

HUMAN FACTOR IN THE PROLIFERATION OF THREATS

M.Szyłkowska. PhD.¹

Faculty of Logistics – Military University of Technology, the Republic of Poland ¹

Monika.szylkowska@wat.edu.pl

Abstract: The article contains considerations regarding in the area of the so-called human factor as a potential source of hazards and proliferation of threats. The issues of conceptual and definition matter as well as selected types of threats were analysed - including attacks of type inside-job and generated by social engineering methods.

Keywords: HUMAN FACTOR, PROLIFERATION OF THREATS, INSIDE-JOB ATTACKS, SOCIAL ENGINEERING

1. Introduction

Human capital has always been one of the key factors that allowed both to gain the competitive advantage, but in particular – the creation of intangible elements of the security environment. *A contrario*: man is thus a potential source of threat and its proliferation.

The security environment is affected by certain conditions, which include: chances, challenges, risks and threats of the implementation of interests and the achievement of goals in the field of security. Chances include all – regardless of the will of the subject – circumstances (phenomena and processes), which are conducive of the implementation of interests and the achievement of the intended goals. Challenges include the decision-making dilemmas and choices that a given subject faces, including the necessity of incurring specific costs. Risks are uncertainties connected with a particular action and its consequences – including the potential risk of adverse effects of the action taken. The principle is to increase the level of risk directly proportional to the level of activity (e.g. an increase in terrorist threats due to involvement in international operations). For this reason, the skilful estimation and reduction of particular risks is becoming ever more important. While threats are the direct or indirect destructive influences on the subject. Threats are a classic environmental factor. The strategic objective of each subject is (or should be) to ensure safe conditions for the implementation of interests by: reducing identified risks, eliminating threats (external and internal), proper estimation of challenges and skilful use of the occurring chances by making proper decisions.



Fig. 2 Enviromental conditions

2. Types of risk

When analysing the concept of risk, it is worth indicating the definition *The EFQM Framework for Risk Management* – according to which: the risk is a *combination of the possibility of occurrence of any event and its consequences* [1]. In each subject, the risk is present in all processes taking place (e.g. IT, logistic and management). The risk phenomenon can come from both the external environment and its interior. *Taming the risk* in a given entity and developing appropriate control mechanisms along with the ongoing monitoring of the course of processes and assessment of the degree of implementation of the adopted goals are crucial. Management in each subject is a sequence of decision-making processes and creating conditions for effective implementation of these decisions.

Table 1: Classification of factors affecting the risk

	External risk	Internal risk	Time horizon	Variability of the environment
Shaping factors	Political	Management	Strategic	Static
	Social	Organization	Operational	Dynamic
	Legal	Human capital and resources		Fixed
	Economic	Financial		Variable

Only some factors shaping the environment allow their *taming* and adaptation within the functioning of the subject. Particularly variable external factors remain, for objective reasons, beyond the reach of influence (see Table 1). However, there is no doubt that internal risks belong to the most important group and the subject has the greatest impact on them – in particular on the possibility of control over them.

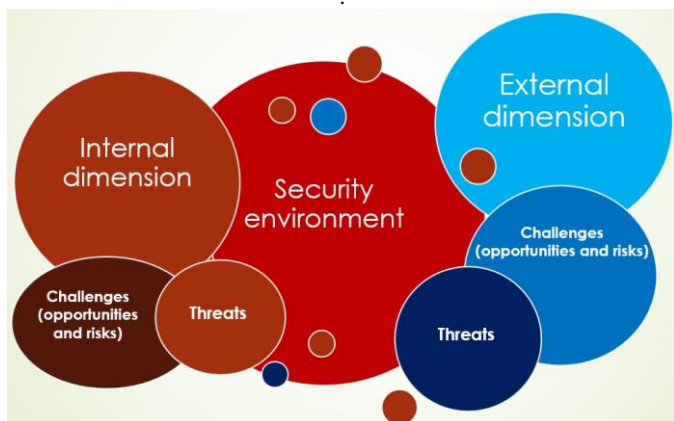


Fig. 1 Security enviroment

3. Type of threats

The general classification of threats is determined mostly by their identification. Due to the accepted criterion – a division can be done into individual groups – the main one, which can include: internal and external threats. Among them, the following can be distinguished: political, economic, social, natural (including ecological). Therefore, a criterion of threats can be adopted for a given subject, then the division into internal and external threats will be subjected to a more detailed identification – including the area of functioning and specific ambient conditions. The internal threats (the source is located in a given subject) can include – in addition to those indicated in Table 1 – more precise, e.g.: device failures, deliberate attacks by employees or unintentional human errors. Due to the type of reason caused by the threats, one can distinguish:

- a) unintentional (unintended) – resulting from random causes or caused by errors of the employee;
- b) intentional (intended) – being the result of a conscious human activity.

Due to the type of losses incurred, the following risks can be distinguished: not causing financial losses and threats causing them. The extent and significance of the consequences of threats may determine further classification, e.g.: significant ones, or causing disruption in the functioning of the subject – and even: threatening further existence.

4. Man as a source of threat

As K. Mitnick rightly states: *Experience and statistics say that the biggest threat for the company comes from employees. They have the detailed knowledge of where to store important information and know where to hit to cause the most damage* [2].

These types of actions are referred to as *inside-job* attacks. According to the studies of the German Federal Office for the Protection of the Constitution, the ration of external attacks to internal attacks amounts to as much as 30:70 [3]. The most common types of internal attacks include:

- database thefts;
- modifications, permanent deletion and/or theft of databases;
- violations of internal security procedures;
- theft or damage to devices on which data is stored;
- attacks on users' passwords and installing malware in the network.

In turn, according to the results of *Studies on the State of Information Security* PwC [4], the main source of incidents and threats is the immediate environment of the company – in particular, the people employed (33%). 13% of respondents indicated the former employees, while 6% - contractors, current service providers or consultants. It should be emphasized that internal attacks may result from intentional or unintentional actions of employees, although – as a rule, it is assumed that in the case of data, they are committed intentionally.

Implications of the *inside-job* attacks include, in particular: loss of key information and databases, loss of technology; loss of licences and access, break in business continuity or costs of restoring full functionality.

Every employee who has not only knowledge but also access to sensitive information is a potential source of the greatest threats. However, apart from intentional actions, one should also indicate circumstances that may favour the materialisation of threats resulting from: light-heartedness, lack of knowledge – resulting from, among others, the lack of adequate training, lack of security

policies and procedures, or poor system security at the functional level of the entity. Among the reasons outside the employer, the individual characteristics of the employee should be indicated, such as: negligence, disloyalty or susceptibility to property benefits. The fact that employees themselves often unintentionally disseminate information and resources because they are not aware of its importance or the risk of losing it is of considerable importance. According to the research results indicated above, as many as 41% of the causes of security incidents were a mistake of an employee – in 15 % - the use of an employee through the use of sociotechnical methods.

Examples of actions and behaviour of employees/users include, among others:

- a.) opening a dangerous link or file received by e-mail – resulting in encrypting data on the computer/network/ or preventing the system from being used;
- b.) making a transfer to a false bank account sent in a prepared message by persons impersonating an existing contractor;
- c.) providing sensitive information about the company in publicly accessible places (e.g. a social networking site).

The social engineering methods include: impersonating a known institution or person to extort information or cause a specific behaviour – negative in consequences for the employee – the user.

The most commonly used are:

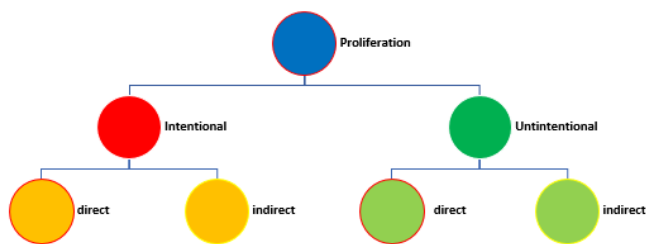
- a.) delivering the dangerous content of the attachment under the pretext of relevant information (e.g. courier delivery, allegedly calling the law firm to abandon unfair competition, calling or requesting to make a payment for an invoice). The result of such an action is usually the blocking of access to the resources of the device on which the malicious software was installed along with the demand to pay the ransom (so-called cyber-trap or cyber-ransom) for unblocking access. It should be emphasized that often paying a fee does not cause the restoration of functionality;
- b.) impersonating an enterprise or institution, and then sending information about the alleged change of the company's current account in a prepared message, to which payments should be made (using real data of the entity).
- c.) extortion of money for an alleged user account blockade and a request to pay a specific amount for unblocking access.

In addition, it is worth emphasizing that digitalization of employees' lives is also important. Social networking sites where they share information from their private and sometimes professional life make them vulnerable to becoming the target of an attack or being used as a *carrier of threat*.

5. Proliferation of threats

Proliferation of threats by man can be done in a dichotomous way: indirect or direct and intentional or unintentional. It can also take place in combinations:

intentional – direct, intentional – indirect; unintentional – indirect; unintentional - direct.



Scheme 1: Proliferation compilation

It can refer to both the organizational, functional and information level – access to resources or data. Additionally, proliferation may occur as a threat *redirection*. In the case of the information level, the risk proliferation may concern, among others: disruptions in the flow of information, intentional or unintentional dissemination of disinformation, but also modification or data or information resources that constitute an element of a decision-making process. In the case of the theft of resources or information, the proliferation of the threat may result in, e.g. disruption of the subject's functioning. Redirecting the threat involves the possibility of its unconscious initiation and materialization, and then further transfer (e.g. redirection of a dangerous attachment to another employee). Uncontrolled and unintended proliferation of threats may also result from the lack of adequate knowledge and training of employees. The same process applies to the possibility of raising the level of risk. The so-called *human factor* can therefore be: the source of threat, its carrier or proliferation element. The indicated division is not exclusive, which means that a human can appear in three described forms together, in a specific sequence of processes, i.e.: become a source of danger, then its carrier and then – proliferation element.

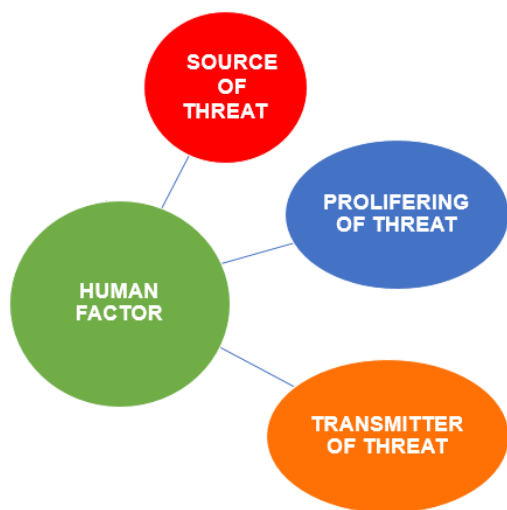


Fig.3. Taking into account the share of a human factor in the compilation of threats

6. Results and discussion

According to the research results of the 19th World Information Security Study of the EY Company "The road to cybersecurity: detect, protect, react [5], the most likely sources of attacks include: employees (57 %), while the main vulnerabilities include: light-hearted or uninformed users (38 %), obsolete security mechanisms

(35 %), the use of mobile technologies (16 %) and the use of social media (7 %).

The most important tasks in the area of minimizing the risks implied by the so-called human factor and minimizing the risk of their proliferation include: identification and introduction of safety rules and procedures adapted to a specific structure and area of the subject's functioning. The methods aiming at minimizing the risk of human attacks – including the *inside-job* include, among others the behavioural analysis and the analysis by indicating deviations and anomalies in individual processes. According to experts, even basic training only in the field of information security and data protection are able to eliminate the main part of the risk resulting from the lack of knowledge or carelessness. He security policy and dedicated procedures should be clear and accessible to employees at all levels. In turn, technical security should be supported by a proper access control and authorization system to secure the most sensitive resources. It is also a good practice to conduct regular audits.

6. Conclusion

Undoubtedly, man is the fundamental and key *element* in any system. In the security environment of the subject, he will fit within its internal structure. In the aspect of information systems, man is: the creator, the sender, the recipient and the manager of information, and the potential *source of threat* and the target of attack. The referenced statistics indicate that the so-called human factor is also decisive in the functioning of entities, and also where it is the most common and susceptible vulnerability or source of danger. In conclusion, it should be noted that the proliferation of threats by the so-called human factor for an organization is an identified phenomenon that confirms the conducted research. This fact means that security policies and dedicated procedures should absolutely include such a factor as crucial for the functioning of a given organization. Only then they will be effective in terms of security, enabling both risk minimization and the ability to adequately respond to them – at every organizational level. Moreover, the actions indicated should also take into account the possibility of risk proliferation – and thus – provide for appropriate *ex ante* and *ex post* procedures. It is also vital to include the time factor in all the specified elements to minimize risk and respond to the already formed threats, creating a decisive element in this respect in terms of effect.

7. References

- [1] EFQM, *The EFQM Framework for Risk Management: Driving Excellence in Risk Management*, European foundation for quality management, ISBN 9052365725, 9789052365725
- [2] Mitnick K., Simon W., *Sztuka podstępny. Łamalem ludzi, nie hasła*, Wyd. Helion, 2011
- [3] Daszkiewicz K., *Bezpieczeństwo w firmie - największe zagrożenie kryje się wewnątrz*, PCWorld from IDG, source: <https://www.pcworld.pl/porada/Bezpieczenstwo-w-firmie-najwieksze-zagrozenie-kryje-sie-wewnatrz,403951.html>
- [4] PwC *Badania Stanu Bezpieczeństwa Informacji - Globalny stan bezpieczeństwa informacji*. Source: <https://www.pwc.pl/pl/pdf/publikacje/2018/cyber-ruletka-po-polsku-raport-pwc-gsiss-2018.pdf>
- [5] 19. *Światowe Badanie Bezpieczeństwa Informacji firmy EY Droga do cyberbezpieczeństwa: wykrywaj, chroni, reaguj*. Source: [https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/\\$FILE/GISS_2016_Report_Final.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/$FILE/GISS_2016_Report_Final.pdf)