Accounting and Management Information Systems
Vol. 16, No. 4, pp. 610-632, 2017
DOI: http://dx.doi.org/10.24818/jamis.2017.04009

Exploring cybercrime – realities and challenges

Victoria Stanciu[a], Andrei Tinca[a,1]

[a] *The Bucharest University of Economic Studies, Romania*

Abstract: Cybercrime is a global, transnational serious problem that needs strong technical and legal responses. The information represents an important asset that must be secured and properly used as it provides the support for value creation and sustainable development. Being a valuable asset, the information is exposed to continuous and virulent attacks conducted by cybercrime groups and significant financial and human resources must be allocated to the cybercrime limitation. The purpose of authors' research was to get more knowledge about cybercrime and attacker's behavior and to develop a discussion on the cyber security and the means of its improvement. The research results attempt to provide useful recommendations on countermeasures against cybercrime and raise the awareness of companies' senior management and governments' representatives on cyber criminality.

Keywords: Information security, cybercrime, organized crime, cybercrime prevention

JEL codes: M15

1. Introduction

Information security is no longer a problem keeping in alert just the security specialists. The companies' high dependence on IT makes the board members more

[1] *Corresponding authors*: Department of Accounting and Management Information Systems, The Bucharest University of Economic Studies; Piața Romana no. 6, Sector 1, Bucharest. email addresses: stanciuvictoria58@hotmail.com, andrei.tinca@gmail.com

concerned in security information issues as this potential threat can negatively impact the business and financial objectives achievement. Public institutions' heads, as well as the entire society, recognize the same concern. Information technology immerged in the individuals, companies, public institutions and society life and we are all exposed to a very diverse set of information security incidents caused by more and more complex attacks. The society itself is exposed to security incidents through its entities that could be targeted as for example military entities, security agencies, nuclear plants etc. In a digital global society, there are no borders and the cyberattacks could focus on any target wherever it is located. Economic chains linking different companies characterize the global economy making the companies, in many cases, dependent. The cyberattack affecting one of the companies in this chain could affect entire business in the economic group.

Cyberattacks are increasing in frequency and impact. Cyber criminals are permanently developing new and ingenious methods to hack into the systems. In this respect, the IT security specialists should prove a proactive and preventive approach in increasing the security level of their systems. As the cyber security assaults are more and more sophisticated, the companies' reaction consists in increased investments in information security solutions based on a prioritization scheme and a cost-benefit analysis. The success driver seems to be the proactive thinking of the security experts and the continuous increase of the financial effort in security solutions.

The purpose of this research is to get more knowledge about cybercrime and attacker's behavior and to develop a discussion on the cyber security and the means of its improvement. The authors conducted their research based on a detailed literature review and documentation on cyber criminality and taking part in information security audit teams, this experience providing useful insights for their study. The research results attempt to provide useful recommendations on countermeasures against cybercrime and raise the awareness on cyber criminality between companies' senior management and governments' representatives. Cyber criminality is one of the most sensitive and concerning problems of nowadays. Even so, the Romanian researches and information dissemination on the topic are not reflecting the expected interest. The authors' research conclusions can provide a useful insight for the Romanian IT specialists, given the shortage of Romanian literature on this topic.

2. Methodology

The authors performed a systematic literature review on cybercrime and information security. The authors focused on researches performed worldwide in regard with the IT security and cybercrime, synthesized the main problems emphasized by the scientific researches and analyzed surveys performed by prestigious international organizations, regarding the evolution of cyber criminality. Investigating the scientists and academics' research on the topic the authors retained their opinions and concerns that were synthetized in the following chapters. The research imposed an investigation in regard with the Romanian IT security specialists concerns consisting of interviews (14 interviews were performed with CIOs – Chief Information Officers, of which operating in banking industry -2, and private companies -12) on the topic of cybercrime topic. Applying the consensual-inductive approach the authors succeeded to synthetize valuable points of view that revealed the real dimension and concern for the cybercrime phenomena. Besides the formal interview, each respondent completed a survey and other surveys were sent by e-mail to security information experts; we received a total of 30 surveys. The survey consisted of 9 items, aiming to identify which types of attacks the companies face and whether the number of attacks is increasing. We also tried to gauge how prepared the companies are for cyberattacks, by enquiring about the overall IT budget and how it compares to the previous year, as well as the percentage of the IT budget spent on cyber security. We also aimed to validate the following hypotheses:

H1: *The number of cyberattacks facing my company this year has not changed since last year.* Although it is well-established by numerous international studies that the number of attacks has grown, we wanted to evaluate the situation within our sample.

H2: *The size of our IT budget has stayed the same compared to the last year.* If we were to find an increase in the number of cyberattacks, we would expect to find an increase in the IT budget.

H3: *The IT security department is well prepared to defend against cyberattacks.* Given the importance of IT and the rising level of threat, we attempted to gauge if the companies perceive they are well prepared to respond to attacks.

The present research is part of a wider research project initiated several years ago aiming at tracking the evolution of cyber security and cyberattacks techniques and provide recommendations for strengthen the information systems' security.

3. Literature review

Cybercrime represents "a single event from the perspective of the victim or on-going series of events, involving repeated interactions with the target" (Arora, 2016: 540). In the new context characterized by the wide spread use of computers, mobile devices, and network systems cybercrime became very attractive and provides unlimited means of action to the attackers (Konradt *et al.*, 2016). We are now part of a global digital society in which "individuals, organizations and governments alike are increasingly exposed to the risk and threats of the cybercriminals" (Hunton, 2012: 201). Hunton invites us to a deeper analysis of the cyber security concept and reveals some of its dark and compromising means of manifestation as for example cyber terrorism, cyber warfare, disinformation, espionage, political attack etc. (idem)

Speaking about cybercrime we must approach the sensitive problem of the underground digital economy that emerged in the last years. The immense amount of critical data, stolen in the cyberattacks, (most of them representing personal identity details and banking clients' credentials) represents precious "merchandise" providing financial gains to the cyber criminals. We are facing organized digital criminal markets facilitating the sale, distribution and illicit use of stolen data that will determine a multiplication of the attacks, waves of attacks, over the same targets.

Companies continue to be exposed to "traditional threats" as for example insider threats, malware, loss of mobile devices, social engineering etc. One of the major causes of these "traditional threats" stays in the users' behavior (not observing of procedures and training issues). In the same time the IT security specialists are struggling with nontraditional sophisticated attacks which are characterized by an exponential virulence determined by the technical means, the scenarios used and the organized crime groups being behind the attacks.

The surveys emphasize the shortage of skilled IT security specialists. This issue has a significant impact over the entities (companies, public institutions, government alike). The effectiveness of the IT security solutions depends not only on the security specialist expertize and certification but also in his/hers understanding of the business and industry's particularities. To approach the risk in the most appropriate manner the information security specialist must prioritize the issues and focus on the most critical ones from the business perspective. In this regard, their knowledge in the business' industry characteristics is essential.

The hackers tend to exploit the weakest link in the security chain. In fact, the level of security of an information system is not provided by the most sophisticated solutions implemented but by the weakest point in the global security architecture and policy. There still exist vulnerabilities, exposing the companies' information security, which, normally should be solved for long as for example default passwords and inadequately secured or configured systems being known the numerous flag alert issued on the topic by the security frameworks. Nevertheless, these kinds of vulnerabilities still exist and as consequence, new attack paths are opened. Nowadays, the hackers' high expertize and techniques allow them to take on systems presumably defended by top security solutions.

Another issue reflected by the global surveys consists in the demarcation between the business management and the IT managers, a problem that continues to exist despite of numerous alerts signaled during the years (Mangiuc, 2016). As the international studies emphasize, most of the chief information officers (CIOs) continue to report through the IT business line. Just 30% of the ISACA 2015 survey's respondents declare that are reporting to the board. This "traditional" reporting line does not benefit the company as long as the business dependence on IT is so critical today and reflects the technical perspective manifested by the business executives in regard with IT. Nowadays, when business is highly dependent of IT systems, business management express its awareness and concern in regard with IT importance for the business and the need to better monitor IT risks in a global approach as business risks. Despite this, management still promotes inadequate reporting lines for the IT function. This new understanding of the IT role and significance for the business is not reflected in the companies' board structure if the IT heads are not members of the board. Exceptions are the big companies, where the IT head is often a board member and, from this position, is part of the decision-making process. Unfortunately, if IT heads consider that IT functions is proving this pro-active role, the business executives still appreciate that IT continues to have a more reactive role (ISACA and ITGI, 2011). This different perception about IT pro-active vs. reactive role reflects the high expectations of business executives and the important existing room for a better communication between IT and business executives.

4. Snapshots on current cybercrime state

The global surveys emphasize as the most powerful types of attacks the followings: phishing, malware, social engineering, hacking, loss of mobile devices, insider theft, SQL injections, watering hole, man-in-the middle attack. So the extent of attacks is very diverse as also the techniques used. This makes their detection more difficult. Nowadays one of the most critical security issues is the attacks detection. The reported attacks and the international surveys show that in many cases, there is a high delay between time to compromise and time to discovery the attack. This reflects the attackers' ability and knowledge in systems penetration and hiding the penetration traces.

Today, it is obvious that the attacks present a stronger economic motivation and are orchestrated by criminal organized groups. Verizon emphasized in its report on 2016 that "89% breaches have a financial or espionage motive" (Verizon, 2016: 1). In 2014, the annual average cost of cybercrime registered per retail US company was up to $8.6 million (Ponemon Institute, 2014). The four primary external consequences emphasized by the Ponemon study are: business disruption, equipment damage, information loss and revenue loss (idem). Kaspersky bulletin on security for 2015 reflects very clear that these attacks focus on financial illegal gains: 1.966.324 registered notification regarding attempted malware infection aimed at stealing money via online access to bank accounts (Kaspersky, 2015a). Online banking attacks are now more oriented via mobile devices. Two Trojan mobile banking, Faketoken and Marcher, developed to steal payment details, are on the top for Android devices attacks. Perpetrators seem to be also focus on ransomware attacks. In 2015, 753.684 computers of unique users were targets for ransomware attacks most of them being conducted by DDoS techniques (Kaspersky, 2015a).

Nowadays, money is present in different formats: traditional metal coins and banknotes, account money (non cash money) and e-money. If "traditional physical money" cannot be subject to cyber attacks, banking accounts and e-money are. We have already presented the concerning consequences of the attacks on companies and banking accounts. E-money is also a tempting target, cryptocurrency wallet services being important targets for cybercriminals. Coinkite (one of the earliest bitcoin wallets) had to shut down its service due to constant DDoS attacks. Kaspersky labs issued the Q2 2016 report regarding DDoS attacks alerting on the virulence of these attacks. In Q2 2016 the "longest DDoS attack lasted for 291 hours" (Kaspersky, 2016).

Verizon report on 2016 considers that "63% of confirmed data breaches involved weak, default or stolen passwords" (Verizon, 2016:20). This is a concerning finding if we take into consideration the impact of this vulnerability and its causes: weak policy in regard with passwords! The good practice in regard with password is so well known, easy to access on professional sites and implement. Why we are not following it? This issue on weak and default passwords is emphasized year by year in the international analysis.

"The companies that have an awareness program in place actually have a higher rate of human-dependent incidents such as social engineering, phishing and loss of mobile devices" states the ISACA report on 2015 (ISACA, 2015: 6). The ISACA survey performed in 2015 emphasize that only 55% of the respondents' enterprises restrict USB access and 42% restrict access to social media (idem). It is like letting the door opened and remained amazed finding strangers into your house!

The 2016 Symantec Internet Security Threat Report emphasizes that there are over one million web attacks against people each day in 2015, and a new zero-day vulnerability is found every week. The same report underlines the recrudescence of ransomware attacks the new targets being represented by smartphones, Mac and Linux systems (Symantec, 2016).

In this landscape, we briefly introduce the most important and consequential cyber-incidents of 2016:

- Emails were stolen from the Democratic National Committee in the United States and leaked on-line; the attack cannot be attributed with certainty although it is believed state actors are behind the breach (Greene, 2016);
- Yahoo announced that half a billion accounts were compromised starting with 2014, making it the largest compromise of user accounts so far.
- In the Panama Papers incident, data was stolen from a law firm, exposing financial information on international political figures. The hack was attributed to software, which was not up to date, and weak security controls (Greene, 2016).
- As-yet unidentified hackers transferred 81 million dollars from the Central Bank of Bangladesh, by initiating transfers in the bank's SWIFT system. The hackers used stolen credentials and the incident was blamed on weak security such as the absence of a firewall (Quadir, 2016).
- Bitfinex, a bitcoin platform, was hacked resulting in a loss of 70 million dollars. The loss was ultimately supported by the platform's users, who took a 36% loss on their holdings (Kaminska, 2016).
- Tesco Bank clients lost 4,5 million dollars in a hack targeting mobile applications with weak security. The bank, which "ignored repeated warnings" on the weak security of its mobile applications, had to reimburse its clients for the lost amounts and undergo investigation by the National Crime Agency in the UK (Arnold, 2016).

The international surveys (Kaspersky, 2015b) place Romania in the group registering medium risk for online infection. Even so, the Cert Report issued in 2016 is concerning (CERT, 2016):

- In 2015, CERT-RO has analyzed 68.206.856 cyber alerts each cyber alert representing a signal related to an IP address or web domain (URL) regarding a possible security incident or a security incident that implied or could imply Romanian information systems own by companies or individuals.
- 26% of the IPs allocated in the Romanian cyberspace were subject of at least one investigation performed by CERT-RO.
- 78% (5.3 millions) of the analyzed alerts were related to unsecured information systems (inadequate secured or configured). Hackers used parts of those vulnerable systems to initiate attacks on other systems (in Romania or outside Romania).
- 20.78% (14 mil.) of the analyzed alerts were generated by malicious software, mainly botnet type.

5. Analysis of the most prominent incident types

In the following section, we will describe the most prominent attack types, their impact and possible mitigation techniques.

4.1. Denial of service

In a *denial of service* (DoS) incident, the attackers send many fake requests to a target server, attempting to overwhelm the server's capacity to respond. Typically, the targeted server cannot distinguish between legitimate requests made by real clients and the large quantity of fake requests sent by the attackers. Thus, the real clients will not be able to access the server, resulting in a service outage. The impact can be considerable for businesses who rely on on-line services to serve their clients, and especially for banks, where a service outage can greatly damage the client's trust in the bank's ability to safeguard a client's funds and offer timely access or financial entities as for example financial markets.

To amplify the size of the attack and the amount of traffic sent to the target, hackers will attempt to use many computers as sources for their fake requests. An attack launched from multiple computers is called a *Distributed Denial of Service* (DDoS) attack. Defense against this type of attack is very difficult because the offending traffic originates from a large pool of IP addresses and the fake requests cannot be easily identified and filtered.

Aiming to take control over computers, hackers infect devices connected to the Internet with malware, using different delivery methods, such as worms or phishing. The malware installs on the host and attempts to stay undetected, employing anti-virus evasion techniques; more advanced malware also attempts to spread to other computers in the network, increasing the number of machines under the attacker's control. Such a network of infected computers is called a *botnet*. The attackers control the botnet by issuing commands from a central control server, indicating the IP address of the target, timing details of the attack etc. More sophisticated communication methods employ encryption, so that commands evade detection.

DDoS attacks are not new, but they constantly increase both in number, size, and the methods of attacks employed. The most important DDoS incident so far took place in October 2016 and involved "tens of millions of infected computers, including a network made of 'internet of things' devices" (Kuchler, 2016).

Unlike previous incidents, the attackers used a botnet made up of IoT devices—webcams, video recorders and routers, connected to the Internet. These types of devices have grown in usage in recent years, but their security is weak. Also, their owners cannot easily observe unusual behavior patterns, because often these devices do not have monitors and keyboards making interaction and configuration difficult. Most of the users just connect them to the Internet, without changing the default password, and hackers who infected tens of millions of devices used this vulnerability.

The attack was also innovative in its choice of the target, by flooding a crucial service on which other users rely to connect to the Internet. The attackers flooded the servers of Dyn, one of the major DNS (domain name service) providers, who translate web addresses into IP addresses. Users connecting to the Internet rely on this service to connect to other sites, and because of the outage, a large part of the Internet was disrupted. Major sites such as Twitter, Spotify and Airbnb were unreachable. The manufacturers of the affected devices who chose to take responsibility also felt the impact and issue software updates or even recalls the equipment. Telecommunication companies affected by the flooding also incurred costs related to upgrading their infrastructure to better respond to such incidents.

This incident highlighted several important security issues, which are difficult to address. First, the attackers took over webcams and other devices with low intrinsic "value" in themselves, as opposed to a high-value targets (such as a server holding credit card data). But because of the sheer number of devices, the effects were greatly amplified. Second, the manufacturers of these "Internet of Things" devices pay little attention to security, because of cost issues and due to a lack of experience. Also, given the many different types of devices (connected TV's, cameras, medical equipment) it is very difficult to enforce meaningful regulation across different types of industries (Kuchler, 2016a).

By simultaneously affecting so many high-profile sites, the attack also highlighted a weakness pertaining to the architecture of the Internet. The DNS was devised during the 1980's when security was not a concern, and scenarios such as these were not envisioned. It is forecasted that denial of service attacks involving Internet of Things devices will affect 25% of companies, but only 10% of budgets are allocated for protection against this kind of attacks (Kuchler, 2016).

4.2. Ransomware

Ransomware is a type of malware that denies a user's access to computer resources, by locking access to the computer itself or to important files on computer. After taking control of the computer, the ransomware usually displays a message asking money from the user in order to restore access to the computer. The main infection mechanisms are via e-mail, when the user opens an attachment, or by drive-by-download, when the user visits a web site with malicious content that automatically downloads on the user's computer. After the infection, users typically have three choices: try to restore the system from backup, pay the ransom and get access to the data, or lose the data (Sittig, 2016).

Ransomware attacks have grown significantly during the last years, with an estimated 2.3 million users being affected in 2016, compared to 1.9 million in 2015, representing a 17.7% increase. In the same period, mobile ransomware (affecting mainly Android devices) has grown 400% (Kaspersky, 2016). During 2015, the cost from ransomware attacks was $24 million, while the cost for the first three months of 2016 was $209 million (Finkle, 2016).

There are two main types of ransomware: locker ransomware and crypto ransomware, both with different methods of extorting money from the users. In the case of locker ransomware, access to the computer is blocked, and the user is asked to buy vouchers or call a pay-line to redeem access. This type of infection is relatively easy to remove using an anti-virus, which recognizes the malware, but advanced users can recover files by bypassing the operating system and accessing files directly on the disk (Savage, 2015).

Crypto ransomware is the more destructive variant of ransomware, with more sophisticated strains causing increased damage recently. After installation, the malware searches for the user’s documents on the computer (text files, images, spreadsheets) and encrypts them with a secret key. Antivirus programs could defeat the first versions of crypto ransomware, as the malware often used symmetrical algorithms and left the encryption keys on the infected machine. However, modern variants implement industrial-strength encryption—such as RSA, 3DES and AES—use strong procedures to make sure the users cannot get around paying the ransom (Savage, 2016). Thus, depending on the strength of the encryption methods used, files might be impossible to recover, if the malware properly implements an asymmetric key encryption scheme. In such a case, a public key is used to encrypt the user’s files, and recovering the public key does not help decrypt the files. The corresponding private key (which can decrypt the files) is held on the attacker’s server, and is only sent to the “victim” after the ransom has been paid. Examples of Trojans that implement strong encryption and key management include CryptoLocker and Cryptowall, which accrued an estimated $18 million by June 2015 (FBI report, 2015).

While locker ransomware asks the user to buy vouchers, crypto ransomware usually asks for a ransom to be paid in bitcoins, as the computer is still functional (only access to the files is blocked) and the user is expected to make the payment through the computer. Bitcoin payments offer anonymity and are hard to track, and hackers are known to use multiple layers of “laundering”, making it even more difficult for authorities to pursue ransom payments back to the hackers (Shulman, 2016).

The amount of the ransom varies depending on the targets chosen by the hackers. When malware is distributed indiscriminately in so-called "blanket attacks", then the usual amount varies from $300 to $700, depending on the country where the "victim" is located. But hackers are also mounting targeted attacks, using specially crafted e-mails to target organizations such as "financial firms, Internet service providers and organizations holding sensitive personal information such as healthcare bodies" (Everett, 2016).

In targeted attacks, hackers choose organizations which don't have very strong security defenses, and for whom data loss would have a major negative impact, affecting their business relation with the clients. Many such cases are not publicized, since the organizations fear losing confidence with their clients, but several high-profile cases are:

- The attack on the Hollywood Presbyterian Medical Center (February 2016) in which all patient and medical records were encrypted. The hospital's computer network and other computer-dependent functions, such as computer tomography scan, laboratories and pharmaceutical records were taken off-line for a week. Despite the involvement of security experts, the hospital finally payed a ransom of 40 bitcoins (equivalent of $17,000) and recovered access to its computer resources. In the same period, other hospitals were hit by ransomware (Tuttle, 2016).
- In October 2016, a hospital in Lincolnshire, United Kingdom, had to cancel all scheduled surgery operations and divert new emergency cases to nearby locations (Krebs, 2016). The hospital had been targeted with ransomware, which then spread across the network to affect the whole IT infrastructure. The hospital called a "major incident" chose to shut down most its system to deal with the attack. It is estimated that during 2016, 30% of the hospitals in the UK have been infected by ransomware (Leyden, 2017).
- In February 2017, the Licking County in Ohio, US, had its servers and approximately 1000 workstations locked down by ransomware, which was delivered by an infected email (Biggs, 2017). The government offices and police force were shut down, and telephone access to emergency lines was restricted and had to be operated manually.

As the number and severity related to ransomware attacks is growing, so are the evasion techniques employed by the malware creators. These involve partial download of the malicious code, and detecting whether the malware runs on a "real" computer, as opposed to a virtual machine. Antivirus companies analyze malware inside virtual machines, to contain potential damage and control the analysis process. But malware creators have become adept at detecting when their software is running inside simulated environments, using advanced techniques such as detecting the entropy of the filenames and their distribution on the hard disk (Kharaz, 2016).

As it is very difficult to recover from a crypto-ransomware attack, the best technique is to prevent and mitigate the effects of possible attacks. Users should (Pathak, 2016):

- Make regular backups of program files and data. Given that malware often infects network shares, it is important to store the backups off-line, separate from the network where an infection could spread from a workstation;
- Use a reputable antivirus program and keep it updated;
- Keep all installed software up-to date, to prevent infection with malware which exploits vulnerabilities;
- Educate the users to be cautious with opening unknown email attachments, as malware often arrives via phishing e-mails.

4.3. Zero-day attacks

Zero-day attacks refer to exploits that affect vulnerabilities unknown to the developers. Thus, since there are no known remedies or patches, this type of attack has a very high chance of spreading quickly, since the usual defenses, such as firewalls and anti-virus solutions are ineffective. However, zero-day vulnerabilities are hard to discover, and those who eventually discover them have some typical options, according to their intentions (Ablon, 2017). Security advocates and white-hat hackers maintain that vulnerabilities should be disclosed to the manufacturer of the software, so that a patch that fixes the vulnerability can be issued. Black-hat hackers can create exploits to take advantage of the vulnerabilities, infecting systems and causing damage. But the discussion is more nuanced for national governments, who invest heavily in cyber security and are actively searching for zero-day exploits. Thus, national governments can choose to disclose the zero-day vulnerabilities, but they lose the advantage over their adversaries once the vulnerabilities are patched. The other choice is not to disclose the vulnerabilities and create exploits for later use—thus effectively creating cyber-weapons. Yet another category is represented by companies who sell zero-day vulnerabilities, with prices ranging from tens of thousands of dollars up to several hundred thousand for vulnerabilities in operating systems considered harder to break, such as Apple’s iOS (Ablon, 2017).

Vulnerabilities exist in all layers of the software stack, from operating systems, middleware up to the application layer—putting every company, as well as individual users at risk. So how can IT professionals defend against such attacks, especially when no known remedies are available? According to a study published by the SANS institute, the best practice is to implement a defense-in-depth strategy, organizing security in layers (Hammarberg, 2017). At the outside, the network must be protected by firewalls with tight rule management, implementing strict controls over the data moved to and from the network. Inside, the network should be monitored for suspicious activity. This is usually achieved with a network monitoring system, which recognizes known patterns of attack—for example hosts from within the network sending spam or participating in a DDoS attacks, or trying repeatedly to contact other hosts in the network, which can be the sign of malware trying to spread. Most notably, transfers of atypical sizes are to be watched, as they can signal that a malicious actor is moving data outside the network.

The last technical defense is the firewall and anti-virus implemented at host level, coupled with other physical security measures, such as USB and network port restrictions. Even if zero-day exploits take advantage of unknown vulnerabilities—and thus are not contained in anti-virus databases—current anti-virus solutions implement advanced detection mechanisms, using statistics and behavior analysis techniques to identify malicious activities. At the same time, hackers expend great efforts to stay undetected, using techniques such as polymorphism to change the appearance of the malware code, to avoid signature-based detection.

But often the “weakest link” in the security chain is the human element. Sooner or later, we are likely to click on malicious links and open e-mails regardless of our level of training and awareness. At that point, the entire chain of defense-in-depth elements and processes must work together to detect and prevent the exploitation of vulnerabilities.

However efficient, the concept of defense in depth is expensive to implement because it involves many technologies and processes. Smaller organizations, with limited security budgets and personnel will find it more difficult to implement a security policy coordinated across multiple elements and processes. Larger organizations have more available resources, and even if the per-user cost is lower than in small organizations, the overall amount is the largest. Most notably, these companies adhere to written policies, implement separation of duties and only grant the privileges necessary for each user to do their job (Hammarberg, 2017).

5. Results and discussion

First, we asked our respondents what type of attacks they most often encountered during 2016-2017, and the most important was ransomware, mentioned by 76.7% of our respondents.

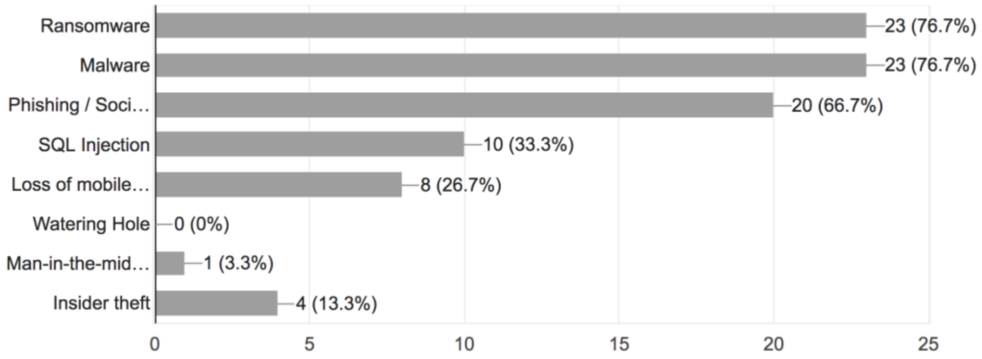

Figure 1. What types of attack affected you most often?

In the formal interview, it was revealed that ransomware grew tremendously compared to the previous period, and that it was by far the most troublesome issue confronting the IT departments. An equal percentage (76.7%) mentioned malware (key loggers, fake antivirus etc.). The third most-mentioned attack was phishing (66.7%), causing constant trouble for IT security personnel. Following were SQL injections (33.3%) and loss of mobile devices (26.7%)—which emphasizes the importance of properly securing mobile devices—which is not easily feasible with devices belonging to the employees. These security issues Romanian companies experienced in the last year are the ones most frequently identified by international surveys as we presented in the above chapters. In this respect, there are no significant differences compared with the international IT security incident types.

In the next question, we attempted to gauge how the number of security incidents has changed compared to the previous period. We measured the responses using a Likert 1-5 scale, and we illustrate the results below:

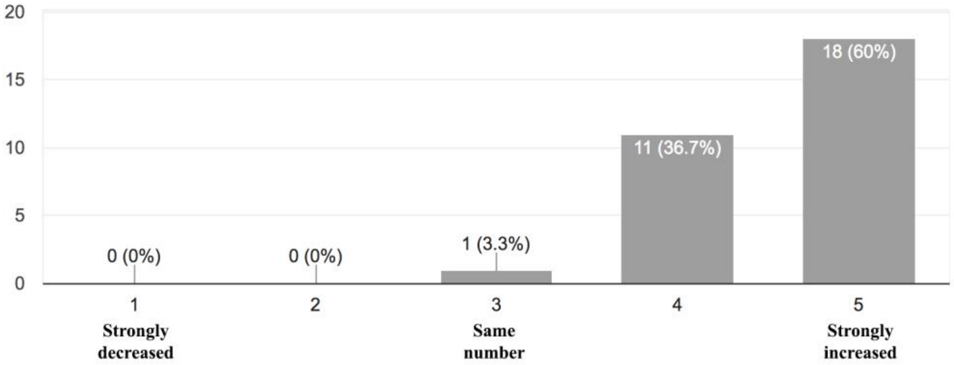

Figure 2. How has the number of attacks changed compared to the previous year?

Over 96% of the respondents agreed that there was an increase in the overall level of attacks. In the formal interviews, some respondents stated that “this year was a nightmare”. Only a single respondent saw a decrease in the number of attacks, which should be interesting to investigate as a further research theme.

To better understand the nature of the attacks, we looked at the motivation behind the attacks. Here, again, the responses were concentrated around two answers, as illustrated in Figure 3:

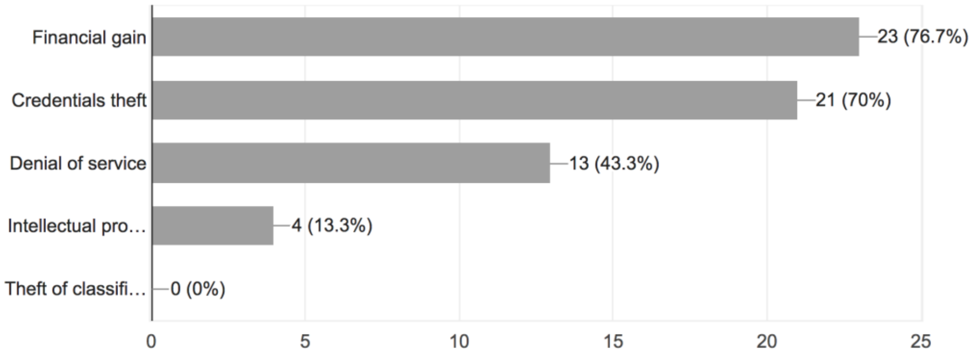

Figure 3. In your opinion, what was the motivation behind the attacks?

The most often mentioned cause of attack was financial gain, which correlates well with the fact that ransomware was the most frequent attack. The next most-important motivation was credentials theft, which can also lead to quick financial gain for the attackers. Denial of service is a distant third, while the rest of the motives seem unimportant. It is apparent that most the attacks are motivated by quick financial gains.

Next, we tried to gauge whether companies restrict access to social media, with the goal of enhancing security and productivity. We expected to see at least some restrictions being implemented, but the results showed otherwise, as per Figure 4.

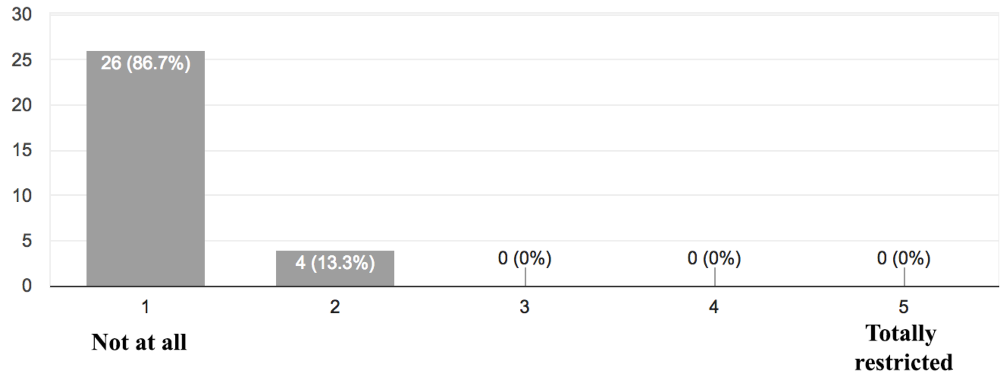

Figure 4. In your company, is access to social media restricted?

The vast majority of the companies in our sample (86.7%) did not implement any restrictions. In our formal interviews, we gathered that access to social media is perceived to be beneficial for productivity, by providing an important communication channel. Also, it was apparent that there was no point in banning access since employees can use social media from their own mobile devices.

The next question focused on the number of security incidents faced by the companies in our sample, and the average number was is 3.1, with a maximum of 5 attacks faced by one single company (Figure 5; on the x-axis we illustrate the number of incidents). The distribution is centred on the average of 3.1 incidents, with the median also at 3.

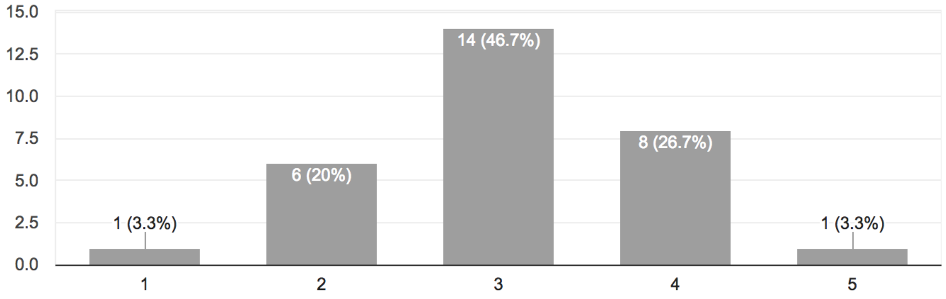

Figure 5. Number of security incidents during the last year

As a further research direction, it would be interesting to find out how the budget expended on IT security and the competence of IT security staff, correlates with the number of attacks faced by a company.

Our next question gauged the percentage allocated to IT from the overall budget of the company. In Table 1, we illustrate the distribution of IT spending among our respondents.

Table 1. Percentage of IT budget in the total budget during 2016-2017

Percentage of budget allocated to IT	Percentage respondents	Cumulative respondents
1%	13.3%	13.3%
2%	16.7%	30%
3%	36.7%	66.7%
4%	16.7%	83.4%
5%	16.7%	100%

On average, the IT budget represented 3% of the total budget, with the median also at 3%. In our informal interviews, we found out that this percentage was similar to 2015-2016, even though we were expecting to see an increase, attributed to the growing number of incidents and the relative importance of IT.

Of the 3% average IT budget, companies spend an average of 5% on IT security, with a median spending of 5%, as illustrated in Table 2.

Table 2. Percentage of IT Security budget in the total IT budget during 2016-2017

Percentage of IT budget allocated to security	Percentage respondents	Cumulative respondents
2	6.7%	6.7%
3	6.7%	13.4%
4	23.3%	36.7%
5	23.3%	60%
6	23.3%	83.3%
7	16.7%	100%

Most the companies spend between 4-6% of the IT budget on security, and the distribution is skewed to the right. Again, as a further research theme, it will be worth investigating the relation between the number of incidents and the security budget.

Next, we attempted to find out whether companies issue formal, periodical IT security reports. In Figure 8, we gauge the answers on a Likert 1-5 scale.

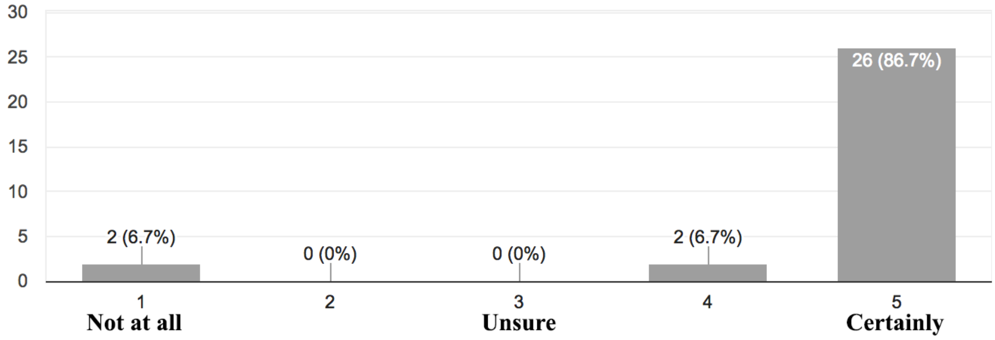

Figure 8. Does your company issue a periodical IT security report?

86.7% of the companies in our sample issue IT security reports, which we appreciate as positive factor for IT security (median of 5 corresponding to “certainly”, the distribution is left skewed). Moreover, in our formal interviews we found out that most the companies address these reports to the CEO, thus enhancing visibility and awareness across the company. It is surprising to see that 6.7% of the companies in our sample are not providing periodical reports on information security. In these cases, it can be considered a misunderstanding of the IT security importance for the company at the top management level and an inadequate risk management process that should also be attentively monitor by the executive management and board of directors.

In our last question, we wanted to evaluate whether the companies feel they are well prepared to face the growing level of IT threats. The responses were recorded on a Likert 1-5 scale, and we present the responses in Table 3.

Table 3. Do you feel you are prepared to defend against future cyber-attacks?

Level of cyberattack response preparedness	Percent respondents
Not at all	6.7%
Very little	43.3%
Somewhat	46.7%
Prepared	3.3%
Well prepared	0%

With the distribution being strongly skewed to the right (median corresponding to “very little”), we conclude that most of the companies think they could be more prepared for cyberattacks. Thus, it would make sense to revise the budgets allocated to IT security as well as propose more training for security personnel.

Informally, most of the CIO’s complained that IT security budgets are insufficient and not commensurate with the current level of threats. Even when there are sufficient budgets, the CIOs opined that there are excessive hurdles in the way of implementing security solutions (bureaucratic, resistance to change etc.) Unfortunately, the overall impression is that security is still treated superficially, with insufficient budgets and attention allocated.

6. Testing the hypotheses

In *H1* we hypothesized that the companies have seen an equal number of attacks between 2015-2016 and 2016-2017. Thus, the hypothesized average was 3 (corresponding to “number of attacks has stayed the same)”. We ran a t-test with a hypothesized mean of 3. The mean of the sample was 4.55 with a standard deviation of 0.57. With a Sig. 2-tailed of 0, we reject the hypothesis and the test concludes significantly that the number of attacks faced by the companies in our sample has increased.

In *H2* we hypothesized that the size of the IT budget has stayed the same, corresponding to a hypothesized mean value of 3 (corresponding to “the budget has stayed the same”). We run a t-test with a hypothesized average of 3. The mean of the sample was 3.06 with a standard deviation of 1.41; the Sig. 2-tailed was 2 so we fail to reject the hypothesis, concluding that the budget has not changed between periods.

In *H3*, we hypothesize that the companies are prepared to deal with cyberattacks, corresponding to a hypothesized mean of 4 (“well prepared”). We run a t-test with the corresponding hypothesized mean of 4. The sample mean was 1.96, with a standard deviation of 0.62. With a Sig. 2-tailed of 0, we reject the hypothesis and the test concludes significantly that the companies assert that they are not sufficiently prepared to deal with cyberattacks.

In conclusion, we show that companies face an increasing number of attacks, relying on stagnant budgets, while the security staff is inadequately prepared. The informal interviews revealed that the CIOs feel that security is treated “superficially” and this should be a warning to management.

7. Conclusions

Cybercrime is a global, transnational serious problem that needs strong technical and legal responses. It is obvious that the attacks orchestrated by criminal organized groups are characterized by a stronger economic motivation. The tremendous increase of criminal attacks and their impact, financial inclusively, are concerning being registered an ascendant spiral that seems to break the most secured systems and networks. Even if the present security picture is not anxious we should recognize that it is not reflecting the complete scene of cyber criminality many of the attacks being unreported.

Aiming at increasing information security it should be promoted a pro-active attitude from IT heads and senior management alike. IT risk is no longer just a technical risk in CIOs responsibility but also a business risk that should be managed in an integrated approach next to all significant risks.

Our quantitative research has shown that companies are confronted with a raising number of attacks, while the budgets are stagnating and the security personnel is insufficiently trained. The informal interviews have also revealed that security is deteriorating, and that even when budgets are available, there are hurdles in the way of implementing security solutions. However, companies issue periodical IT security reports addressed to the CEOs; this should raise visibility and awareness on security issues.

The divers and virulent attacks show us the need for a permanent improvement of the information security architecture. A risk based-approach meaning a permanent risk monitor and assessment, risk response prioritization in a cost-benefit approach should characterize this ongoing process. “Traditional vulnerabilities”, most of them involving human behaviour and actions, continue to expose companies to tremendous risks. In this regard, risk culture improvement and continuous employees’ training should provide the needed risk awareness. New IT threats should be treated by CIOs in a more pro-active approach based on critical business analysis and risk response strategy.

References

Ablon, L. & Bogart, A. (2017) “Zero days, thousands of nights”, RAND Corporation, Available on-line at http://www.rand.org/content/dam/rand/pubs/research_reports /RR1700/RR1751/RAND_RR1751.pdf. [Accessed on March 2017]

Arnold, M. (2016) “Tesco Bank ‘ignored warnings’ about cyber-weakness”, *Financial Times*, November 13, Available on-line at: https://www.ft.com /content/ec81f30a-a82b-11e6-8b69-02899e8bd9d1. [Accessed on March 2017]

Arora, B. (2016) “Exploring and analysing Internet crimes and their behaviour”, *Perspectives in Science*, vol. 8: 540-542

Biggs, J. (2017) "Ransomware completely shuts down Ohio town government", *Techcrunch.com*, 2rd of February 2017. Available on-line at https://techcrunch.com/2017/02/02/ransomware-completely-shuts-down-ohio-town-government [Accessed on March 2017]

Federal Bureau of Investigation Report (2015) "Criminals continue to defraud and extort funds from victims using Cryptowall ransomware schemes", June 23, available on-line at https://www.ic3.gov/media/2015/150623.aspx. [Accessed on December 2016]

Everett, C. (2016) "Ransom note-pay or don't pay? Ransomware on the rise", *Diginomica.com*, February 16. Available on-line at: http://diginomica.com/2016/02/16/ransom-note-pay-or-dont-pay-ransomware-on-the-rise/ [Accessed on December 2016]

Finkle, J. (2016) "Ransomware: Extortionist hackers borrow customer-service tactics", *Reuters*, 12 April. Available on-line at http://www.reuters.com /article/us-usa-cyber-ransomware-idUSKCN0X917X [Accessed on December 2016]

Greene, T. (2016) "Lessons learned from the 7 major cyber security incidents of 2016", available on-line at http://www.networkworld.com/article/3150075/ security/lessons-learned-from-the-7-major-cyber-security-incidents-of-2016.html. [Accessed on February 2017]

Hammarberg, D. (2014) "The best defences against zero-days exploits for various-sized organizations", SANS Institute. Report available on-line at https://www.sans.org/reading-room/whitepapers/bestprac/defenses-zero-day-exploits-various-sized-organizations-35562

Hunton, P. (2012) "Data attack of cybercriminal: Investigating the digital currency of crime", *Computer Law & Security Review*, vol. 28: 201-207

Kaminska, I. (2016) "Bitfinex and a 36% charge from the school of life", *Financial Times*, August 9. Available on-line at https://ftalphaville.ft.com/2016/08/09/ 2172299/bitfinex-and-a-36-per-cent-charge-from-the-school-of-life/ [Accessed on March 2017]

Kaspersky (2016b) "KSN Report: Ransomware in 2014-2016", *Kaspersky Labs*, June 2016, available on-line at https://securelist.com/files/2016/06/ KSN_Report_Ransomware_2014-2016_final_ENG.pdf. [Accessed on January 2017]

Kaspersky (2016) "Kaspersky DDoS Intelligence Report for Q2 2016", *Kaspersky Labs*, Available on-line at http://AO Kaspersky Lab. [Accessed on February 2017]

Kaspersky (2015a) "Kaspersky Security Bulletin 2015. Overall Statistics for 2015", *Kaspersky Labs*, Available online at http://AO Kaspersky Lab. [Accessed on February, 2017]

Kharaz, A., Arshad, S., Mulliner, C., Robertson, W. & Kirda, E. (2016) "UNVEIL: A large-scale, automated approach to detecting ransomware", *Proceedings of the 255th USENIX Security Symposium*, August 10-12, 2016, Austin, Texas. Available on-line at https://www.usenix.org/system/files/conference /usenixsecurity16/sec16_paper_kharraz.pdf. [Accessed on March 2017]

Konradt, C., Schilling, A. & Werners, B. (2016) “Phishing: An economic analysis of cybercrime perpetrators”, *Computer and Security*, vol. 58: 39-46

Krebs (2016) “Computer virus crillpes UK hospital system”, October 2016. Available on-line at https://krebsonsecurity.com/2016/11/computer-virus-cripples-uk-hospital-system/ [Accessed on December 2016]

Kuchler, H. (2016) “Internet of things was mobilized for internet outage, says Dyn”, *Financial Times*, October 23 [Accessed on March 2017]

Kuchler, H. (2016) “Connected devices create millions of security weak spots”, *Financial Times*, October 23 [Accessed on February 2017]

ISACA (2015) “State of Cybersecurity: Implications for 2015. An ISACA and RSA Conference Survey”, Available on-line at https://www.isaca.org /cyber/documents/State-of_Cybersecurity_Res_Eng_0415.pdf. [Accessed on February 2017]

ISACA, ITGI (2011) “Global Status Report on the Governance of Enterprise IT (GEIT – 2011)”, Available on line at www.isaca.org/Knowledge-Center. [Accessed January 2017]

Leyden, J. (2017) “Ransomware brutes smacked 1 in 3 NHS trusts last year”, *The Register*, 17 January, Available on-line at: https://www.theregister. co.uk/2017/01/17/nhs_ransomware/ [Accessed on March 2017]

Mangiuc, D. (2016) “Accountants and the cloud – Involving the professionals”, *Accounting and Management Information Systems*, vol. 16(1): 179-198

Ponemon Institute (2014) “Cost of cyber crime study”, Traverse City, Available on-line at http://www.ponemon.org/glog/2014-global-report-on-the-cost-of-cyber-crime [Accessed on December 2016]

Quadir, S. (2016) “Bangladesh Bank exposed to hackers by cheap switches, no firewall: police”, *Reuters*, April 22, Available on-line at http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0XI1UO [Accessed on February 2017]

Savage, K., Coogan, P. & Lau, H. (2015) “The evolution of ransomware”, August 6, Report available on-line at http://www.symantec.com/content/en/us /enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf. [Accessed on October 2016]

Shulman, A. & Patel, D. (2016) “CryptoWall ransomware attacks are carried out by a small set of attackers”, February 9, Available on-line at https://www.imperva.com/blog/2016/02/cryptowall/ [Accessed on December 2016]

Symantec (2016) “2016 Internet Security Thereat Report”, Available on-line at www.symsntec.com. [Accessed on February 2017]

Sittig, D. & Singh, H. (2016) “A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks”, *Applied Clinical Informatics*, vol. 7(2): 624-632

Tuttle, H. (2016) “Ransomware attacks pose growing threat”, *Risk Management Magazine*, May 2, Available on-line at http://www.rmmagazine.com/2016/05/02/ransomware-attacks-pose-growing-threat/ [Accessed on December 2016]

Verizon (2016) “2016 Data Breach Investigation Report”, available on-line at http://www.verizonentreprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf. [Accessed February 2017]