CYBER SECURITY – BUILDING A SUSTAINABLE PROTECTION

KAFOL, C. & BREGAR, A.

Abstract: *Extensive cyber usage and applications have created vulnerability to attacks from anywhere in the world. It is therefore necessary to devise protection against cyberattacks. The purpose of this article is to propose methodology that will lead organisations through creating high level and sustainable protection against cyberattacks. Authors have addressed the question whether it is possible to create single methodology covering as many aspects as necessary to protect organisations assets against known and possibly developing types of cyberattacks. Following the research authors are proposing 6 step methodology which provides organisation with holistic approach to achieve desired level of cyber security. Methodology has steps: simulate, analyse, plan, develop, build and operate. Feedback loops and interconnecting relations between steps are proposed, which suggests that the methodology requires constant and intensive development in order to build up necessary defence level. The very essence of proposed approach suggests continuous verification of defence strategy and tactics, building security operation centre that is self-sustainable and resources around it to analyse big data content that is building up on daily basis. This approach to cyber security is devised in a way to build a sustainable protection against attacks.*

Key words: *cyber security, methodology, attacks, vulnerability, sustainability*

Authors´ data: Dr Sc **Kafol**, C[iril]; Dr Sc **Bregar**, A[ndrej], Informatika d.d., Vetrinjska ulica 2, 2000 Maribor, Slovenia, ciril.kafol@informatika.si

This Publication has to be referred as: Kafol, C[iril] & Bregar, A[ndrej] (2017). Cyber Security – Building a Sustainable Protection, Chapter 07 in DAAAM International Scientific Book 2017, pp.081-090, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-12-9, ISSN 1726-9687, Vienna, Austria
DOI: 10.2507/daaam.scibook.2017.07

1. Introduction

Cyber-dimension of the world in which we live is essential for the normal functioning of modern society as well as for its further development. It is therefore not surprising that there are intensive activities in cyberspace, which brings a profit for one, while others lose. Modern society has new challenges such as the need to protect critical points of cyber vulnerabilities (Orlic&Kafol, 2017).

The number and intensity of cyber attacks is rising at incredible speed. Only recently two major attacks have been launched on large scale level (named Petya and Wannacry) and were publicized heavily. The fact that cyber attacks were reported worldwide and given names shows that this kind of activity is gaining in influence and is expected to be frequent.

The statistics of the attacks shows that most attacked are military, energy, financial and critical infrastructure installations. There is a need to develop common approach and methodology which will set the systematic path to building sustainable protection against cyber attacks.

The phenomena of cyber attack is not new and some government bodies have set early roadmaps to protect important infrastructure. Ministry of Energy in USA have adopted »Roadmap to Secure Control Systems in the Energy Sector« in 2006 (Eisnehauer et al, 2006) which is one of the key points of cyber protection modernisation in energy sector in USA.

New business paradigm arises while the need for constant IT support rises significantly and companies must adopt to it which makes them more and more vulnerable to the cyber attacks. As the pace of business accelerates steadily, the company realizes that it is not enough just to analyze the data but the activities that are being imposed on the basis of the results of the data analysis must also be operationalized as soon as possible (Suman&Pogarcic, 2016).

The purpose of this article is to propose methodology that will lead organisations through creating high level and sustainable protection against cyberattacks. Authors have addressed the question whether it is possible to create single methodology covering as many aspects as necessary to protect organisations assets against known and possibly developing types of cyberattacks. Following the research authors will propose methodology that will lead the organisation through the process of creating sustainable and hollistic protection against cyber attacks.

2. Observation and description of cyberattack phenomena

Wikipedia defines cyberattack as any type of offensive manoeuvre employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labelled as either a cyber campaign, cyberwarfare or cyberterrorism in different context. Cyberattacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations. (Wikipedia, 2017)

The number and impact of cyberattacks activity are well illustrated by data from WatchGuard which blocked in Q2 2017 over 2,902,984 network attacks and 16,403,723 malware variants (Cyber attacks, 2017) (Security Report, 2017).

Networks are constantly exposed to security threats. Security analysts and security operation centers (SOC) have the responsibility to identfy cyber attacks and implement appropriate solutions. Although these tasks are repetative, they are usually performed manually. It is of great benefit to automate defense tasks by designing effective technologies for security operations that are taken up by the analysts and security operation centers, and thus improve their work efficiency (Sundaramurthy et al., 2016; Kansas State University, 2013). A solid basis for such automation are anthropology studies, which reveal that communication between IT security professionals and users is rarely effective, and that security technology is only as good as the people who use it (Squires &Shade, 2015).

Wang and Lu (2003) argue that cyber security is one of key topics in smart grids, which integrate high-speed communication technologies into millions of power equipments to establish a dynamic and interactive infrastructure with new energy management capabilities, such as advanced metering infrastructure and demand response. Increased interconnection, integration and dependence on information networking expose smart grids to vulnerabilities associated with communications and networking systems. Cyber attacks may lead to a variety of severe consequences, from customer information leakage to unreliable system operations and failures that can potentially result in the destruction of infrastructures and disasters for both utilities and consumers (Yan et al., 2012). The objective of providing security in cyber grids is to protect the availability, integrity, and confidentiality of information. Three types of cyber attacks exist in relation to these attributes: (1.) attacks targeting availability, also called denial-of-service (DoS) attacks, attempt to delay, block or corrupt communication, (2.) attacks targeting integrity aim at deliberately and illegally modifying or disrupting data exchange, and (3.) attacks targeting confidentiality intend to acquire unauthorized information from network resources.

According to Wang and Lu (2003), the standard design for cyber security comprises of various countermeasures. These include secure protocols and standards for system communication, secure data aggregation protocols, and secure network architectures. Cryptographic approaches and algorithms are also widely applied, and are a well researched topic (Wikipedia, 2017). They are based on encryption, authentication, and key management (KPI).

Several other studies also deal with cyber security in smart grids and electric power grids (Liu et al., 2012). Sridhar et al. (2011) highlight the significance of cyber infrastructure security in conjunction with power application security to prevent, mitigate, and tolerate cyber attacks. Risk is evaluated based on the security of both the physical power applications and controls required to support the smart grid, and the supporting cyber infrastructure for communication and computations that must be protected from cyber attacks.

Extensive studies have been performed in the field but there is no methodology that would address all stakeholders and deal with the matter hollisticly. Hence authors propose methodology that combines the approach.

3. Developing a methodology and approach

Proper price efficient methodology for reasonable protection against cyber attach is difficult to define. Approach has been developed by USA National Bodies, methodology is however difficult to define and especially to define cost benefit criteria. There are several methodologies which try to define price efficient ways to reach cyber security goals. Organizations in both the private and public sectors have struggled to determine the appropriate investments to make for protecting their critical intellectual property (Carin, Cybenko, Hughes, 2008). However, multidisciplinary holistic approach is necessary to address the problem due to its perplexion and complexity.

Authors will suggest methodology through which the organisation may effectively reach the reasonable level of protection against cyber attacks. Lapiedra suggests that the process shall encompass 3 elements: prevention, detection and response which protects 3 unique attributes of information which are: confidentiality, integrity and availability (Lapiedra, 2002). Methodology has been developed for

Utilities and is called preemptive. The key points are: A. Taxonomy – report: classifying the utility networks, taking into account type and communication technology, sensibility to Cyber threats B. Modelling – software: models and virtual environment for simulating and gathering data on cyberattacks C. Software detection (network, host and process based) and event correlation tools - software: prevention and detection tools to improves security on SCADA utility networks. D. Cyber Defence Methodology Framework – guidelines: Risk and Vulnerability Assessment methods and standard policies, procedures and guidelines to prevent cyberattacks. E. Privacy and Data Protection – guidelines: Legal and Ethical aspects and impact of Preemptive (Valentini& Sinibaldi, 2016).

Methodology approaches vary from business to business. Based on a deductive approach we propose the methodology that consists of 6 steps:

1. Simulate
2. Analyse
3. Plan
4. Develop
5. Build
6. Operate

First two phases, simulate and analyse, are starting phases though which we are beginning the process of creating the sustainable protection. Planning phase is in between starting phases and implementation phases and is very important for designing and planning technical and economic criteria to build proper level of protection. Last three phases, develop, build and operate, are so called implementation phases and consist of element neccessary to build resorces and assets that will protect the organisation agains cyberattacks. There are several feedback loops, in the starting phase, we may return from analitic phase to simulation phase to test the hypothesis. In the implementation pases we shall constantly be returning from operational to developing phase in a circular manner in order to constantly upgrade the defenses against ever changing hostile environment. And last, there is a neccessity to constantly return from implementation to starting phases is order to evaluate whether strategy and tactics of the activity is still up-to-date and sustainable.

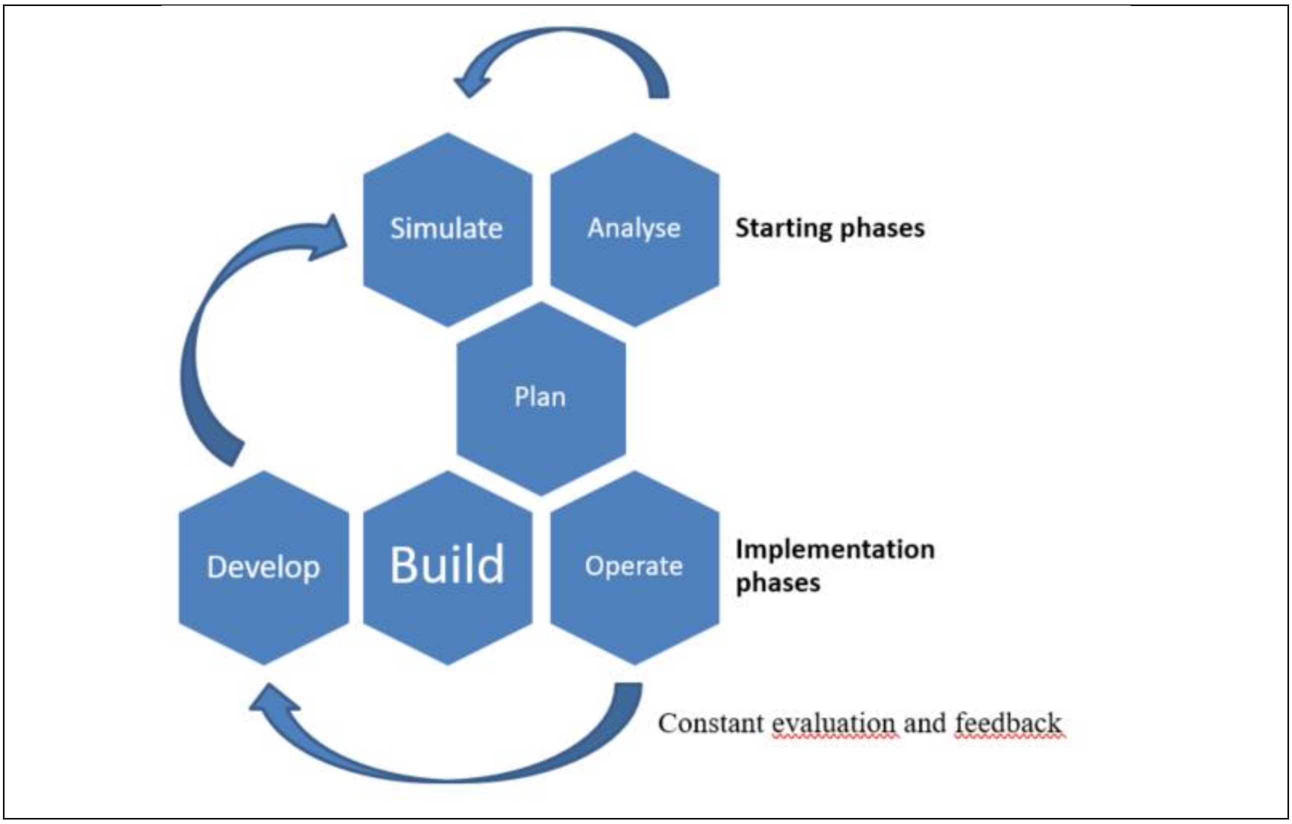

Fig. 1. 6 step methodology

3.1 Simulate

Conducting cyberattack experiments on computer systems that contain critical data is undesirable (Arena Simulation Software, 2017), especially in some important fields, such as smart grids. It is very expensive to (re)design, test and install a smart grid, because the power system in operation must always be available, so taking it down in order to perform tests is not possible (Baumeister, 2010). Therefore, two alternatives can be used. One alternative consists of setting up a physical computer network absent of any critical data, performing cyberattacks on the network, and collecting data from intrusion detection systems. The second alternative is to generate synthetic data through the use of simulation. A simulation model can then be used to analyse security risks and other network aspects.

Simulation of attack is powerful tool used in testing organisations vulnerability and exposure to cyberattacks.

Simulation is best performed by third party organisation, unknown to key players within the target organisation, in order to test actual organisational vulnerability to cyberattacks.

In the proposed methodology, the simulation phase incorporates four subsequent sub-steps:

1. A model of the system or network topology is built. Key objects include computers, technical devices (such as electricity metering devices, electricity consumers, etc.), software applications, data sources, connectors, subnets, subsystems, and organizational units.
2. Probabilistic variables are defined for various events that pertain to potential cyberattacks on various nodes, connectors, and parts of the modelled system/network. Probabilities are estimated and assigned for different variables.
3. Discrete event simulation is performed with regard to the network model and probabilistic variables that refer to cyberattacks.
4. Simulation results are aggregated to statistically expose vulnerability of individual network objects, as well as groups of interconnected and functionally dependent objects.

3.2 Analyse

In most networks, the analysis of simulation results is a challenge because the observed system may be large and complex. Many components are thus connected, and changes in one component may cause unforeseen effects on other components in the system (Baumeister, 2010). A systematic and holistic approach to analysis is hence needed.

At first, each object in the modelled topology is analysed in isolation. If it is subjected to high security risks, this is an indicator that appropriate security measures to avoid and reduce risks must be taken. Partial risks of an individual object are estimated based on the frequency of simulated cyberattacks on this object.

However, it is even more crucial to assess the severity of risks. If an object in the modelled network is interconnected with many other objects which are also subjected to high frequencies of simulated cyberattacks, then the risk severity of the observed object is critical. Groups and subnets of connected objects must hence be analysed to expose dependencies and strengths of correlations. In such cases, the adopted and implemented risk aversion measures must result in modifications and improvements of the network topology, which may lead to the iterative repetition of the simulation step.

3.3 Plan

This phase is critical when designing wanted security level. Feasibility study shall be conducted to assess the approach, outline the findings from previous two phases and define economics of the action. It is important to define and list the activities that will lead us from AS IS situation to TO BE stage. Planning shall include all stakeholders and identified risks shall be dealt with mitigation strategies. Clear document with economics and at least three scenarios shall be prepared and discussed with decision makers. Economical and technical efficiency of scenarios shall be assessed by applying a multi-criteria model supporting incomplete or fuzzy information, and various preference structures and styles in a group decision making setting.

Plan phase shall thoroughly and systematically address three key elements of the cyber security process. Sustainable prevention strategies will be defined based on identified and analysed risks. Detection mechanisms shall be designed to deal with known and potentially unknown risks, where methods of machine learning and artificial intelligence will be adopted to discover the latter. Efficient response strategies and mechanisms shall also be specified to overcome detected security threats, attacks, and issues.

3.4 Develop

Developing phase is first step of implementation process. Developing process shall be performed in all areas: human resources, hardware components and software components. Defining of the key elements for security operation center is important part of this phase, as well as depth and way of operation. Organisational impacts shall be assessed and addressed, organisational changes envisaged and communicated. The organisation must embrace the process in this phase (Kansas state university, 2013).

3.5 Build

Building phase is the second part of implementation process and consists of purchasing and installing elements of Security Operation Center. A security operations center (SOC) is a centralized unit that deals with security issues on an organizational and technical level. A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology. Typically, a SOC is equipped for access monitoring, and controlling of lighting, alarms, and vehicle barriers (Wikipedia,2017). The starting points is building SIEM (Security information and event management) platform. Security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware. Final stage of this phase is pre-production action and go-live strategy.

3.6 Operate

Operation phase starts with commissioning of the system and putting the SOC into production. Not only the operational issues must be addressed, organisational and cultural issues shall be addressed as well. Efforts to improve the efficiency of security operation centers (SOCs) have emphasized building tools for analysts or understanding the human and organizational factors involved (Sathya et al, 2016). This may require more effort and require longer transition period. Trial operation must outline potential gaps and security threats. Operation phase shall constantly evaluate performance and feedback to development phase established to bridge potential gaps. It is important to stress that last three phases shall constantly be repeated to deal with changes in cyber environment and maintain and improve cyber security level. If the feedback and response is faster than the environment security level rises and if it is slower it is declining. This process is never ended and requires constant care.

4. Conclusion

The objective of this article was to define the methodology to achieve a sustainable level of cyber security. Although several related studies and approaches exist that have dealt with cyber security issues in the past, they have all considered only partial and limited aspects of the problematics. In contrast, the main scientific and practical contribution of our methodology is in its holistic approach, which addresses all aspects, characteristics and parameters of cyber security in complex technical and information systems, and supports various activities, constructs and concepts of the complete cyber security life cycle. It introduces appropriate procedures and measures for all consecutive and iterative phases of the cyber security life cycle, which starts with simulation and analysis, and ends with implementation and operation. It focuses on all key security parameters, such as availability, integrity and confidentiality of information. It also clearly defines the role and importance of the security operations center in the process of building and implementing a sustainable and cost effective cyber security.

The implications of using the proposed methodology may be that the protection system and process is not well build, all stakeholders are not incorporated and that the overall protection system is more vulnerable to cyberattacks than it would be if the methodology was dully followed. Positive consequences of using methodology following continuous feedback and building of the defences is higher protection against cyberattacks and resistibility of organisation's assets. The negative consequences are possibly higher costs and higher use of assets than necessary, if the organization is not attacked or is not interesting for cyberattackers. However, this is less likely event, as cyberattackers do not choose only large and important organizations but also attack physical persons and smaller organisations demanding low ransom from large number of individuals or organisations.

We believe that it is of essential importance for each complex technical or business information system to adopt and implement the proposed methodology in order to sistematicaly, considerably and effectively reduce cyberattack risks. If such systems do not address cyber security issues, or if they apply a partial approach to implementing cyber security measures, they are exposed to high risks of cyberattacks, which may consequently result in high financial losses and infrastructure failures. We are hence convinced that the introduced methodology has significant potentials and implications, both in research and practice. It thoroughly and systematically solves the problem of achieving a sustainable and cost-effective protection against cyberattacks and builds sustainability in approach.

The conducted research and its presentation in the article consisted of three phases. In the introduction phase, authors outlined the importance of raised security awareness due to the ever-changing cyber environment. It was followed by observation and description of cyberattack phenomena, where basic definitions and occurences were described. The last phase dealt with the development of a holistic methodology and approach, where a 6-step methodology was proposed to address a sustainable protection against cyberattacks.

Although the methodology is fully applicable and operational in its current state, there are several possibilities for its extensions and developments. Further study will lead into detailing methodology steps and actions as well as upgrading the methodology to address ever changing phenomena. The methodology will also be fitted and adjusted to various types of complex systems, such as smart grids in the energy sector.

The limitation of the study is that the methodology has not been tested and experimentally evaluated with full scope yet. An installation of the model shall therefore be performed and analyzed within the scope of future work. Organisation will build a full-scale model with all necessary elements, build-up resources and infrastructure in order to test and assess the methodology approach. A case based study and a simulation study are planned for the formal assessment of efficiency.

5. References

Arena Simulation Software (2017). Cyber Security Simulation. Available from: https://www.arenasimulation.com/industry-solutions/resource/cyber-security-simulation. Accessed on: 2017-09-03

Baumeister,T. (2010). Literature Review on Smart Grid Cyber Security. Department of Information and Computer Sciences, University of Hawaii. Available from: https://link.springer.com/chapter/10.1007/978-3-319-03964-0_8, Accessed on: 2017-09-29

Carin M., Cybenko H. (2008): Cybersecurity Strategies: The QuERIES Methodology, Available from: http://www.dartmouth.edu/~gvc/IEEE_Queries.pdf, Accessed on: 2017-09-13

Cyber attacks 2017. Report (2017) , Available from:http://it.tmcnet.com/news/2017/09/28/8620703.htm, Accessed on: 2017-09-30

Eisnehauer J., Paget D., Mark E., O'Brien M. (2006). Roadmap to Secure Control Systems in the Energy Sector«, Available from: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf, Accessed on: 2017-08-20

Lapiedra J. (2000). The Information Security Process. NGIAC © SANS Institute 2000 – 2002, Available from: https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197, Accessed on: 2017-09-30

Lebanidze E. (2011). NRECA National Rural Electric Cooperative Association: Guide to Developing a Cyber Security and Risk Mitigation Plan, 2011, Available from: https://www.smartgrid.gov/files/CyberSecurityGuideforanElectricCooperativeV11-21.pdf, Accessed on: 2017-09_30

Liu J., Yang X., Shuhui L., Wei L., C. L. Chen P. (2012). Cyber Security and Privacy Issues in Smart Grids. IEEE Communications Surveys & Tutorials. 14 (4) 981–997.

Kansas State University (2013). Cybersecurity algorithms, techniques being developed through anthropology methods. ScienceDaily 7 November 2013. Available from: www.sciencedaily.com/releases/2013/11/131107103406.htm. Accessed on: 2017-09-30

Orlic D., Kafol C. (2017) : Kibernetska varnost energetskega sektorja v Sloveniji , Availablefrom:http://www.cigrecired.si/staticAdminMgr.php?action=read&menu=potrjeni_referati_2017, Accessed on: 2017-09-10

Sathya C.S., McHugh J., Ou X., Wesch M., Bardas A., Rajagopalan S.R. (2016). Turning contradictions into innovations or: How we learned to stop whining and improve security operations. Symposium On Usable Privacy and Security (SOUPS 2016), Denver, CO, USA, pp. 237–251. Accessed on: 2017-09-13

Sridhar S., Hahn A., Govindarasu M. (2011). Cyber–Physical System Security for the Electric Power Grid. Proceedings of the IEEE. 100 (1) 210–224.

Security Report Q2 (2017). Available from: https://www.watchguard.com/wgrd-resource-center/security-report, Accessed on: 2017-09-30

Squires S., Shade M. (2015). People, the Weak Link in Cyber-security: Can Ethnography Bridge the Gap? EPIC, Ethnographic Praxis in Industry Conference. 2015 (1) 47–57. Available from: https://www.epicpeople.org/people-the-weak-link-in-cyber-security-can-ethnography-bridge-the-gap/ Accesed on: 2017-09-30

Suman, S. & Pogarcic, I. (2016). Development of ERP and Other Large Business Systems in the Context of New Trends and Technologies, Proceedings of the 27th DAAAM International Symposium, pp.0319-0327, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-90273408-2, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/27th.daaam.proceedings.047 Available from: http://daaam.info/?page_id=3684, Accessed on: 2017-09-30

Ye Y., Yi Q., Hamid S., Tipper D. (2012). A Survey on Cyber Security for Smart Grid Communications. IEEE Communications Surveys & Tutorials. 14 (4) 998–1010.

Valentini A. , Sinibaldi G. (2016). PREEMPTIVE PREventivE Methodology and Tools to protect utilitIEs. Fast abstracts at International Conference on Computer Safety, Reliability, and Security (SAFECOMP), Sep 2016, Trondheim, Norway. Available from: https://www.ntnu.edu/safecomp2016. <hal-01370266>, Accessed on: 2017-09-30

Wang W., Lu Z. (2013). Cyber security in the Smart Grid: Survey and challenges. Computer Networks. 57 (5) 1344–1371. Available from: https://research.ece.ncsu.edu/netwis/papers/12WL-COMNET.pdf, Accessed on: 2017-09-30

Wikipedia (2017). Cryptography. Available from: https://en.wikipedia.org/wiki/Cryptography. Accessed on: 2017-09-30

Wikipedia (2017). Cyberattack, 2017 Available from: https://en.wikipedia.org/wiki/Cyberattack. Accessed on: 2017-09-30

Wikipedia (2017). Security Operations Center. Available from: https://en.wikipedia.org/wiki/Cyberattack. Accessed on: 2017-09-30