Information security as a factor shaping modern management

Agnieszka Dziedzic
Faculty of Management and Command, War Studies University
Al. Gen. Chruściela 103, 00-910 Warsaw, Poland
E-mail address: eduexpertaga@gmail.com

ABSTRACT

People managing economic entities have to face one of the main challenges in the modern world, which is the security of data resources. The dynamic development of cyberspace changes the conditions for running a business. The aim of the article was to indicate how important information security is in the management of an enterprise. According to the analysis of the economic reality of the 21st century, it is the cyber security problems that should constitute the focus of every economic entity and create effective actions counteracting such phenomena.

Keywords: information security, cyberspace, cyber security, management, people managing, running a business, explicit data, case study

1. INTRODUCTION

The functioning of every business entity is connected with cyberspace, it is unavoidable. Using the virtual space, among others, the purchase/sale transactions, marketing activities, as well as basic functioning of the unit, such as e-mail contact with employees or contractors, registration of events/business operations are made. Thanks to cyberspace, running a business does not depend on the place occupied by the physical space in a geographical context [1, 2].

The context of cyberspace was created and popularized in 1984 by William Gibson in the Neuromancer novel, describing it as “consensual, hallucination, experienced every day by
billions of legitimate users in all countries, by children taught mathematical concepts […] a graphical mapping of bank data of all computers in the world. Unimaginable complexity […] [3]. Using a certain metaphor, cyberspace can be referred to as a mega network or the network of networks. Access to it provides opportunities to implement a range of social needs in the sphere of education, culture, economy, communication, etc. At the same time, cyberspace has become a source of threats, which led to the emergence of cybercrime, cyberterrorism, cyber-espionage and cyberwar. The figure illustrates key concepts related to cyberspace [4].

![Figure 1. Key concepts related to cyberspace](image)

The constant fast pace of changes taking place in the cyberspace forces the people managing the business unit to increasingly secure data resources, which should be ordered and at the same time be characterized by confidentiality, integrity and accessibility.

The aim of the article was to indicate how important information security is in the management of a business entity. In the implementation of the purpose of the article, the starting point was to define information security and cyberspace. Then, in order to analyse the actual market situation, the PWC reports and the market reports were analysed.

Some companies understand that the cyber activity of the criminal world exposes their own action to an unprecedented risk. 80% of CEOs of the world’s largest organizations recognize digitization and new technologies as the first factor to ensure their innovation, and thus their competitiveness on the market. In turn, 80% realize that cyberattacks are one of the biggest threats to the development of their business (in Central and Eastern Europe, the percentage of convinced CEOs is 77%). An extremely important factor that must be faced by the management in the area of IT infrastructure security and the security of personal data obtained in the course of activity is the fact that enterprises in all sectors (services, production, trade) must implement EU standards. This means that less depends on their un (awareness) and more on debentures introduced by EC directives:
1) Regulation of the European Parliament and the Council (EU) 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free flow of such data and repealing the Directive 95/46/EC (general regulation on protection data), which applies from May 25, 2018.

2) Directive of the European Parliament and the Council (EU) 2016/1148 of July 6, 2016 on measures for a high common level of security of network and information systems in the territory of the Union. According to art. 25 of the Directive: Member States shall adopt and publish, by May 9, 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately notify the Commission about this, and from May 10, 2018 shall apply these measures.

2. INFORMATION SECURITY

The term of state information security (business entity) was introduced in the second half of the 20th century, but it does not mean that information as a security factor was of no importance before and was not noticed. Nothing more wrong – problems related to information have always been in the centre of attention of rulers, chiefs, apparatus, state. Reliable, credible, accurate and also up-to-date information has always been and is important in making decisions of the state (business entity), in particular, both internal and external security [5].

In the literature on the subject, the definition of state information security is most commonly found, nevertheless, it can be attributed to the information security of every business entity [6]. Piotr Sienkiewicz believes that “the starting point should be the concept of information security as an integral part of national security, and then of information threats”.

Information security is “a state of internal and external conditions that allows the state to have, survive and the freedom to develop an information society”. Piotr Bączek proposes a layered (structural) model of information security, where the core are the techniques and information technologies surrounded by the following areas: social, ethical, cultural, scientific, political, security and defence. Each of the areas of human life generates a different type of threats, characterized by its own specificity and, at the same time, capable of affecting the state of national security separately. At the same time, each of these spheres forms a separate subsystem of national information security, which must be secured in two ways: through universal solutions that apply to all layers and through solutions specific to each area. Threats to information security are of a trans-sectoral nature [7, 8].

“Practitioners often understand information security as protection of information from undesirable (accidental or conscious) disclosure, modification, destruction or prevention of processing. Security measures are taken to ensure the confidentiality, integrity and availability of information. Their goal is to eliminate the threat to information. This indicates that the definition of information security cited above was formulated in negative terms. Along with the intellectual development and polytechnicization of life, information began to gain more and more values. Their possession has become a condition for a better and safer existence. Against this background, competition emerged. Information was more and more protected as material good. The desire to create something similar to other or better living conditions has created the need to obtain information. Thus, a kind of struggle was born – some, with accessible ways, seek to obtain information, while others – with similar involvement – try to prevent this. In such proceedings, there is a contradiction of goals and actions, i.e. the most distinctive features that
are associated with the designation of the concept of “fight”. One could say that the subject of this struggle was information, and the tools – all means adapted to its acquisition, disruption and defence. Such a fight is called the “information fight” [9].

It should be noted that modern activities related to cybersecurity are based on the actions of major players on the global market. The division of the world into the main economic blocks is shown in Figure 2.

![Global GDP](image)

**Figure 2.** The main economic and business blocks of the world

In the Cybersecurity Strategy of the Republic of Poland for 2017-2022, the security of network and information systems (cyber security, IT security) has been defined as „resistance of IT systems, at a given level of trust, to all activities violating the availability, authenticity, integrity or confidentiality of stored or transmitted, or processed data, or related services offered or available through these networks and IT systems” (Cybersecurity Strategy of the Republic of Poland for 2017-2022 [10].

The definition of networks and IT systems (ICT systems) is illustrated in Figure 3.
Cyberspace is the natural sphere of information fight, because ex definitione it is used to transfer, process and store information. Cyberspace is a global electromagnetic space accessible via electronic technology, used by appropriate modulation of electromagnetic energy. The essence of cyberspace is the use of information in a digitized form [11].

3. INFORMATION SECURITY IN POLISH ENTERPRISES

In the fifth study conducted by PWC, in autumn 2017, 127 Polish IT and information security experts took part in the online survey method. The size and industries of the surveyed companies (are illustrated in Figures 3 and 4).

The conducted research is important not only because of checking the level of information security of enterprises but also due to the fact that in mid-2018, two important acts that regulate the principles of cyber security enter into force:

1) the regulation on the protection of personal data (RODO);
2) NIS directive.

65% of the surveyed companies indicated that incidents were detected within 12 months, during which information security or IT systems were breached. However, not all incidents have been identified and included in the reports. A worrying phenomenon, as in 2016, is the fact that 33% of the surveyed companies indicated that the main source of incidents and threats was the immediate environment, i.e. current employees (13 % of former employees, 6% of
current service providers, consultants/contractors, 4% of clients, 2% of former service providers and suppliers) [12].

Figure 4. Size of the surveyed companies

![Figure 4](image_url)

Figure 5. Industries of activity of the surveyed companies

![Figure 5](image_url)

Taking into account the circumstances of the incidents, 41% of the surveyed companies indicated that they were the result of errors committed by system users, 24% - use of previously stolen data/information, 21% - computer configuration errors and 20% phishing attacks. A worrying phenomenon is the fact that despite the fact that companies know both the source of incidents and the situation that led to them are identified, they do not undertake activities aimed at sealing functioning security systems.

In the area of determining financial losses of cyberattacks, it is often not exactly calculated. 44% of surveyed companies indicated that they suffered financial losses (3% in 2016), 30% - cannot indicate it, and 26% - did not record it [13].

21% of companies indicated that the systems were infected with malware of the ransomware type. Considering the downtime in business, this was indicated by 15% of surveyed companies, of which 40% (47% in 2016) of incidents were related to over a 3-hour break (12%
- from 3 to 8 hours and from 9 to 24 hours, 15% - more than one day). Another worrying situation is that every tenth surveyed company has an insurance policy against risks related to cyberattacks.

![Figure 6. Information security analysis on the example of Polish enterprises](image)

**Figure 6.** Information security analysis on the example of Polish enterprises

![Figure 7. Types of implemented security](image)

**Figure 7.** Types of implemented security

18% of surveyed companies admitted that the cyberattack was a threat to the company’s reputation. 10% admitted that information about clients/employees/business partners leaked out [14].
65% of surveyed companies declared that they had a general security strategy, and 54% that they have developed incident response processes.

34% (21% in 2016) of surveyed companies have SIEM class systems to manage information and security events. When it comes to launching the Security Operations Centre (SOC), 63% of the respondents said that the company does not have and, at the same time, no commissioning is planned, 15% - plan the implementation, and 14% has launched it [15].

![Challenges for information security](image)

**Figure 8.** Challenges for information security

In the area of priority actions in the surveyed companies, there are no protections against developing technologies, e.g. when it comes to social media only 23% showed that they have a security strategy associated with them, in the case of Big Data – 25% and the computational cloud – 27%.

20% of medium and large companies do not have any person who would be responsible for information security. 21% of the surveyed companies declared that one employee was responsible for information security. In 10% of companies, it was determined that there are units dealing with information security consisting of 20 or more specialists. 19% of medium and large companies do not employ any IT specialist (41% - employ from 2 to 10 employees) [16].

8% of the surveyed companies have competences in the area of cyber security and 7% do not have all the key securities and infrastructure elements, but they have plans to implement them within 12 months. In order to determine the index of security, the following data was taken into account:

- implemented systems: SIEM, Anti-APT, IPS/IDS, SOC,
- security budget equal at least 10% of IT expenses,
- cybersecurity team – at least 2 people,
- reporting on the security status directly to the board,
- created position of the Director/Head of Cybersecurity [17].

Enterprises from the industry of financial sector, telecommunications, Energy and industrial production are the most mature in terms of cyber security. Examples of cyberattacks in the world with their effects are presented in Table 1.

**Table 1. Examples of cyberattacks in the world**

<table>
<thead>
<tr>
<th>Year</th>
<th>Crisis situation</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>1962</td>
<td>Mariner 1 rocket going off course, which resulted in its destruction.</td>
<td>The “-” sign has not been moved to the control application.</td>
</tr>
<tr>
<td>1983</td>
<td>The computers of the USSR defense system showed the start of 5 ballistic missiles.</td>
<td>Erroneous interpretation of the reflection of sunlight on clouds in the USA.</td>
</tr>
<tr>
<td>1996</td>
<td>Ariane 5 rocket going off course, which resulted in its destruction.</td>
<td>Moving the software of the Ariane 4 rocket, which resulted in the maladjustment of the speed of the rocket.</td>
</tr>
<tr>
<td>1997</td>
<td>The NORAD system detected the attack of 2020 USSR missiles.</td>
<td>Sending random bits of information to the system.</td>
</tr>
<tr>
<td>2001</td>
<td>10 od 13 DNS (Domain Name Server) servers were shut down.</td>
<td>DoS (Denial of Service) types of attacks.</td>
</tr>
<tr>
<td>2004</td>
<td>During the construction of the A-380 airplane, the aircraft equipment was not adjusted to the body of the aircraft, which resulted in a loss of about 5 billion euro and a delay of several months.</td>
<td>The CAT-CATIA program was used in the production of the aircraft in two versions 4 and 5 (Toulouse, Hamburg), two different operating systems (UNIX, WINDOWS) and programming languages (Fortran, C++) were used.</td>
</tr>
<tr>
<td>2007</td>
<td>3 of 6 attacked DNS servers were shut down.</td>
<td>DoS type of attacks, but the attack was limited after the introduction of the ANYCAST technology.</td>
</tr>
<tr>
<td>2008</td>
<td>Airbus SPAINAIR plane crash, which killed 154 people.</td>
<td>Incorrect positioning of the flaps during the take-off of the aircraft, caused by the introduction of malicious software during the servicing of the aircraft.</td>
</tr>
<tr>
<td>2008</td>
<td>B-2 Spirit (~ 1,3 billion $) crashed during the start from the Guam base.</td>
<td>No calibration of the sensors.</td>
</tr>
<tr>
<td>2010</td>
<td>First attack on critical infrastructure – taking over industrial processes at the nuclear power plant in Iran.</td>
<td>Taking control of the SCADA (Supervisory Control And Data Acquisition) system by the Stuxnet malicious program.</td>
</tr>
<tr>
<td>Year</td>
<td>Crisis situation</td>
<td>Cause</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>2012</td>
<td>Attack on the government websites in Poland with their immobilization for a certain period as a protest against the signing of ACTA agreements.</td>
<td>DDoS (Distributed Denial of Service) types of attack carried out by the Anonymous group.</td>
</tr>
<tr>
<td>2014</td>
<td>150 Ukrainian websites were blocked, NATO website and American security agencies websites.</td>
<td>DDoS type of attack.</td>
</tr>
<tr>
<td>2014/2015</td>
<td>Attack on 22,1 million users in the USA, data theft of 1.1 million people.</td>
<td>Hacker attack.</td>
</tr>
<tr>
<td>2015</td>
<td>Security breach of the Patriot missile launcher (Turkey).</td>
<td>Hacker attack.</td>
</tr>
<tr>
<td>2015</td>
<td>Immobilization of the power plant in Ivano-Frankivsk (Ukraine).</td>
<td>Hacker attack.</td>
</tr>
<tr>
<td>2016</td>
<td>Attack on smart buildings – failure of the heating and water supply system for the building - Lappeenranta (Finlandia).</td>
<td>Hacker attack.</td>
</tr>
<tr>
<td>2017</td>
<td>Stopping the Nissan (Sanderland) and Renault (Great Britain) car production.</td>
<td>Hacker attack.</td>
</tr>
<tr>
<td>2017</td>
<td>Attack on the network of nuclear power plants in the USA.</td>
<td>Attack using ransomware (Petya).</td>
</tr>
</tbody>
</table>

### 4. CONCLUSIONS

The research carried out by PWC (Figure 5) and the observation of the market, for example, WannaCry attacks, Petya in 2017, do not raise optimism. The management staff, which balances between ensuring the company’s security and its growth and economic development, often does not realize the scale of threats posed by the constant and rapid development of technology (Figure 5) and the associated cyberspace in which it operates. The
consequences of a cyberattack on an economic entity are not only financial losses but also loss of credibility and trust of business partners and clients. Lost trust is difficult to estimate but also to recover. 58% of the surveyed companies demonstrate cyber security as a key competence for functioning.

44% of companies incurred financial losses due to cyberattacks
62% of companies recorded disturbances and at the same time breaks in functioning
21% of companies were the victim of an encrypted disk (ransomware)
20% of medium and large companies has no one responsible for cyber security
46% of companies does not have operational procedures of responses to incidents
3% of the IT budget, on average, are the security expenses
8% of companies are mature in terms of information security

**Figure 9.** Conclusions from the conducted research

Hybrid attacks, which scenarios combine the susceptibility of technology and the vulnerability of employees to socio-technical attacks are the most difficult to prevent and detect early. Strategies for the development of enterprise security should take into account the appropriate development of security mechanisms in organizational and technological layers.
adapting to business needs and the market situation, through the prism of the dimensions of modern technology (Figure 9).

At the same time, the management staff and employees of the company need to be aware of the reality in which the cyberspace and related facilities currently operate, and at the same time threats become commonplace. In order to ensure stable operation and development in the future, management should strengthen activities in the field of information security and at the same time immunize the company for all kinds of attacks. The implementation of appropriate safeguards, policies and procedures defining how to proceed in the event of a cyberattack and at the same time a better awareness of employees of existing threats form the basis for the functioning of the business unit in the modern world.

Currently, in the globalization conditions, there are several basic trends determining the functioning of modern enterprises that can be indicated. They include:

1) progressive concentration of capital on a global scale,
2) fast, less and less limited flow of information,
3) development of modern information technologies,
4) increasing the importance of company and brand knowledge,
5) growing importance of relationships with suppliers and customers,
6) unification of consumption patterns and lifestyles,
7) the increase in the importance of standardized after-sales services,
8) the development and dissemination of new products,
9) development and dissemination of modern telecommunications technologies,
10) dissemination of concepts and management methods on a world scale.

The changing socio-economic reality and the challenges of the 21st century are a resulting from the dynamic development of globalization.

References


