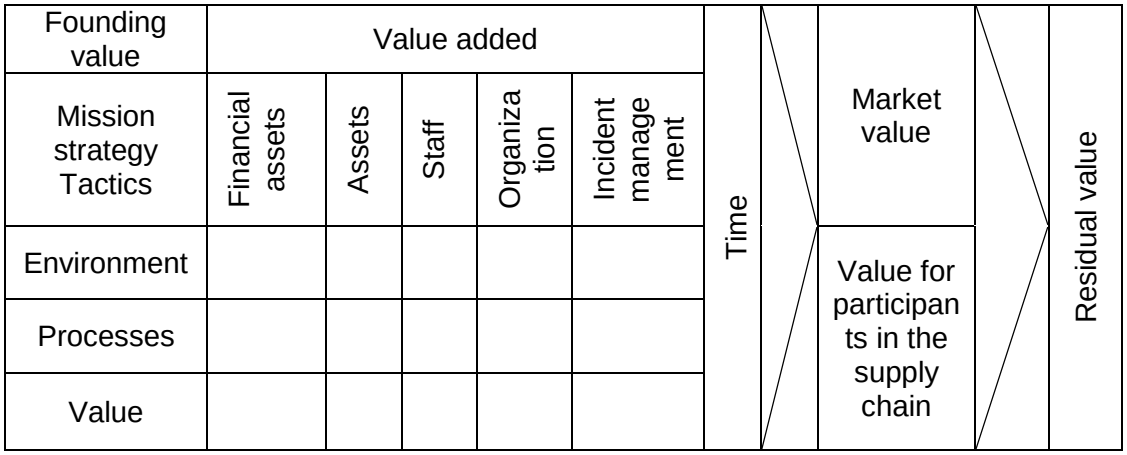

Fig. 4. Creating value by managing an incident in an enterprise

The value of the company affects its competitiveness. The conducted research has shown that over time, the contractors show increasing satisfaction with the conducted activities in the scope of incident management, which has a positive impact on the added value of the examined enterprise.

3. CONCLUSION

The reason for the study was the previous numerical analysis regarding the occurrence of information security threats. Their repeatability led to the analysis of events over time. These studies showed the causes of incidents and their frequency.

Disturbing results of the research led to the creation of a research question about the consequences of their occurrence. If it is impossible to eliminate them to zero, there should be taken such actions that would not cause the loss of customers only because of their occurrence.

Despite the initial resistance of the management and owners, they agreed to inform about incidents and actions taken against them. Counterparties reacted in a bad or neutral way until there was a meeting in order for the authors of the in-depth interview to make them aware that the incident also relates to their data, so it also threatens their business. Building awareness allowed to create a plan of joint action, thanks to which trust is built among cooperating companies, which constitutes the added value of the examined enterprise.

Reference

Axelrod, C.W., Bayuk, J.L., Schutzer D. (eds.), 2009. *Enterprise Information, Security and Privacy*. Artech House, Norwood.

Białas, A., 2007. *Bezpieczeństwo informacji i usług w nowoczesnej firmie*. WNT, Warszawa.

Borowiecki, R., Kwieciński, M. 2003. *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji*. W stronę integralności przedsiębiorstwa, Zakamycze, Kraków.

Brdulak, H., (eds.), 2012. *Logistyka przyszłości*. PWE, Warszawa.

Bugajski, J., 2018. http://www.zabezpieczenia.com.pl/bezpieczenstwo-it/bezpieczenstwo-aplikacji-biznesowych-czesc-1-bezpieczenstwo-sieci?Itemid=200 (2.10.2018).

Calder, A., 2005. *A Business Guide to Information Security*. Kogan Page, London.

Ciecińska, B., Łunarski, J., Perłowski, R., Stadnicka, 2006. *Systemy zarządzania bezpieczeństwem w przedsiębiorstwie.* Oficyna Wydawnicza Politechniki Rzeszowskie, Rzeszów.

Fischer, B., 2000. *Przestępstwa komputerowe i ochrona informacji.* Kantor Wydawniczy Zakamycze, Kraków.

Klonowski, Z., 2004. *Systemy informacyjne zarządzania przedsiębiorstwem*. Modele rozwoju i własności funkcjonalne, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław.

Kolbusz, E., 2010. *Analiza potrzeb informacyjnych przedsiębiorstwa*. Wyd. Uniwersytetu Szczecińskiego, Szczecin.

Łuczak, J., Tyburski, M., 2010. *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań.

Majdecki, M., 2005. *Zarządzanie bezpieczeństwem informacji*. Forum Jakości, 1.

Mottord, H.J., Whitman, M.E., 2008. *Management of Information Security*. 2nd ed., Thomson, Boston. Osborn, M.

Polaczek, A., 2006. *Audyt bezpieczeństwa informacji*. Helion, Gliwice.

Stewart, G., 2009. *A safety approach to information security communications*. Information Security Technical Report, 14.

Żywiołek, J., Staniewska, E., 2012. *Zagrożenia zarządzania bezpieczeństwem informacji w przedsiębiorstwie*. Logistyka, 6.

Żywiołek, J., 2018. *Monitoring of Information Security System Elements in the Metallurgical Enterprises*. MATEC Web of Conferences, https://www.matec-conferences.org/articles/matecconf/pdf/2018/42/matecconf_qpi2018_01007.pdf, 2018.