IT SECURITY MANAGEMENT IN SMALL AND MEDIUM ENTERPRISES

Zdzislaw POLKOWSKI[1], Jakub DYSARZ[2]

[1]Jan Wyzykowski University, z.polkowski@ujw.pl
[2] Ministry of Digital Affairs, Poland, dysarz.jakub@gmail.com

***Abstract**: The work concerns the problem of the management of security issues in Poland, especially in the perspective of Small and Medium Enterprises. The growth of Information and Telecommunication Technology has caused major impacts on business. Thus, serious security questions may be raised concerning small companies. Significant aspects of security issues are discussed, e.g. types of targets, types of attackers, legal issues and some recommendations for businessmen. The research is based on a review of works published in recent literature. The main method used in this inquiry was a case study. Additionally, the paper contains assumptions regarding further development of methods to secure information and communication systems. The results of the research reported here can be important both for business and academia. The recommendations may constitute the basis of improvement in the security area of activities supported by computers.*

***Key words**:* computer security; cybercrime; ICT; SMEs; management.

JEL Classification Codes: A10, C80, C88.

1. INTRODUCTION

Businesses have adopted information and telecommunication solutions in their daily activities, therefore the structure of IT systems is changing within companies. The effects of these technologies tend to be relevant to security management issues. These are effects in the legal field and method of company management. IT security management aspects are increasingly of interest to researchers, businessmen and users of IT systems. Furthermore, they have a significant impact on people's behaviour and their appreciated value. For these reasons, further research on IT security management is essential. Users and ICT professionals should be guided by certain principles, the use of which can prevent a lot of problems and abuses in the use of computer technology, such as loss or destruction of important data, loss of business or positive image.

The article focuses on issues related to cybercrime. Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offence (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime (Techopedia, 2017).

Areas of research selected to study in this paper are the following: types of targets, types of attackers, and legal issues. But the most important part of the article is the description of the

research on methods and recommendations regarding to IT security management. This paper is structured as follows: after the introduction, in section 2, the literature review is presented. Section 3 describes the current research gap, the purpose of the article, and methodology. In the next section there is the outline of the results of the research. Finally, the last part contains the conclusion, research limitations and scope of future study.

2. LITERATURE REVIEW

IT security management in SMEs is an offshoot of applied business informatics that considers IT security issues raised by computer technology. IT security management deals with how computing professionals should make decisions concerning professional use of ICT. It identifies the controls that an establishment needs to carry out to ensure that it is sensibly managing risks of loss, misuse, disclosure or damage. Information security management in organizations includes a set of guidelines aimed at achieving and maintaining an optimal level of security, including levels of confidentiality, integrity and availability of data.

According to Ioannis Koskosas (2013) there is an equal need to contract research within the social – organizational context of data systems security in order to mix it with the technological characteristics of data protection. In so performing, information systems security planning, development and management can be achieved more effectively than ever before since senior managers, and the IT staff involved, will take in a wider perspective of the issue concerned either from a technological or non-technological position.

Zahoor Ahmed Soomro et al. (2016) in their work admit that, along with the role of management as a whole, various management aspects mentioned in table 1. have been found to have a meaningful role in information security management.

Table 1. Management and its aspects discussed in the literature with the number of articles

No	Concept	Number of articles
1	Management role is critical for Information Security	12
2	Management role in business IT alignment and security issues	05
3	Management role in enterprise information architecture	03
4	Management role in information infrastructure development	04
2	Effective information security policy, awareness and training impact on information security management	13
3	Role of human factors in information security management	08
4	Information security should be a board level issue	04
6	Employee role in information security breaches	03
7	Employee adherence to security policy and its effects	02
8	Top management support is critical for information security	05
9	Integration of technical and managerial activities for information security effectiveness	04
10	Information security should be dealt with as a business issue	03
11	Security issues in cloud computing and management role	06
12	Security risk assessment and management role	06
13	Management role in security issues related to social media	02

Table 1. shows various aspects of management, which have a significant role in information security management. The management role in information security is becoming increasingly important and is gaining the attention of researchers. The literature shows that the development and implementation of an effective information security policy have a critical role in managing information security (Zahoor Ahmed Soomro, 2016).

3. RESEARCH METHODOLOGY

The aim of this work is to analyse IT security management in SMEs. The research is based on the review of scientific and professional works recently published in the literature. Additional information was acquired from specialists representative of ICT and owners of Polish SMEs in Polkowice and Lubin. Moreover, a cooperation with the Ministry of Digital Affairs in Poland has placed in this work. This study leads to recommendations for SMEs to protect their IT systems.

While studying the literature, two research gaps concerning the role of ICT in SMEs have been noted:

1. The theoretical - insufficient number of publications, particularly in the Polish literature.
2. The empirical - small number of descriptions of the experiences, implementations, recommendations and knowledge benefits of the occupation (especially in national literature), and the use of methods to protect IT systems. The description of the inquiry can be obtained and the generalization of empirical knowledge fills, at least partially, this research gap.

The problem presented above leads to a considerable need to conduct studies in this area. The work has been concentrated on cyber security issues to the following aims:

1. To appropriate the types of targets.
2. To identify the types of attackers.
3. To analyse legal issues in the context of IT security.
4. To present some recommendations for SMEs.
5. To present the framework of IT Security Management in SMEs.

4. RESULTS

Cybercrime is one of the biggest threats for small and medium enterprises. Meanwhile, many of them believe that they are safe, because in their opinion cyber criminals focus only on the largest entities that turn the largest amount of money. Companies with this attitude are an easier target for criminals. According to the Orange Insights (2017) survey, over the last year as much as 13 percent of small and medium-sized enterprises were the target of hacking attacks - Jabczyński (2015).

Orange Insights (2017) in its research has shown that every fourth respondent (23%) notices a dynamic increase in the number of IT threats to SMEs. Among the greatest threats to data security and information systems, the respondents mention in turn:

- Cybercrime - 31 percent indications.
- Problems with data transmission via the Internet - 26 percent.
- Employee dishonesty and server, computer and link failures - 25% each.

Particularly noteworthy is the fact that despite the growing threat of cyber attacks on mobile devices, small and medium-sized companies do not treat the risks associated with the use of laptops, mobile phones, smartphones and tablets as seriously as the risks of using a regular desktop computer. Mobility is not perceived as a threat by more than half of the surveyed companies - as many as 61 percent. This is a worrying conclusion pointing to insufficient awareness of real threats. Considering that such companies constitute the vast majority of enterprises in Poland, the scale of the attacks is enormous. Almost half of them are attacks on websites, servers and mail; however, a growing number of attacks are financial blackmails and some generated by malicious viruses and trojans (MobilityNews, 2017).

4.1 TYPES OF TARGETS

It is imperative to know that there are different types of targets – and to know to which category a particular SME belongs to protect itself better.

The first type of target is private entities – this is usually individual end-user or group of

such. The architecture of systems for this target is not very complicated, thus attacks are relatively easy. However, the possible gain is not very impressive, unless the attacker is pursuing a specific target (e.g. personal data of particular person). The upside is the least chance of being detected during the attack. According to a data report from Bill Hau et al. (2016), most companies did not know for months that they were hacked (469 days from incident to detection, on average). The most possible outcomes are: identity theft, fraud, data theft.

Identity theft is a serious problem, but when detected early and handled wisely, its outcomes can be limited to the minimum. Fraud is particularly harmful, but with the right dose of self-preservation one can protect oneself from it. Data theft is more malicious – it is difficult to detect and, as every undetected harm, it can escalate.

The second type of targets are corporate persons. It does not matter if it is a large company or an SME, the problems they face in case of an attack are very similar. It will be clarified in the next part of this article that deals with types of attacks. The most probable motivations to attack a company are extortion of corporate secrets and theft.

The last type of target are government entities. As large agencies and organizations they are usually protected and have enough resources to train their employees.

4.2 TARGETS IN SMES

According to the Whitepaper issued in collaboration by Chubb, CoverHound and Symantec, there is a basic reason why SMEs are popular targets. Attackers look for easy targets, and small companies with a limited budget, which do not identify cybersecurity as their main concern are easier to hack than large ones, which spend even six figures on security (Millaire et al.,2017).

FireEye (2016) in the document titled "5 reasons cyber attackers target SMEs" has published that:

- High-profile data breaches of corporate giants make the headlines. But 77% of cybercrime actually targets small and medium-size enterprises (SMEs). 65% of SMEs have no data security policy.
- Only 10% of cybercrimes reported to police by SMEs result in a conviction.
- Attackers bypassed multiple layers of security in 96% of SME deployments in a real-world study.
- Data breaches cost an average of $217 per stolen record, which adds up quickly.
- 58% of SME managers do not see cyber attacks as a sign of a significant risk (FireEye, 2016).

This short analysis clearly shows that employees of small and medium companies are most exposed to cyber attacks. This situation results from the necessity of precise compliance by government institutions in accordance with the recommendations of the inspector of data protection and ENISA (The European Union Agency for Network and Information Security). In the case of SMEs, even if they are obliged to similarly secure information systems, they only take into account those elements that may affect the company's business continuity disruption, data loss or data theft by the competition.

4.3 TYPES OF ATTACKERS

In the literature you can find many categories of attackers. In this study, four types of cybercriminals have been presented: hacktivists, professionals and organized crime, insiders, and, last but not least, state actors. They have different motivations and aim at different targets.

Hacktivists usually keep the need for social or economic change in mind; types of their attacks vary from simple defacement of websites and renting a botnet for distributed denial of service attack, to breaching professionally secured entities. An example of such actors is Anonymous Group and Wikileaks.

Professional criminals are a type well known by the police – their modus operandi is cleaning out bank accounts, industrial espionage, sabotage, extortion of critical data or simply damaging a company's assets, resources, operations or public image. Most of the actions are done for profit. They sometimes intersect with traditional crimes, e.g. organized crime moving their drug trafficking operations into the Darknet.

Insiders are people that should be considered a possible risk factor in every organization. Disgruntled or vengeful employees can pose a serious threat to an organisation of any size, given their access to crucial data and knowledge of the inner workings of an organisation.

Finally, state actors, the most resourceful groups, who rarely aim at financial gain, although there are exceptions. State actors rarely aim at corporations, besides the situations when they are part of the national security system (such as weaponry manufacturers).

Although the image of the computer criminal is often associated with a young man with a console-based OS, hiding in the basement, this is no longer even considered a viable stereotype. As the business moved online, so did the criminal activities feeding on them. Criminals are well trained, focused and success-oriented.

4.4 TYPES OF ATTACKS

The next issue to tackle are the types of attacks. As firewalls and malware-detecting software became more sophisticated, it became clear to perpetrators that they need to attack in the soft spots, not the most secured ones. Thus, in SMEs traditional malware and exploit kits are still the main tools of these new types of criminals, but not the only ones. Phishing methods have a surprisingly high success rate, although stories of successful phishing campaigns appear in media relatively often.

4.5 MALWARE

Malware is an umbrella term for a variety of cyber threats, including, but not limited to the following: viruses, worms, ransomware (malware that encrypts data on an infected computer), spyware (including trojan horses), keyloggers (malware that tracks keyboard activity, allowing to copy a user's passwords), rootkits (enabling administrative access to the victim's computer) and adware (unwanted and not ordered advertisement software). Malware is often defined as a program designed with malicious intent that steals or destroys data. As two programs are rarely alike, so there are different methods of protection against them. There are, though, basic rules of protection that will be presented later in this paper.

4.6 PHISHING

Phishing is a type of attack that exploits weaknesses. In short, the attacker poses as someone else (authority, bank, customer or friend) to get access to certain information. It is an old crime, well-known to authorities, and dates back to a time before the digital age. The difference between old-fashioned fraud and phishing lies in how massive the attacks can be (up to millions of fake e-mails) and that they are relatively cheap and effective. It is much easier now to obtain and copy the pattern of a company letter, together with logo, and send it worldwide.

However, old-fashioned mass phishing campaigns are a thing of the past; most effective campaigns compose now of spear-phishing (targeted phishing). Spear-phishing differs from mass-phishing campaigns as it targets particular people, calibrating and tailoring the attack to that end. This type of attack demands more effort, information and time, but has a much higher rate of success, especially when attackers focus on a particular target. It is more probable to reach one's goal with a tailored attack than a massive one (Jill McCabe, 2016).

Darren Guccione (2017) admits that the rising incidence of ransomware attacks on SMEs noted earlier found the attacks were unleashed 79% of the time through phishing or other social engineering, most notably burying harmless looking clickable URLs into a scam email. A prime

defence against this can be ongoing phishing simulations to try to educate negligent employees (Warwick Ashford, 2017).

4.7 DDOS

One of the most critical types of attacks is the distributed denial of service (DDoS) attacks. In short, the perpetrators take over a number of computers (or other devices) and make them "flood" the victim's server with a huge number of requests. In the age of weak home security, many computers can be infected with malicious software and used as a part of a botnet – i.e. the network of computer, unwillingly used to conduct attacks and then return to normal. Botnet, can consist of hundreds of thousands of devices and perform attacks exceeding Giga- or even terabytes per second (Pierluigi Paganini, 2017). Such an intense attack can crash even the most potent servers and thus shut down the operation of any company.

4.8 WATERING HOLE ATTACK

Trust is the basis of any business relation – an anecdote says that the thickness of a contract between parties is proportionate to the mistrust between them. It is impossible to separate oneself from the outside world. Even such a simple thing as web browsing with enabled JS (Java Script) blockade is impossible. One must allow some pages to run JS, and it is based on the trust we place in the owner of the website.

However, blind trust can be harmful. It is not only about trusting a particular website vendor, but also his security capabilities. A"Watering hole" attack exploits this trust. It is based on the idea that there are websites which are trusted because of the authority they represent (e.g. governmental websites). The target is not the website, but the visitor of the website, who trusts its content.

4.9 ATTACKS IN SMES

According to the Cyber Essentials Scheme for UK government, most common threats against organizations belong to one of two groups: phishing or hacking. Phishing is a malware infection through users clicking on malicious e-mail attachments or website links. Hacking, on the other hand, is the exploitation of known vulnerabilities in Internet connected servers and devices using widely available tools and techniques. The same problems concern SMEs.

Moreover, it is worth mentioning that the overwhelming majority of cyber attacks on small to medium-sized enterprises (SMEs) result from poor password management (Warwick Ashford, 2017).

LEGAL ISSUES IN THE CONTEXT OF IT SECURITY

In this part, documents related to main international and European legislation in the context of SMEs have been described. I will conclude this part with some examples of national legislation in Europe for comparative reasons.

4.10 UN AND GLOBAL LEVEL

There is no global document concerning cyber security. The UN attempted to harmonize regional and national documents, but no document that would deal with the problem in a holistic way has been devised. Cybersecurity is an interdisciplinary problem. It touches on criminal law (cybercrime sensu stricto – e.g. phishing and sensu largo – for instance using the darknet for criminal purposes), commercial law (e-signature, digital market, safe transactions), human rights (right to privacy, data retention and surveillance) regulatory law (everything related to communication companies, Internet architecture and Internet providers) and everything related to national security (military grade encryption, communication for army and police and managing state secrets). As more and more devices are connected to the Internet, every issue becomes a

cyber issue. Still, there are some internationally recognized documents that we can scrutinize (United Nations, 2017).

4.11 THE BUDAPEST CONVENTION

The Budapest Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the searching of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

4.12 THE EUROPEAN UNION

The European Union devised a cybersecurity strategy in 2013 that focused on five priorities:

1. Increasing cyber resilience;
2. Drastically reducing cybercrime;
3. Developing EU cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
4. Developing the industrial and technological resources for cybersecurity;
5. Establishing a coherent international cyberspace policy for the EU and promoting core EU values.

Although general in wording, the EU cybersecurity strategy was an important step ahead for other policies. It was followed by The European Agenda on Security (2015), regarding fighting cybercrime, and The Digital Single Market Strategy (2015), signed by the Commission, and the The European Cyber Security Organization (ECSO) – an industry-led association, which includes a wide variety of stakeholders. The partnership is supported by EU funds coming from the Horizon 2020 with a total investment of up to €450 million until 2020.

Those acts gave way to more concrete actions. In 2016, the NIS directive (hereby: NISD) was adopted. In comparison with other acts, it is groundbreaking, as it requires states to identify so called "operators of essential services", vital for the correct functioning of the states and enforcing legal measures that will improve their safety. To be regarded as an operator of essential services, an entity must meet a few criteria:

- It provides a service which is essential for the maintenance of critical societal and/or economic activities;
- The provision of that service depends on network and information systems; and
- An incident would have significant disruptive effects on the provision of that service.

Services are limited to selected sectors (energy, transport, water supply etc.). Together with the eIDAS directive, the PSD2 and GDPR regulations, NISD forms a framework for effective protection of essential services, electronic identification services, payment services and personal data. That includes incident notification, international cooperation, public-private partnerships and cooperation platforms.

Several more EU legislative actions contribute to the fight against cybercrime. These include a Directive on attacks against information systems (2013), which aims to tackle large-scale cyber- attacks by requiring Member States to strengthen national cybercrime laws and introduce tougher criminal sanctions; a directive on combating the sexual exploitation of children online and child pornography (2011), which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse); and last but not least, the Framework Decision on combating fraud and

counterfeiting of non-cash means of payment (2001), which defines the fraudulent behaviours that EU States need to consider as punishable criminal offences.

RECOMMENDATIONS FOR SMES

There are three pillars of IT security – technology, procedures and people. Only when all three are up-to-date, appropriately funded and prepared for future threats, will you be able to say that the system is secured. Taking into account the pillars mentioned above, some recommendations for SMEs have been presented.

General access rules organizations' internal network and thus all devices and assets connected within should be protected against unauthorized access. Using firewalls or equivalent solutions is essential.

The default administrator password for any firewall should be changed to an alternative, strong password. This rule is a valid for passwords in general. The quality of a password is dependant on the number of characters, the types of characters, type of algorithm and the quality of the hardware that is attempting to break the password. The table below shows approximated times of cracking a password. However, it assumes that the password is random (i.e. not dictionary-based). A dictionary-based password can be cracked in seconds.

Table 2. Time needed to crack a password (Oleg Afonin, 2017)

Type of file (encryption algorithm) and processing unit\ Length and type of password	6 characters, lower-case	6 alphanumeric, both cases	7 characters, lower case	7 alphanumeric, both cases	8 characters, lower case	8 alphanumeric, both cases
MS Office 2013, CPU	119 days	60 years	8.5 years	3700 years	220 years	Eternity
MS Office 2013, GPU	0,5 days	3 months	2 weeks	16 years	1 year	975 years
RAR5, CPU	56 days	28 years	4 years	1744 years	103 years	Eternity
RAR5, GPU	2 hours	26 days	4 days	4.4 years	3 months	273 years
BitLocker, CPU	5 years	900 years	127 years	eternity	3300 years	Eternity
BitLocker, GPU	4 days	2 years	3.6 months	130 years	7.7 years	Eternity

It is worth noting that table 2. above will be soon out-of-date. As BetterBuys.com noted, it took 3 years and 10 months to crack the password "password1" in 2000, only 7 months in 2005 and mere 2 months in 2016 (BetterBuys, 2017). Together with the improved quality of technology, methods of attacks are also improving – in fact, today "password1" would be cracked in seconds, due to its popularity and listing in most popular passwordslists (David Wittman, 2017).

Some recommendations related to password in IT systems present Chmielarz & Zborowski (2017). They admit, that the security of using e-banking services and e-payments are still very important from the point of view of users, but to a smaller extent than a few years ago. The most

frequently used security methods are passwords enabling the users to log into the system and one-time SMS passwords entered to confirm the transaction (Chmielarz & Zborowski, 2017).

Each rule that allows network traffic to pass through the firewall should be subject to approval by an authorized individual and documented (including an explanation of business need). This is self-explanatory, however difficult to implement in practice. It demands constant or at least periodical inspection of allowed services. It is important to make sure that obsolete firewall rules are removed or disabled in a timely manner.

Additionally, every network before going live for the first time, but also, periodically, should be inspected for the most common issues:

- Has it been correctly segmented?
- Is the least-privilege rule in place?
- Is the whole traffic monitored both ways?
- Is it possible to reach the internet from my network without the administrator's knowledge?
- Has the integrity of the firewall rules being tested?
- Is all software updated?

Also, although making the administrative firewall management interface accessible from the internet is tempting and promises remote access for the administrator, it should be limited and used only when absolutely necessary even when it's protected by login and password and restricted to static IP.

4.13 USER ACCESS CONTROL

User accounts should be assigned to authorized individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

ISO/IEC 27002 presents the most important elements of user access control. It consists of access management policy (with the default approach of minimal access), access management (registering and unregistering users, managing standard and special access rules, managing confidential user data and periodical review of the access management mechanisms) and preventing unauthorized access to systems and application.

It is worth noting that user accounts and special access privileges should be removed or disabled when no longer required (e.g. when an individual changes role or leaves the organisation) or after a pre-defined period of inactivity (e.g. 3 months). However, this is a minimum requirement; optimally, accounts should be removed right after termination of employment and, to mitigate the risk the revenge of a disgruntled employee, even during the termination period. This includes: assessing the employee's level of access (number of accounts, privilege levels, company's devices in possession) and limiting it (wiping out the company's devices in the employee's position, removing access to accounts or deleting accounts when necessary). It is crucial to cooperate between departments – HR should closely work with the IT department on accounts and security to restrict physical access. All keys to rooms and key cards to restricted areas, as well as special access and authorization papers to represent the company outside it (e.g. Bank), should be returned and kept in check. Remote access (e.g. via VPN) should be revoked and any shared passwords (if they exist) should be changed.

4.14 MALWARE PROTECTION AND PHISHING

CERT Orange Polska issues an annual report on cybersecurity. They found out that in 2016, only 6.7% of incidents registered by their CERT were related to malicious software. As explained, the term "malware" refers to any kind of infections or distribution of malware as well hosting C&C servers for botnets. According to their report, malware attacks can be observed in three different classes: as malware object (identified malware files delivered to the end user), as web infection (when malware is installed in real time, when the end user is connected to the

internet) and as malware call-back (when malware contacts with designed C&C for further instructions). Most of the security events were connected to malware callback, due to the nature of modern attacks. It also emphasizes the low level of general security among end-users.

CERT Orange also presents five types of malware, associated with their main function. Thus, Dropper is malicious code that downloads additional data after connecting to C&C; well-known Bots allow the perpetrator to take control of the end user's device; Datastealer is usually set for finding particular data (e.g. credit card number or personal information) and sending it to the perpetrator; and last but not least, Ransomware that encrypts the user's data and demands payment to decrypt them (CERT Orage, 2017).

It is worth noting that some types of malware pretend to be ransomware and demand money for decrypting files, whilst it is often not technically possible. An example of such was Petya (NotPetya, Nyetya) – a wiper disguised as a ransomware (Matt Suiche, 2016).

There are basic rules that will increase the level of security for users, both private and corporate.

First of all, it is crucial to have installed malware protection software. As the malware evolves and changes, it is crucial also to update one's antimalware software. It should be standard procedure for all units that are connected to the internet. It is worth noting that there are different methods to deal with malware. For example, your security software may just remove blacklisted programs (the simplest way of solving the issue), analyse the activity of a particular program (so called heuristic analysis – effective, but RAM-consuming) or finally, it can sandbox (isolate) the program and see what it does in a controlled environment. The latter demands a high rate of expertise and attention and is not standard for most companies. It is essential to perform risk analysis for the particular case.

Secondly, it is important to keep the antimalware software on all the time and automatically scanning all files and websites upon access.

Thirdly, some content should be blocked by definition. For example, known malware sites should be blacklisted, the use of only HTTPS protocol should be mandatory, common unwanted (i.e. not yet malicious, but close to) pop-ups and scripts should be disabled (Basques, 2018).

Incidentally, there is no technological solution that will replace a vigil user. According to new research by Comodo Threat Intelligence Lab, up to 56% of users will click a link from an unknown source (University of Erlangen-Nuremberg, 2016). Comodo also suggests how to protect oneself from phishing (Orhan, 2017): If you were not expecting an email attachment, check back with the sender before opening it. Always compare the domain name in a browser address bar with the content on the page (if they do not match, be cautious). Do not click on unverified links in an email without checking where the actual link redirects. Finally, be wary of unexpected emails purportedly from your company's devices (e.g.scanner or copier) and other automatic messages with links or attachments.

4.15 PATCH MANAGEMENT

Software running on computers and network devices should be kept up-to-date and have the latest security patches installed. Usually, when a vendor abandons his products – e.g. what Microsoft did with Windows XP in 2014 – he stops sending patches when a vulnerability is detected. Sometimes, vendors break this rule – Microsoft issued a patch for Windows XP during the WannaCry ransomware campaign (Horowitz, 2017), but it is an exception to the rule. Windows XP still runs on around 6.94% of all computers in the world (Netmarketshare, 2017).

It is essential to keep all running software up to date and to ensure that security patches for known vulnerabilities are made available. All updates should be installed in a timely manner, depending on the type of patch. Patches crucial for the security of the data should be implemented immediately, whilst others can be installed at a more appropriate time. Also,

outdated or not used software should be removed from computer and network devices – it can have vulnerabilities that can be later exploited.

4.16 LONG TERM GOAL: ESTABLISHING PROPER BEHAVIOR PATTERNS

ENISA recognizes five levels of IT security behaviour, See Figure 1:

Figure 1. Five levels of IT security behaviour, (ENISA, 2017)

Firstly, the user (both private and corporate) must be aware of an existing problem. ENISA and other organisations try to achieve that through awareness campaigns. Implementing security in IT solutions without awareness is possible, but ineffective. For instance, ISO 27001 states that support and participation of top executives is essential for implementation of an information security management system. Lack of awareness at the executive level of management will make it disproportionately difficult to implement the right security measures.
ENISA recognizes five initial awareness areas for end users:

- Description of main threats through exploitation (malware, ways of infection, targeted attack, vulnerabilities);
- Description of the main threats through using online services (online banking/shopping, cloud based storage, ways of authentication);
- Description of online social behaviour (social networking, cyberbullying, illegal and harmful contents);
- Trends in most common hardware and software (desktop computers, laptop, mobile devices, untrusted applications, unpatched software, pirated software, wifi threats);
- Legal issues.

The second issue is attitude. When someone is aware of the possible risk, he or she can still neglect it. It can be observed daily – skipping software updates, the sharing of logins and passwords between employees, keeping passwords and personal data in open, cutting funds for security. All those symptoms indicate the approach of the company towards security.
When the company is aware of the dangers out there and is dedicated to making their business safer, another issue emerges – the lack of proper skill to do so (Morgnan, 2016). It is already common knowledge that the cybersecurity industry is booming and will need a larger workforce. The Internet and many related technologies were not designed to be resilient from cyber attacks and it is a job for the company's executives and employees (or contractors) to secure one's business from danger. It is not a case of keeping software up to date and installing anti-virus software. It may be enough for micro or small enterprises, but aspiring companies should also monitor their networks and conduct regular backups. For a small business owner, it may be crucial to outsource these services.

Having the right knowledge, management support and skills are halfway towards securing one's business. It is important to implement all of the above mentioned elements in the company's work that is to be determined to secure one's business. Proper intentions, supported with real-life actions can slowly change an employee's behaviour – and that's the last step in this process.

The company cannot say it is secured, just because they have prepared information security policy, established SOC and keep their software updated. If an employee knows the company policy, but does not follow its rules due to his or her laziness, lack of skills or because of other reasons that means that his behaviour has not been sufficiently altered. According to the CompTIA report, 17 percent of people would pick up an unbranded USB found in the street, plug it in their personal or corporate device and act in accordance with the instruction that had popped up (Chickowski, 2015). Additionally, 36 percent use their work email address for personal accounts and 38 percent use weak passwords for personal accounts.

Only when full congruence is achieved and the company gather necessary knowledge, take dangers seriously, invest the right amount of resources and convince its employees of the importance of their actions, – can it say that it implements some sort of compliant IT security actions.

This study suggests that information security issues should be considered as a responsibility of management, as it has an impact on the market position of a firm (Rossouw von Solms, 2004). Our company's information security plan should fully take into account table 3:

Table 3. Security governance plan, (Soloms, 2004)

Name of activity	**Choice**	
Information security is a corporate governance responsibility (the buck stops right at the top)	Yes	No
Information is a business and not a technical problem	Yes	No
Information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single 'off the shelf' solution)	Yes	No
The information security plan must be based on proper risk analysis	Yes	No
International best practices for information security governance drives our plan	Yes	No
A corporate information security policy is absolutely essential	Yes	No
Information security compliance enforcement and monitoring is absolutely essential	Yes	No
A proper information security governance structure (organization) is absolutely essential	Yes	No
Information security awareness amongst users is core to the success of our plan	Yes	No
Our information security manager is empowered with the infrastructure, tools and supporting mechanisms to properly perform his/her responsibilities	Yes	No

If the answer to any of the above is 'no', serious attention must be given to revisit and reevaluate that aspect, as well as the complete information security governance plan (Solms et al., 2004).

Figure 2 below presents the framework of ISMS (Information Security Management System) dedicated to SMEs.

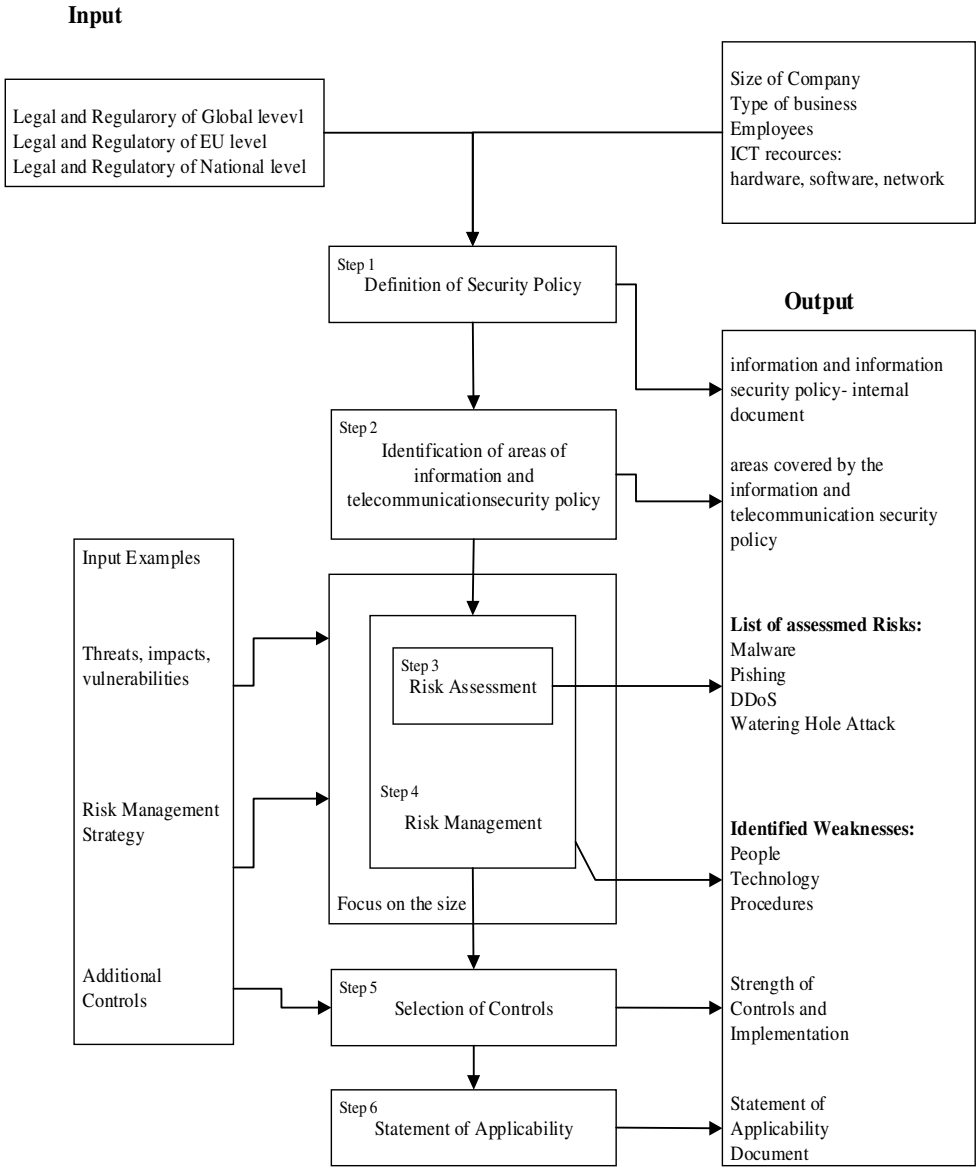

Figure 2. The framework of ISMS (Information Security Management System), elaboration based on ENISA (2017)

Responsibility for the flow of information, shaping the expected skills and implementing the commitment and responsibility of subordinate employees lies with the entrepreneur. It is noted that this responsibility is greater in the case of companies in which decisions are taken by ordinary employees. Therefore, it is now an important issue to make the right recruitment of employees with specific professional and ethical predispositions (Nogalski & Śniadecki, 2007).

As a suggestion for the future research on ethics, the study creates an opportunity towards the ethical principles, which could be implemented in companies regardless of the type and of their activity.

5. CONCLUSION

Due to the huge contribution to global income, SMEs are very important in the economy of all countries in the world.

Nevertheless, although the outcomes of the inquiry, especially in relation to the security of ICT in SMEs may rather be described as negative, in that respect there are some plus signs on the security of ICT, especially in Poland. Considerable pressure from the data protection authority has caused significant issues involving information processing system security. SMEs should have and apply security policy related to technology, procedures and people.

This work demonstrates that the top barriers to adopting better cyber defences are a lack of trained security staff and not sufficient budget. Also, despite the lack of BYOD (Bring Your Own Device) policy in SMEs, they can respond to the overall situation by quickly establishing the mobile device. In fact, IoT (Internet of Things) and in particular mobile devices represent the most vulnerable endpoints in SMEs.

SMEs shouldn't run outdated business software and antivirus software. Moreover, they ought to receive and utilize encryption software, digital signatures, email authentication, policy and reporting protocol.

Business owners should take a look at their data and processes to see how well protected they are. Other recommendations include: providing staff with access to simple, freely available cyber security training and taking a cyber security risk assessment.

REFERENCES

1. Afonin O., How Long Does It Take to Crack Your Password?, Elcomsoft, 2017. [Online] Available at: https://blog.elcomsoft.com/2017/04/how-long-does-it-take-to-crack-your-password/, accessed 2017-12-23
2. Ashford W., SMEs more vulnerable than ever to cyber attacks, survey shows, ComputerWeekly, 2017. [Online] Available at: http://www.computerweekly.com/news/450428246/SMEs-more-vulnerable-than-ever-to-cyber-attacks-survey-shows, accessed 2017-12-21
3. Ashford W., SMEs more vulnerable than ever to cyber attacks, survey shows, ComputerWeekly, 2017. [Online] Available at: http://www.computerweekly.com/news/450428246/SMEs-more-vulnerable-than-ever-to-cyber-attacks-survey-shows, accessed 2017-12-21
4. Basques K., 2018. [Online] Available at: https://developers.google.com/web/fundamentals/security/encrypt-in-transit/why-https, accessed 2018-01-22
5. BetterBuys, Estimating Password-Cracking Times, BetterBuys, 2016. [Online] Available at: https://www.betterbuys.com/estimating-password-cracking-times/, accessed 2017-12-23
6. Chickowski E., State Of Employee Security Behavior, DarkReading, 2015. [Online] Available at: https://www.darkreading.com/endpoint/state-of-employee-security-behavior/d/d-id/1322737, accessed 2017-12-23
7. Chmielarz W., Zborowski M., Analysis of the Use of Electronic Banking and e-Payments from the Point of View of a Client, 2017, Proceedings of the Federated Conference on Computer Science and Information Systems pp. 965–969, [Online] Available at: https://annals-csis.org/Volume_11/drp/pdf/103.pdf, accessed 2017-12-18
8. ENISA, [Online] Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework, accessed 2017-12-23
9. FireEye, Inc., 5 reasons cyber attackers target SMEs, FireEye, 2016. [Online] Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/offers/pdfs/SME-Infographic_web.pdf, accessed 2017-12-20
10. Hau B., Penrose M., Hall T., Bevilacqua M., M-Trends 2016. EMEA Edition, June 2016
11. Horowitz M., Patching Windows XP against WannaCry ransomware, ComputerWorld, 2017. [Online] Available at: https://www.computerworld.com/article/3196289/security/patching-windows-xp-against-wannacry-ransomware.html, accessed 2017-12-21

12. Jabczyński W., Orange Insights: Czyli jak wygląda informatyzacja w małych i średnich firmach w Polsce, [Online] Available at: https://biuroprasowe.orange.pl/informacje-prasowe/orange-insights-czyli-jak-wyglada-informatyzacja-w-malych-i-srednich-firmach-w-polsce/, accessed 2017-12-18
13. Koskosas I. A short literature review in information systems security management approaches, [Online] Available at: http://beman.ase.ro/no32/1.pdf, accessed 2017-12-18
14. McCabe J., FBI Warns of Dramatic Increase in Business E-Mail Scams, FBI Phoenix, 2016. [Online] Available at: https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams, accessed 2017-12-19
15. Millaire P., Sathe A., Thielen P., What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets, 2017. [Online] https://www2.chubb.com/us-en/_assets/doc/17010201-cyber-for-small_midsize-businesses-10.17.pdf, accessed 2017-12-21
16. MobilityNews, [Online] Available at: http://mobilitynews.pl/orange-insights-maly-biznes-duze-zagrozenia-bezpieczenstwo-it-malych-i-srednich-firm/, accessed 2017-12-20
17. Morgnan S., One Milion Cybersecurity Jon Openings In 2016, Forbes, 2016. [Online] Available at: https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#557d022e27ea, accessed 2017-12-23
18. Netmarketshare, Data from Netmarketshare.com , accessed 2017-12-21
19. Nogalski B., Śniadecki J., Zachowania etyczne przedsiębiorców w zarządzaniu polskim przedsiębiorstwami – ujęcie kontekstowe., the chapter In: Wpływ społecznej odpowiedzialności biznesu i etyki biznesu na zarządzanie przedsiębiorstwami, EQUAL, Warszawa 2007, [Online] Available at: http://iped.pl/pliki/publikacje/podrecznik_zfp_2007.pdf, accessed 2017-12-23
20. Orhan F., *Phishing Got Darker. And Smarter,* Comodo Threat Intelligence Lab, January 2018. [Online] Available at: https://www.comodo.com/lab/pdf/phishing-got-darker-and-smarter.pdf, accessed 2017-12-22
21. Paganini P., The hosting company OVH was the victim of a 1 Tbps DDoS attack that hit its servers, this is the largest one ever seen on the Internet, Security Affairs, 2016. [Online] Available at: http://securityaffairs.co/wordpress/51640/cyber-crime/tbps-ddos-attack.html, accessed 2017-12-20
22. Raport CERT Orage Polska za rok 2016, [Online] Available at: https://www.cert.orange.pl/pobierz-raport/14, accessed 2017-12-27
23. Solms B., Solms R., The 10 deadly sins of information security management, Elsevier, 2004. [Online] Available at: https://www.sciencedirect.com/science/article/pii/S0167404804001221?via%3Dihub, accessed 2017-12-23
24. Soomro Z. A, Shah M. H., Ahmed J., Information security management needs more holistic approach: A literature review, International Journal of Information Management, Elsevier, 2016
25. Suiche M., Petya. 2017 is a wiper not a ransomware, 2017. [Online] Available at: https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b?gi=7f56393669bd, accessed 2017-12-26
26. Techopedia, [Online] Available at: https://www.techopedia.com/definition/2387/cybercrime, accessed 2017-12-20
27. United Nations, The ESCWA Cyber Legislation Digest, UN-ESCWA, 2013. [Online] Available at https://www.unescwa.org/sites/www.unescwa.org/files/page_attachments/escwa_cyberlegislationdigest_v7-1_0.pdf, accessed 2017-12-19
28. University of Erlangen-Nuremberg, Researchers investigate user behaviour when unknown messages are received online, PHYS.org, 2016. [Online] Available at: https://phys.org/news/2016-08-user-behaviour-unknown-messages-online.html, accessed 2017-12-19
29. Wittman D., 1000 most common passwords, Github, 2015. [Online] Available at: https://github.com/DavidWittman/wpxmlrpcbrute/blob/master/wordlists/1000-most-common-passwords.txt, accessed 2017-12-18