Chapter 4

Aligning a Cybersecurity Strategy with Communication Management in Organizations

Ileana Hamburg and Kira Rosa Grosch

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75952

Abstract

Cyberattacks are a constant threat to organizations. Despite the improvement of cybersecurity (CS) techniques, criminals have developed sophisticated ways to disrupt systems and steal data particularly in organizations. The need to prepare them for cyberattacks is very important. **CS professionals** (CSPs), have a responsibility that should include protection against moral damage and protect moral rights to ensure the correctness, reliability, availability, and security of all aspects of information and information systems. In case of an emergency, effective communication is crucial. If IT systems fail, a quick communication with employees is necessary as well as to coordinate an effective response. This chapter starts with some explication about CS and later shows the problems organizations face when cyberattacks appear: The chapter describes methods for an efficient communication and its integration into CS strategy of the company. The scope of the chapter is to discuss with academics who work in the field of communication and CS and with students to find new scientific methods in this relative new domain based on some practical experience; and to help organizations and employees particularly CSPs to develop communication plans and to integrate them in their CS plans. The authors have experience will contribute that results will be integrated in the curriculum of cybersecurity from VET and HE students.

Keywords: cybersecurity CS, CS professionals, cyberattacks, cloud computing, platforms

1. Introduction

In the last years, cyberattacks are a constant threat to organizations. The companies and public offices have taken some cybersecurity precautions to strengthen security within the

information technology field. The cybersecurity (CS) industry increases every year both the employment chances and the requirements at staff working in this field and at education. Despite the improvement of cybersecurity techniques, criminals have developed sophisticated ways to disrupt systems and steal data particularly in organizations. The need to prepare people and organizations for cyberattacks is very important. According to Cisco's 2017 Annual Cybersecurity Report (https://engage2demand.cisco.com/en-us-annual-cybersecurity-report-2017), more than one-third of the organizations that experienced a cyber breach in 2016 reported a loss of customers, business opportunities, and revenue.

In January 2013, cybersecurity strategy has been prepared by the European Commission to take precautions against the cyberattacks, which are performed, continuously to companies, public offices, and other strategically important offices.

The **CS professionals** (CSPs), who are individuals, which maintain CS, have a special role in preventing cyberattacks. They have a responsibility with a moral dimension that should include protection against moral damage and of moral rights to ensure the correctness, reliability, availability, and security of all aspects of information and information systems. In the event of a threat to security systems, the decisions of CSPs are very important. In case of an emergency, effective communication is crucial. If IT systems fail, a quick communication with employees is necessary as well as to coordinate an effective response. Two surveys sponsored by Websense and conducted by Ponemon Institute shows the damage that the lack of communication between CSPs, upper management, and employees can do in terms of overall performance of the company and public image.

There is no more literature about communication in case of a cyberattack being a recent and difficult topic. The authors presented besides their opinions the practical experience of consultants in the field of cybersecurity. The scope of the chapter is to help organizations and employees particularly CSPs to develop communication plans and to integrate them in their CS plans. Discussions with organizations within projects showed this necessity. The results will be integrated in curriculum of cybersecurity from VET and HE students who prepare CS field in the countries of partners of the project cybersecurity described shortly in this chapter. The topic of communication in CS is missing in the existing curriculum. The chapter is organized as follows:

In Part II of this chapter, some notions of CS and CS strategy are presented as well as the problems, which organizations have when cyberattacks came, and the role of CSPs.

In Part III, issues for planning a CS communication strategy are given, based on the experience of practical experts in this domain.

Part IV is dedicated to the methods for an efficient communication and its integration into CS strategy of the company. The scope is not to develop theoretical methods but to give practical help to the organizations in case of cyberattack and students who prepare in CS.

An example of the current European project Cyber Security about CS with partners from education and industry from seven European countries is given in Part V. The project aims to develop measures to improve the training of future CSPs and CS knowledge of organizations in developing suitable CS strategies including communication as an important part.

The scope of this chapter is on the one hand to discuss with academics who work in the field of communication and CS and with students to find new scientific methods in this relative new domain based on some practical experience; on the other hand, the authors would like to help organizations and employees particularly CSPs to develop communication plans and to integrate them in their CS plans. The authors have experience in cloud computing and work in project about CS. It is planned that research and project results will be integrated in curriculum of cybersecurity from VET and HE students.

2. Cybersecurity

Information security (IS) and cybersecurity (CS) are very closely related terms and are used sometimes interchangeably. Richard Kissel gave the following definitions *(*https://www.quora.com/Whats-the-difference-between-cyber-security-and-information-security*)*: Information security—IS is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. It is a broader field that is concerned with information and the protection of information whether be it physical or computerized [1].

Cybersecurity—CS is defined as the ability to protect or defend the use of cyberspace from cyberattacks. It deals with protection of cyberspace and use of it against any sort of crime. Confusion about terms is because most of the information today is saved electronically and most of the cyberattacks are executed to disclose confidential information, harm the integrity of it, or deny access to authorized users [2, 3, 4].

The information threats that do not involve cyberspace come under information security but *not* under cybersecurity.

CS is a broad term, which comprises the protection of critical information infrastructure from hackers, as well as elements, which are considered critical information infrastructures, such as information networks of small- and medium-sized enterprises or personal computers. CS strategy aims at preventing malicious cybernetic incidents, which affect both critical information infrastructures and noncritical information infrastructures. This has a purpose to protect goods and resources of organizations from the organizational, human, financial, and technical point of view, so as to allow them to continue their mission. Cyberattacks are a constant threat to organizations. Organizations must ensure that no significant prejudice is caused to them consisting in reducing probabilities that a threat materializes, in limiting the tried prejudice or deficiency and ensuring that, following a security incident, the normal functioning can be restored in an acceptable time frame and at a fair cost. CS is a complex process involving the entire society.

Referring to the design of a cybersecurity process and strategy, first it is important to correctly identify the goods and the resources, which must be protected, so that the scope of the security necessary for an efficient protection is precisely determined. This requires a global approach of security that must be multidisciplinary and comprehensive.

The elaboration of a cybersecurity strategy is necessary first due to the society's dependence on cyberspace, so that that security, resilience, and trust in information and communication field represent a problem of national interest. Secondly, economic role and possibilities of information and communication technologies and the intention to maximize benefits and exploit their opportunities are great [5].

Cybernetic attacks, especially committed against critical information infrastructure, could represent a threat to the national security and so cybersecurity strategies are related to security and national defense strategies. A cybersecurity strategy is necessary for the protection of confidentiality, integrity, and availability of data and information systems, to enhance security, resilience, authenticity, and trust in the field of information and communication technology [6, 7].

3. Communication issues and a cybersecurity communication plan

Almost in all countries, not only cybersecurity (CS) techniques have improved in organizations, but also criminals improved their ways to disrupt systems and steal data of persons and particularly in organizations. The need that organizations and employees are prepared for cyberattacks is very important.

In order to avoid decisions that could negatively affect organization reputation, a comprehensive and strategic crisis communications plan is necessary [8].

A communication plan requires a collective work, with the right roadmap and tasks not too daunting. One way recommended by Josh Merkin is to inspire from an old journalism trick and use the 5Ws: who, what, when, where, and why *(*http://www.odwyerpr.com/story/public/9215/2017-08-09/communications-plan-for-cybersecurity-breaches.html*)*.

Why: The main objective of the plan is to prevent the loss of clients and revenue. Many firms do not have a crisis communications plan, i.e., for a data breach, often, due to less resources like time and money. Sometimes, the plan has no priority because it has no immediate or direct impact on business profit.

Who: First, it is important to establish who should be involved in developing the communication plan. A firm is managing partner/director, CEO, etc. A marketing or communication director is not probably the best decision; input should come from the firm's executive management team and IT (CS) department/team, legal counsel, administrative leadership, HR executives, and any communications agency and software vendors (if applicable). Strategic high-level input from senior leadership and department heads is necessary to ensure that all scenarios are covered *(*http://www.odwyerpr.com/story/public/9215/2017-08-09/communications-plan-for-cybersecurity-breaches.html*)*.

The second important aspect is in case of a cyberattack; immediate decisions with potentially significant impacts will need to be made. So, activities outlined in the plan should be implemented quickly.

Within the planning process, it is important to determine who the key decision-makers are, how will they work when the time comes, and who is taking specific tasks.

In the third aspects, stakeholders including employees, clients, and possibly media, professional associations, law enforcement, and even government entities should be contacted.

What: The plan should include basic key messages and categories of information the firm will need to share with its audiences in case of a cyberattack. Information should be shortly adapted according to the situation, but a basic content should be put together in advance, including statement for press, internal and external memos, a news release, and messaging for the firm's digital channels and website.

Questions should be answered, i.e., if the attack was the result of an employee or software error, how much data was compromised and by whom? Some such scenarios could be written in advance, and it is beneficial to have all the key decision-makers involved in the development process *(*http://www.odwyerpr.com/story/public/9215/2017-08-09/communications-plan-for-cybersecurity-breaches.html*).*

Where: It should be planned which channels the company has available to communicate its messages to its audiences, i.e., social media, email, phone trees, and directly to the person. For each case depending on situation and actions needed, it will be decided which channels are preferred over another or to use them all.

When: The point at which the plan will be implemented should be determined as well as how it will activate the response team should be activated. These issues should be specified in detail.

One particular role has the CSPs so it is expected that CSPs contribute to the development and application of a Telic communication plan for a worst-case scenario.

4. Issues to be considered by a communication/response

Multiple communication methods and channels can be affected in case of a cyberattack like own phone and voice mail system if they are VOIP-based, company phone system, company website (if it is hosted in-house), connections with customers, employees, the public, and the media *(www.continuitycentral.com/…communications…communications…/file).*

In case that the core network is compromised, every computer becomes a stand-alone machine with no access to company record. Employee contact information, vendor lists, or other key phone lists could be unreachable.

Besides a communication/response plan, some issues in connection with the IT infrastructure shall be regarded; affirm Nick Hawkins from EMEA.

Who needs to be included in an IT response plan?

- IT security responsible: should fix the issues and if the organization does not have a security team, employees must be assigned to be responsible for a response plan in case of a crisis.
- Incident team to coordinate the response, i.e., who should be contacted to define an escalation point.
- Legal counsel is necessary, i.e., if customer credit card details are stolen.

Who are the stakeholders?

Many stakeholders should be considered:

- C-Level executives
- Media relation department for messaging and informing customers about the incident and the press
- Customer services to prepare for incoming enquiries
- Employees to be kept up to date throughout the process to be prepared for calls from customers and the press
- Customers to be informed in real time about data breach

5. Cybersecurity internal communications best practices

In case of a cyberattack, the cooperative work and communication between the departments are very important in order to make sure that all security measures are aplite. The IT department should communicate with the chief information security officer (CISO)—who is a senior-level executive with duties including developing the company's information security architecture to best protect its systems and assets. In the following there are some true stories presented by Brad Berney (http://blog.securitymetrics.com/2015/03/internal-communication-for-it-security.html).

The head of the customer has to speak with the director of development when a customer found a security bug in their website (true story).

In case of an attack, the head has to action if the department is affected by lack of interdependent communication and customers whose data was stolen by a hacker due to such communication debacle.

In the following, some aspects will be presented to avoid communication problems within an organization. The first one refers to:

6. Cybersecurity communication culture

"It is possible that the poor communication culture from other companies gets thrown in the mix when employees are hired on from the outside. If an IT department hires three

new employees from three very different technology companies, each will have a different expectation of how their team should operate" said Brad Berney (http://blog.securitymetrics.com/2015/03/internal-communication-for-it-security.html).

It is possible that industry branches in companies with the similar industry profile used different terms to describe it, and so some tension could appear.

Bad communication could determine loosing of skill employees than being demotivated.

Right communication involves also internal meeting where the employees can talk to each other about the cybersecurity problems. Sometimes, in the internal meeting, other goals have a priority, or the CSPs have no idea which is the right strategy.

Demotivated employees doing bad communication are at risk to leave the company. Brad Berney shows some such problems in a demotivating environment: "Nobody even cares about security around here (…) nobody even likes me in this company (…) nobody even asked me for that security report last month." (http://blog.securitymetrics.com/2015/03/internal-communication-for-it-security.html).

Brad Berney discussed with some unhappy CSPs and other employees and the firm that salary does not always play a role to motivate them for work, but they consider company culture and team communication as keys to success and happiness. A better and sure work environment is a good point to be happy.

Missing communication and company's diminishing security, particularly cybersecurity, are important factors often.

Berney told that on an audit he conducted, a company supervisor and he were confused why logs from the IDS/IPS are not being checked. When he asked, the IT employee simply stated "The alerts from the IDS were noisy, so I turned them off."

In the following we present some methods to improve communication in CS:

6.1. Improving communication in cybersecurity strategies through training

"Don't let employee training fall to the side of data security" said David Page, Security Analyst, QSA (https://de.search.com/web?q=microsoft+onlineportal&qo=serpSearchBox&qsrc=1).

Cybersecurity does not refer only to locks, firewalls, and the latest technology to protect employee's sensitive data but also their vulnerability.

Employees make mistake and hackers take advantage to access to data. Many cyberattacks and destroying of data happen because of unintentional employee actions which make organization business vulnerable i.e., by clicking a phishing email that downloads malware and gives sensitive information to someone or using non-protective passwords.

One common problem is that a cybersecurity strategy and security policies in an organization are requiring the employees who are not aware of them, i.e., to be informed about contained policy about on what to do if a cyberattack is supposed. In this case the employees could make an error or waste time in reporting it to the right people, potentially causing more damage for the organization [9].

Another problem is **social engineering**, which is rapidly becoming a big threat against businesses of all types and sizes. In security, social engineering is a broad term used to describe an information technology attack that relies heavily on human interaction and often involves tricking other people to break normal security procedures [10].

Social engineering refers to the techniques used to exploit human vulnerability to bypass security systems to gather information. Social engineering attacks imply interaction with other individuals, indicating also psychological and ethical aspects. About social engineering (SE), there are many differing opinions [11, 12].

Social engineering:

- Is known as human hacking
- Refers to the use of human error or weakness to gain access to any system despite the layers of defensive security controls that have been implemented via software or hardware
- Is the art of tricking employees and consumers into disclosing their credentials and then using them to gain access to networks or accounts

The problem with social engineering is that it targets employees specifically. If employees are not trained to recognize social engineering tactics, they could be vulnerable to a data breach. A moral of urgency should be trained in employees within CS strategies.

It is important to train employees on basic CS best practices, because problems like email phishing scans and social engineering can affect each employee in the organization. Employees with access to sensitive data should learn how to protect it.

Some topics for training could be:

(https://de.search.com/web?q=microsoft+onlineportal&qo=serpSearchBox&qsrc=1)

- Technology use
- Password management
- Data handling procedures
- Incident response plans
- Data security best practices
- Social engineering techniques

Regarding communication and meetings, it is not enough to hold yearly meetings because employees have to be aware to prioritize cybersecurity aspects in their daily activities. Some tips given by David Page are as follows:

(https://de.search.com/web?q=microsoft+onlineportal&qo=serpSearchBox&qsrc=1)

- Set monthly training meetings: focus each month on a different aspect of cybersecurity, such as passwords, social engineering, e-mail phishing, etc.

- Give frequent reminders: these could be sent out in an email or newsletter that includes tips for employees.
- Train employees on new policies ASAP: also, newly hired employees should be trained on policies as quickly as possible.
- Make training materials easily available: intranet sites are a great way to provide access to training and policy information
- Create incentives: reward employees for being proactive.

Through an active communication, all employees should understand that they have an important role in keeping business's data secure. Training of employees should be a top priority in each CS strategy.

6.2. Internal communication as a permanent task

Communication, also within CS, is a complex problem, and not each step can be defined before, but some aspects could be considered:

1. Department directors and CEOs should recognize a poor internal communication about CS.
2. Define training with some topics like:
3. The problem itself
4. How the problem is damaging company, employees, and customers
5. Clearly define process how communication should happen
6. What to do if feelings have been hurt
7. How complaints can be brought up
8. Hold interdepartmental "need" meetings focused on discussing what each department needs from the other, including timelines, milestones, and goals.
9. Address hurt feelings—Everyone has their own view on how certain issues should be handled.
10. Tell employees why—Sometimes employees just want to know "why" of things. Why are we buying this product? Why did not we buy the product I researched and suggested? Why did not we implement this solution? Why? When employees do not get answers to their "why's," they decide to make matters into their own hands. And, that's when security and process problems start. Remember, employees have the keys to the kingdom. You rarely hold anything other than the check book. Answer those employee questions as quickly and succinctly as possible.
11. Start fun communication exercises.

7. The role of CSPs

The **CS professionals** (CSPs) have a special role in preventing cyberattacks. In case of a threat to security systems, the decisions of information security professionals are very important. In case of an emergency, effective communication is crucial. If IT systems fail, a quick communication with employees is necessary as well as to coordinate an effective response. The survey, sponsored by Websense and conducted by Ponemon Institute, shows the damage that the lack of communication between CSPs and upper management can do in terms of overall performance of the company and public image (https://www.entrepreneur.com/article/235318).

Many CSPs believe that their organizations' security controls do not provide adequate protection against advanced cyberattacks, according to more than 5000 IT professionals from 15 countries including the USA. They affirm that executives do not put effective security controls in place and do not evaluate a data breach with financial loss. This is also the conclusion of a study conducted, also by the Ponemon Institute (https://www.ponemon.org/data-security), that the majority of CSPs professionals fail to communicate security risks effectively to upper management.

These reports show that along with managing and developing response plans against emerging security threats, cybersecurity professionals also need to inform upper management about the seriousness of security threats and convincing them to allocate adequate resources to protect against data breaches.

According to a study sponsored by HP Enterprise Security Products (http://www8.hp.com/us/en/hp-news/press-release.html?id=1571359), 30% of the cost of a data breach was due to business disruption or lost productivity. The study found that companies that invest in adequate resources develop communication plans, define a high-level security leader, and employ CSPs who have costs lower than companies that have not implemented these practices.

Some ideas are how the communication between CSPs and executives can be seen in the 2014 Websense-Ponemon report (https://de.search.com/web?q=microsoftonlineportal+login&qo=serpSearchBox&qsrc=1). The report found several key reasons why communication between executives and CSPs is so ineffective.

Security discussions occur at a low level and are rarely brought to executive's attention. Sometimes, CSPs warnings are too technical in nature and do not translate the threats into easy-to-understand language. Criticisms of existing practices are often filtered out before being presented to management.

Some helpful aspects:

- Ensure that cross-functional teams can communicate effectively and that awareness of these risks spread. People in engineering, sales, and marketing departments also need to be aware of security risks.
- CSPs must turn technical details of security risks into information that can be easily understood by upper management.

- CSPs should address these issues directly with the CEO and executive team broughing directly their attention and not be filtered out by intermediate players.
- As more data moves into the cloud and across other devices, companies face a greater risk of losing sensitive information to attackers or unauthorized users. According to Lobley (https://www.linkedin.com/in/colinlobley/), too many businesses fail to set quantitative parameters for risk (risk appetite) instead, to align the language.

In a real-world example, Lobley worked with a client outside the tech sector. When he asked frontline staff how the business was impacted from an incident that caused the IT system to go offline for 2 hours, the response was simply "not a lot." Upon talking to management, however, it soon became apparent that the company had exposed itself to significant risk.

7.1. Cloud computing offers many opportunities for communication platforms

An IT-oriented communication platform can be used for the following:

- Employee information: pushing information to employees about the company status and messaging
- Conference bridges: using Toll-free conference bridges for employee, vendor, senior management, board of directors, and other key stakeholder phone calls
- Stakeholder groups: using predefined groups that had been created for key stakeholders to push information via phone, text, or email

Cloud computing "is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NIST definition). Cloud computing enables companies to use resources as a utility rather than having to build and maintain computing infrastructures in-house [13–15].

Most organizations trust on internal email to communicate in the event of a crisis, even though a cyberattack might impact the email network. In doing so, organizations are exacerbating the problem and potentially providing hackers with critical company information.

By having a system that operates entirely independent of an internal communications network, organizations can ensure that the bilateral lines of communication between management and staff remain open—even in the event of a cyberattack or IT outage that may compromise an internal network or a rush of calls which may overload a telecommunication network.

The benefits of selecting to use a cloud-based platform in the event of crisis are twofold. Firstly, they allow for location-mapping functions to be easily installed on employee's smartphones, meaning that business' can receive regular alerts and updates on their employee's last known locations. This wealth of data is then readily accessible should a crisis develops, ensuring that management is not only able to locate all of their staff but are also able to coordinate a more

effective response, prioritizing and deploying resources to help those employees who are deemed to be at risk. Without this location-mapping function, businesses are being forced to rely solely on traditional routes of communication to find out if their staff are in.

Organizations with crisis management plans that include using a cloud-based location-mapping device are instantly able to know that Employee A is out of the impact zone and safe, while Employee B is at the epicenter of the crisis and likely to be in danger, making communication with them the top priority.

The second advantage to implementing secure, cloud-based communication platforms into a business' emergency communications plan is that it enables users to quickly and reliably send secure messages to all members of staff, individual employees, and specific target groups of people. These crisis notifications are sent out through multiple contact paths which include SMS messaging, emails, VOIP calls, voice-to-text alerts, app notifications, and many more. In fact, with cloud-based software installed on an employee's smartphone, there are more than 100 different contact paths that management can use to communicate and send secure messages to their workforce, wherever they may be in the world. This is a crucial area where cloud-based platforms have an advantage over other forms of crisis communication tools; unlike the SMS blasters of the past, emergency notifications are not only sent out across all available channels and contact paths but also continue to be sent out until the recipient acknowledges them.

8. The case of the European project cyber security

The European project Cyber Security (www.cybersecurityplus.org) with partners from education, research, and industry/business supports the European Cybersecurity Strategy.

The seven partner countries of the project are preoccupied to develop a strong strategy which is the sum of all national and international measures taken to protect the availability of information and communications technology and the integrity, authenticity, and confidentiality of data in cyberspace [16].

One difficult aspect is the preparation of future CSPs. Referring to cybersecurity education particularly in VET, the project partner countries like Germany do not have any body responsible for educational and professional training programs for raising awareness with the general public, promoting CS courses and communication in CS. There are no CS courses in vocational schools; this is a gap in the present, nor is a cybersecurity discipline included in the curricula of professional courses. So, one of the objectives of Erasmus + project Cybersecurity is to disseminate cybersecurity issues in formal and nonformal education and organizations, and fostering the development and skills of teachers, trainers, and CSPs will contribute to create a CS culture and communication strategies in organizations.

Through short research in European practices and education, development of a curriculum in cybersecurity education including communication strategies; organizing seminars and conferences in VET, HE, and other organizations; and development and distribution of a book about cybersecurity, including a chapter about communication the project will contribute in

http://dx.doi.org/10.5772/intechopen.75952

improving knowledge and skills of people in avoiding cyberattacks. The cooperation with the industry assures a practical character of the project outcomes [16, 17].

A workshop with academics, students, and representatives of the organization having the main topics (communication within cyberattacks) will be held this year in Gelsenkirchen, Germany.

A platform for communication and training will be also developed, and cloud computing will be used for a pilot environment.

9. Conclusions

The CS environment is rapidly changing. Cyberattacks are on the rise by using advanced technological means and are interesting because businesses use more technology. There are needs for rapid shifts in business strategies to adapt to other changes due to CS risks which change in scope and potential impact quickly. Organizations need to have the tools prepared to be able to communicate and recover quickly in the event of a crisis. The severity of a cyberattack and its impact depends on these factors.

Consequently, particularly CSPs must be prepared to communicate effectively in this challenging environment, using the best communication means and data for the right audience at the right time. The consequences of ineffective communication, resulting in misunderstanding security risks, can be catastrophic. Having a plan and understanding the business objectives, the stakeholders, their needs, and the risks themselves will help the CSPs to provide a clear, relevant message. It is important to ensure that communication is addressed to the right stakeholder group and then to verify that it has been understood.

The severity of a cyberattack and its impact depends on these factors. Critical communication platforms, a communication culture, corresponding training support in case of a breach to limit downtime and damage are important issues for further research of the authors. Students could learn how to develop an efficient, well-practiced incident response plan which can minimize cyberattacks damages.

Acknowledgements

The paper describes objectives and outputs of the European Erasmus+ project Cybersecurity.

Author details

Ileana Hamburg* and Kira Rosa Grosch

*Address all correspondence to: hamburg@iat.eu

Institute of Work and Technology, WH Gelsenkirchen, Gelsenkirchen, Germany

References

[1] Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Elsevier; 2011

[2] Anonymous. FBI. Cyber-Attacks Surpassing Terrorism as Major Domestic Threat. https://www.rt.com/usa/fbi-cyber-attack-threat-739/

[3] Rattray G. Strategic Warfare in Cyberspace. Cambridge MA: MIT Press; 2001. DOI: 10.1006/tpbi.2001.1531

[4] Singer PW, Friedman A. Cybersecurity and Cyberwar. Oxford; Oxford University Press; 2014. DOI: 10.1111/cob.12074

[5] Engebretson P. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy: Elsevier; 2011. DOI: 10.1016/j.phrs.2011.06.024

[6] Himanen P. The Hacker Ethic: A Radical Approach to the Philosophy of Business. New York: Random House; 2001. DOI: 10.1038/414933a

[7] Laurie GT. Genetic Privacy: A Challenge to Medico-Legal Norms. Cambridge UK: Cambridge University Press; 2002

[8] Davies J. Benefits of Cloud Communications in a Crisis". 2016. http://www.business-cloudnews.com/2016/06/09/benefits-of-cloud-communications-in-a-crisis-situation/

[9] Gulati R. The Threat of Social Engineering and Your Defense Against It. SANS Reading Room; 2003

[10] Maan PS, Sharma M. Social engineering: A partial technical attack. International Journal of Computer Science Issues. 2012;**9**(2):557-559

[11] Bisson D. 5 Social engineering attacks to watch out for. The state of security. security/security-awareness/5-social-engineering-attacks-to-watch-out-for/. DOI: 10.4158/EP-2018-0101

[12] Chitrey A, Singh D, Singh VA. Comprehensive study of social engineering based attacks in India to develop a conceptual model. International Journal of Information and Network Security. 2012;**2**(1):pp. 45-53

[13] Antonopoulos N, Lee G, editors. Cloud Computing. Principles, Systems and Applications. Springer International Publishing AG; 2017

[14] Assante D, Castro M, Hamburg I, Martin S. The use of cloud computing in SMEs. In: Procedia computer science 83, special issue: The 7th international conference on ambient systems, Networks and Technologies (ANT 2016) / The 6th International Conference on Sustainable Energy Information Technology (SEIT-2016) / Affiliated Workshops. 2016. pp. 1207-1212. DOI: 10.1007/s12350-017-0924-x

[15] Hamburg I. Improving e-learning in SMEs through cloud computing and scenarios. In: Gradinarova B, editor. E-Learning - Instructional Design, Organizational Strategy and Management. Rijeka: InTech; 2015. pp. 481-498

[16] Hamburg I, Grosch KR. Ethical aspects in cyber security. In: Archives of Business Research 5, no. 10, 2017. p. 199-206 PD, DOI: 10.1016/j.jaut.2017.12.006

[17] Warren MJ, Hutchinson W. Deception: A Tool and Curse for Security Management. IFIP/SEC 2001, 16th International Conference on Information Security. Paris, France, 2001. DOI: 10.1007/s00127-018-1529-7

IntechOpen