Study of Baseline Cyber Security for Various Application Domains

Mudit Chaturvedi¹, Shilpa Sharma² and Gulrej Ahmed¹

¹Department of Computer & Communication Engineering, Manipal University Jaipur, Jaipur-Ajmer Express Highway, Dehni Kalan, Near GVK Toll Plaza, Jaipur, Rajasthan 303007 India
²Department of Computer Applications, Manipal University Jaipur, Jaipur-Ajmer Express Highway, Dehni Kalan, Near GVK Toll Plaza, Jaipur, Rajasthan 303007 India

E-mail: shilpa_1819@yahoo.com

Abstract. In today’s technical life, the means of production and creation, process, storage and exchange of information and data, rather than in paper-based methods, as an alternative to electronic data and electronic means of communication. That means all information / data is done on the paper as not a written document, but in the form of digital and electronic data. A special type of computer-based system is used in preparing, receiving, processing, transmitting or storing this electronic data / information and the main feature of this computer-based system is that there is a rapid data processing by logical, arithmetic, membrane resources by the systems of electronic, magnetic or optical waves by instruction or communication, work of input, product, investment, processing or storage is done. It is very important for the common man to know about the basic security of information / data in every domain of life. This paper analyses the technical changes and cyber risks arising in various fields, as well as a detailed study of technological security efforts and measures to mitigate cyber risks in various technical areas.

1. Introduction
The main purpose of baseline security is that there must be a legal recognition process to maintain the privacy, reliability, control and legal process of information in the preparation, enrichment, expansion or conservation of information so that the information is secured from unauthorized, access, disclosure, disturbances, conversion, destruction, etc. It is very important for the common man to know about the basic security of information / data in every domain of life [1]. All information that is in the form of electronic data is virtual (imaginary), intangible and invaluable fund and due to being virtual it does not have its geographical boundaries and is driven at very rapid pace throughout the universe; uniformity of law is necessary on this subject in the whole world. Since, all activities depend on the internet, all the related information or data are available on network or in the end points or in the processor or in the storage media. Since the electronic data exchange has no geographic and physical boundaries and is virtual in nature, hence base line security should be adapted by all users to secure their data from hacker and cyber frauds [2].

Section 2 talks about the increasing use of cyber security in various fields and various cybercrimes, attacks and frauds. Today, knowledge and compliance of cyber security is an important subject in all...
areas. In this paper, the need of cyber has been mentioned in five different domains related to cyber security. Section 3 studies the suggestions related to cybercrime, cyber-attack, cyber deception and measures to protect them in bank and financial sector. Section 4 studies the data available in the education institute and information about the side effects of cybercrime on children and how to avoid them. Then, section 5 contains information about the applications used in health services, tools in which computers and internet services are used and studies of computer related crime and prevention measures. Section 6 includes studies on cybercrime related to security services, which is an important part for any country. Section 7 delineates information about automation in the manufacturing industry through technology and the growing cyber threat from them [3]. The paper has focused many daily matters affecting the life of a person and the cyber-attack on them and the measures to avoid them. In the eighth decisive part of the paper, information has been provided about the study of the cyber incidents in all the areas and about the related escape measures [4].

2. Role of Cyber Security in Various Domain
Cyber Security is a Protection of Information, Equipment, Devices, Computer, Computer resource, Communication device and Information stored therein from unauthorized access, Use, Disclosure, Disruption, Modification or Destruction. Through the technologies, processes and practices to ensure preservation of Confidentiality, Integrity and Availability. The all type of business, financial institute, education, healthcare, defense etc. depends on the internet, all the related information or data are available on network or in the end points or in the processor or in the storage media. Since the electronic data exchange has no geographic and physical boundaries and is virtual in nature, it is a global phenomenon hence security is needed in every aspect [5]. For enlighten the cyber security need in every domain, here we consider few areas:

- Baseline Cyber Security in Financial Industry
- Baseline Cyber Security in Education Institutions
- Baseline Cyber Security in Health Care
- Baseline Cyber Security in Defense
- Baseline Cyber Security in Manufacturing Industries

3. Baseline Cyber Security in Financial Industry
Increased use of internet is not untouched by financial organizations like finance, banking etc. Today, all the transactions, details, deposits etc. facilities of the bank are easily completed online. Due to the convenience of providing the facility through internet, all the confidential data of customers such as name, address, mobile number, bank account number, deposit amount, etc. are all easily available to the hacker. Therefore, it is very important to have basic cyber security in the financial industry. During the study it has been found that all people should be aware of all cyber frauds related to banking, how they happened, ways to find out, and measures to be taken in the event of an incident or loss of money [6]. Also, it has been found that cyber insurance can be a way to stop the increasing cyber-crime in the finance industry. A small finance institution or a finance unit operating within an organization can conduct cyber security by making small investments to reduce the damage caused by cyber-attacks.

To prevent cyber-crime in the banking sector growing, there are ways of financial fraud to the customers through the bank, every possible risk in online banking facility, immediately if there is any kind of wrong transaction Information should be given about the method of making information available, etc. [7]. The risk of the customers coming before the banking facility and getting information about the right way will also help in reducing cyber-crime in the financial sector. I read that, every financial institution should adopt a cyber-security model in order to avoid loss of its data, customer data and financial loss. Data protection laws (GDPR) as enforced by the European Union and similar international standards of organization (ISO) etc., should apply any type of security model to the institution and periodically check them with an independent audit body as per rules [8].
Table 1. Cyber Threats in Financial Organization

| Author          | Key Findings                                                                 | Reference |
|-----------------|-----------------------------------------------------------------------------|-----------|
| Bendovschi A.   | i. Increase technology and lack of awareness is one of the main causes of cyber-attack.  
                           ii. Loss of Social Image, Money Trap, Online Fraud. | [3]       |
| Shaun S. Wang   | i. Mitigate Impact of cyber-criminal via investment of Security.            | [5]       |
| Rupesh D. Manna A. | i. Use of Internet allow banking facility Anytime, Anywhere and anyhow banking to all.  
                               ii. Awareness of Fraud using online technology.  
                               iii. Risk Management                           | [6]       |
| Iustina A. Boitan R. | i. Prevention, Identification, Assessment and Management of sensitive and personal sensitive data should be maintained properly.  
                           ii. Monitoring and triggering of transaction should be maintained properly. | [7]       |

4. Baseline Cyber Security in Education Institutions

Education sector is also not deprived of cyber-attacks and fraud. Educational institutions are the easiest way for cyber criminals and hackers. Personal and hyper-sensitive modal data is available in all educational institutions such as names of children, mobile number, address, bank details of staff, health related data of children and staff. Even institutions providing higher studies are not as aware of the increasing cyber-crimes as they should be. Increasing internet competition in the children of the institution and lack of knowledge of the correct use of the Internet, low technical literacy and different types of increasing cyber-crime methods are responsible for cyber-crime in higher educational institutions [9]. During the study of a paper, I found that for the prevention of cyber-crime, the educational institution should use new tools and new technology in its institution, that is, it should update the IT infrastructure of the educational institution and all staff members and children should use the Internet correctly. It should be related to the awareness of student and staff members.

We also found that due to the increasing impact of cyber-crime, the organization should keep the staff related to its own cyber security in order to protect the data, children and staff of the organization so that people from outside and through inside the organization Cyber-crime can be prevented and monitored [10]. Staff members and children’s training programs should be run in the organization. Staff members and children should be proficient in the use of technology through an ongoing exchange program on cyber topics in other universities and countries [11]. To increase cyber security, we should make efforts to raise awareness for students through out of the class activities such as, workshops, tests, quizzes etc. Students and staff members should be made aware of reporting and mitigation related methods by providing real time cyber-crime related scenes [12]. In the study of a similar paper, I also found that to reduce cyber-crime, a new topic and framework should be brought into syllabus in the name of cyber work force so that children can get information about the growing virtual world and preventive measures allow them to be introduced [13].
Table 2. Potential Cyber Threats in Education System

| Author | Key Finding | Reference |
|--------|-------------|-----------|
| Mayieka J.  | i. Institute have personal and sensitive personal data like name address, phone number, health data, banking details.  
Dr. Masese N.  | ii. Cyber Security tool  
iii. Protection against internal and external potential threat. | [10] |
| Hwee J.  | i. Out-of-class learning approach.  
Tampa P.  | ii. Cyber security education among the students.  
Katerattanakul K.  | iii. Course consist some outside cyber security activity. | [11] |
| Moti Z.  | i. User identity theft, privacy sabotage, malicious code, cyber bullying and others.  
Dušan L.  | ii. Each level of the evaluated education systems and practice.  
Srečko N.  | iii. Develop a cyber-awareness education framework (CAEF)  
Kongkiti P.  | | [12] |
| Frankie E.  | i. Cyber-literate workforce  
Catota M.  | ii. Nation’s critical infrastructure  
Granger M.  | iii. Education institute start cyber security course in isolation but it needs combined public awareness  
Douglas C.  | | [13] |

5. Baseline Cyber Security in Health Care

Where the increasing use of technology and the changes taking place day by day is making the work easier in every field, but with the use of technology, their increasing side effects cannot be denied with the changes in the field of medical [14]. The use of technology in the medical field has proved to be very helpful, patient examination, medicine, and necessary advice can be available at any time. In the field of medical, the use of technology, such as oxygen control, ventilator, e-health, m-health and other facilities can be easily operated [15]. Similarly, the patient data is available at any time through the database available in the computer at the time of investigation, due to which all the information related to the patient is available on time and speed up in the disease diagnosis and start therapy [16]. But due to the easy availability of data and work awareness related to data security in the medical department, cyber-attacks are also increasing day by day [17]. For cyber criminals, one-stop adjustment and easy access to all important information like health-related data of the patient, data of health staff, bank details, health policy of the person, etc. is the main reason of increasing cybercrime in the medical field [18]. During the study, I found that for the prevention of cyber-crime, the medical department should properly deploy a cyber-security framework like ISO 27001-2013, ITIL, Health Insurance Portability Accountability Act [recommended for health specific] etc. in the organization and execute independent audit by third party auditor time to time, it should be examined, and measures should be taken to protect it from deficiencies and new cybercrimes [19].

In the study, I found that the reason for the increasing cybercrime in the medical department is the easy availability of data, so to prevent misuse of data, it is necessary to control the availability of data on a remote machine [20]. For which access to the data through remote machine should be available only to the authorized person and the data should be allocated based on the role and responsibility of the personal. The network of the hospital should be isolated from the public network to protect it from public access to data and access to hackers [21]. Pacemakers, cardiology machines etc. are also operated and controlled through many applications, so it is necessary to protect the security of such applications. I found that Machine Learning, Artificial Intelligence and Less Interaction medical facility model should be used in the medical department to further enhance cyber security [22]. To increase cyber security, health staff should be regularly informed about data security, correct use of
technology, methods of happening various cybercrimes, reporting and prevention measures [23]. Third party solution should be deployed in medical department with proper technical knowledge and requirement for additional security of data such as cloud infrastructure, cyber-attack alarm, antivirus etc. The medical institution should recruit cyber security staff so that data and other tools can be timely checked, updated, and upgraded [24].

Table 3. Cyber Attack on Health Care Data and Application

| Author                   | Key Findings                                                                 | Reference |
|--------------------------|------------------------------------------------------------------------------|-----------|
| Martin G.                | i. WannaCry malware attack in health sector.                                | [18]      |
| Martin P.                | ii. Health data and personal data defined in category of Sensitivity by GDPR, Personal Data Protection bill, HIPPA. |          |
| Hankin C.                | iii. Soft Target and weakness in security posture.                           |           |
| Darzi A.                 |                                                                              |           |
| Kinross J.               |                                                                              |           |
| Giansanti D.             | i. Application allow to access patient data.                                | [19]      |
| Monoscalco L.            | ii. Cardiology Machine operated by application.                             |           |
|                          | iii. Exchange of data exposed Administration level vulnerability system.     |           |
|                          | iv. M-Health & E-Health are measure concern in cyber threats.                |           |
| Kieseberg                | i. P4 medicine (personal, predictive, preventive, and participatory) model.  | [20]      |
| P. Malle B.              | ii. “doctor in the loop” seems to be a logical consequence of the application of machine learning technologies and derived knowledge into medical science. |           |
| Fruhwirt P.              |                                                                              |           |
| Weippl E.                |                                                                              |           |
| Holzinger A.             |                                                                              |           |
| Majhia S.                | i. Cyber physical systems are Smart Grid Networks, Smart Transportation System, Enterprise Cloud Infrastructure, Utility Service, Infrastructure for Smart Cities, etc. | [21]      |
| Patrab G.                | ii. Dangers in this transformation are allows flexible control and resource use. |           |
| Dhale S.                 | iii. Due to misconfigurations and deliberate attacks by outsiders and insiders. |           |

6. Baseline Cyber Security in Defence
The cyber world has filled the distances everywhere, the country has brought people living abroad and the same cybercrime has also increased the concern of people and countries. Unauthorized access to data available in every region has increased to a great extent by easy availability and increasing use of internet [25]. The use of technology in the security of countries, state-of-the-art weapons, storage of sensitive and sensitive information of the country, safe use, transfer, etc. has made the country's cyber security to be considered as very important. DDOS Attack, child pornography, religious misinformation, website defection, data dealing, credit fraud, financial damage etc. are common to damage the sovereignty and integrity of the country by cyber criminals [26]. Today, cyber war is also an important challenge due to increasing prevalence of cybercrime, day to day changes in technology, and lack of awareness [27]. To improve the cyber security of the country, it is necessary that special attention should be given on the technology used in the defence sector and the security of the highly sensitive data available [28]. During study I found that all information related to cybercrime and new cyber terminology like Cyber terrorism, Espionage, Hungry for Recognition, Evil-twin, Ransomware etc. and all about the way of being reported, redressal process and preventive measure [29].

We have found that every device and technology related rules and method of use for prevention of cybercrime should be available to everyone in a documented form so that each user can use the device
correctly and according to the rules of cyber security [30]. Before any new device is used, it is mandatory to have an action plan, need, user training etc. in a planned way. In all security related services, it is important to have a meeting of cyber networks related to people, so that they know what things to share [31]. To further enhance cyber security in defence, more filtering processes and security controls should be implemented, so that a cyber-attack can be prevented at an early stage [32]. People related to cyber defence should be trained through training, workshops and other similar type’s activities and there must be IT verification before joining the defence service. We found that Intrusion Detection and Intrusion Prevention System should also be installed for cyber security [33].

| Table 4. Cyber Security Threats in Defence |
|------------------------------------------|
| Author                        | Key Findings                                                                 | Reference |
| Seemma P.                     | i. Cyber terrorism                                                           | [26]      |
| Nandhini S.                   | ii. Cyber Warfare                                                            |          |
| Sowmiya M.                    | iii. Cyber espionage                                                         |          |
|                              | iv. Cybercriminals – hungry for recognition                                  |          |
|                              | v. Cybercriminals – not interested in recognition                            |          |
|                              | vi. Cybercriminals – the insiders                                            |          |
|                              | vii. “point product” approach.                                               |          |
| Galinec D.                    | viii. Strong sense of network security and an effective incident response plan|          |
| Možnik D.                     | i. Critical Communication and Information Infrastructure and Crisis Management| [27]      |
| Boris G.                      | ii. Cybernetic Crime                                                         |          |
|                              | iii. Data Protection                                                         |          |
|                              | iv. Technical Coordination in Computer Security Incidents                     |          |
|                              | v. International Cooperation.                                                |          |
|                              | vi. Developing cyber security within the Strategy and Action Plan             |          |
| Zargar S.                     | i. Disrupt a legitimate user’s connectivity.                                 | [28]      |
| Joshi J.                      | ii. Disrupt a legitimate user’s services.                                    |          |
| David T.                      | iii. Zombies & Botnets                                                        |          |
|                              | iv. Denial of Service attack [DOS]                                            |          |
|                              | v. Distributed Denial of Service attack [DDOS]                               |          |
|                              | vi. Reflection/amplification-based flooding attack                            |          |
|                              | vii. More reliable mechanisms are required to authenticate.                 |          |
|                              | viii. Trusted Communication Mechanism.                                       |          |
| Eric M. Michael J. Rohan M.   | Intrusion Kill Chain                                                         | [29]      |
|                              | i. Reconnaissance                                                            |          |
|                              | ii. Weaponization                                                            |          |
|                              | iii. Delivery                                                                |          |
|                              | iv. Exploitation                                                             |          |
|                              | Indicators and the Indicator Life Cycle                                      |          |
|                              | i. Atomic                                                                    |          |
|                              | ii. Computed                                                                 |          |
|                              | iii. Behavioral                                                              |          |

7. Baseline Cyber Security in Manufacturing Industries
There is a widespread use of technology in all types of industry in developed countries. Use of technology reduces working time and improves quality [34]. But if the correct use of the technology is not planned and if not used properly by skilled users, then this technology can prove fatal for any
industry [35]. During the study, I found that before using the technology in the industry, we have to check risk of the technology, teach employee through training about the new technological change adopt by the industry and should be used manual etc. in a planned manner [36]. The loss from any type of cyber side effect is widespread: All the rules of security should be followed in the proactively. Today is the time of Internet ofThing, and due to the smooth functioning of all devices from any location through the internet, the danger of illegal access remains constant [37].

Hackers or any unauthorized person can detect the deficiency in the system and access data. Therefore, it is mandatory to keep the system updated and follow the appropriate rules in use. Small industry that cannot invest more in cyber security should use cloud-based infrastructure to improve the security of their data [38]. Sensor-based cyber security technology can be used for cybercrime prevention and data monitoring [39]. Appropriate action can be taken on the cyber threats from outside through Intrusion Detection and Intrusion Prevention, so the confidential documents, sensitive data, working model and other important information can be prevented by unauthorized disclosure [40].

Table 5. Cyber Security in Manufacturing Industry

| Author | Key Findings | Reference |
|--------|--------------|-----------|
| Katariina K. Ilona I. | i. Industry automation (ICS)  
ii. Identity and access management  
iii. Lack of cyber security professionals and young employees’ commitment to the cyber secure | [35] |
| Lee J. Jaime A. Christopher B. Jules W. | i. Cyber-security weaknesses in manufacturing systems  
ii. Concerns of industry  
iii. Quality control  
iv. Industry oriented cyber security education | [36] |
| Jaco P. Sinha S. Basie V. | i. 3D Printing  
ii. Traditional Approach to Manufacturing Process Security  
iii. Convergence of IT and OT  
iv. Cloud Based Industries | [37] |
| Cayir E. Bilal E. | i. Getting digital records through sensors.  
ii. Sensor fusion  
iii. Signal processing to optimization, visualization, cognitive and high-performance computation.  
iv. Public and private company executives/authorities | [38] |

8. Conclusion
Every Domain of Computer application should plan for preventive controls which helps to reduce the risks of cyber security by adopting the security preventive controls and should establish cyber security policy, should appoint chief information security officer (CISO), assess the cyber security risks, backup of organization data at different geographic locations, encrypt valuable data, continuous monitor user activity, build an incident response plan, training to employees, regular review of authentication and IT security controls, cyber security drills, cyber security audits, integration of artificial intelligence and machine learning to identify threats and vendor remote access management with multifactor authentication controls. Through the paper, we have learned about the growing technological use in various fields like Financial Industry, Education Institutions, Health Care, Defense, Manufacturing Industries and different type of cyber risks associated with it like loss of money, data theft, loss of reputations, tampering in medical equipment and effect on patient health, damage to the country sovereignty and
integrity etc. Every company is using different types of security method which include cyber insurance, cyber awareness, cyber security in the curriculum of higher studies, training, enhance cyber efficiency etc. to avoid these cyber security related risks.

By the use of preventive controls and baseline security, organization can be able to respond as per Incident response plan, assess the damage and severity, collection of the incident Log and tracing of the suspicious activity, report to nodal agency like Computer Emergency Response Team (CERT-In) and Service providers like Operating System, Hardware, Network devices, Telecom Service Providers, Internet Service Providers, Application Service Providers etc., Backup & recovery of important business data to resume business activities, Notify affected parties so they can protect themselves from cyber incident or secure their computer resource from the disclosure of confidential personal or financial data.

9. References

[1] Andreea B., “Cyber-Attacks – Trends, Patterns and Security Countermeasures” 7th International Conference on Financial Criminology, Wadham College, Oxford, United Kingdom, 13-14, April 2015.
[2] Shaun S., “Integrated framework for information security investment and cyber insurance”, Insurance Risk and Finance Research Centre, Nanyang Business School, Nanyang Technological University, S3-B1A-16, 50 Nanyang Avenue, 639798, Singapore, 2019.
[3] More, Dr Manisha M., and M. P. J. D. K. Nalawade. "Online banking and cyber-attacks: the current scenario." International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, 2015.
[4] Kumar, Ankit, et al. “An improved quantum key distribution protocol for verification.” Journal of Discrete Mathematical Sciences and Cryptography 22.4 (2019): 491-498.
[5] Andersson M., Kok C., Mirza, H., Móré, C. and Mosthaf, J. “How can euro area banks reach sustainable profitability in the future?”, ECB Financial Stability Review, 2018.
[6] Bouveret, A. “Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment”, IMF working paper WP/18/143, 2018.
[7] Cebula, J.J, and Young, L.R. “A taxonomy of Operational Cyber Security Risks”, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University. 2010.
[8] Allied P., Bostan H., “Cybersecurity in Finance Getting the policy mix right!” Report of a CEPS-ECRI Task Force, June 2018 Centre for European Policy Studies-CEPS, (2018).
[9] Mayieka J.M., Masese N., “Emerging Issues in Cyber Security for Institutions of Higher Education” Department of Computer Science and IT, Kabarak, University – Kenya.
[10] Brophy J., “Toward a model of the value aspects of motivation in education: Developing appreciation for particular learning domains and activities. Educational Psychologist, 34(2), 75–85. https://doi.org/10.1207/s15326985ep3402_1
[11] Conklin, W. A., Cline, R. E., & Roosa, T., “Re-engineering cybersecurity education in the US: An analysis of the critical factors”, in Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS), Waikoloa, HI (pp. 2006-2014). Retrieved from https://www.computer.org/csdl/proceedings/hicss/2014/2504/00/2504c006.pdf
[12] Cooper D., & Schindler P., “Evaluation theory and practice applied to cyber security education” Business research methods (7th ed.). New York, NY: McGraw-Hill. IEEE Security & Privacy, 13(2), 75–80. https://doi.org/10.1109/MSP.2015.27. 2015.
[13] Davis, J., & Dark, M., “Defining a curriculum framework in information assurance and security”, In Proceedings of the 2003 ASEE Annual Conference, Nashville, TN (pp. 1-15). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84227&rep=rep1&type=pdf
[14] Katerattanakul, Pairin, and Hwee-Joo Kam. "Enhancing student learning in cybersecurity education using an out-of-class learning approach." Journal of Information Technology
Education: Innovations in Practice 18.1 (2019): 29-47.

[15] Katerattanakul, Pairin, and Hwee-Joo Kam. "Enhancing student learning in cybersecurity education using an out-of-class learning approach." Journal of Information Technology Education: Innovations in Practice 18.1 (2019): 29-47.

[16] Catota, Frankie E., M. Granger Morgan, and Douglas C. Sicker. "Cybersecurity education in a developing nation: the Ecuadorian environment." Journal of Cybersecurity 5.1 (2019): tyz001.

[17] Seemma, P. S., S. Nandhini, and M. Sowmiya. "Overview of cyber security." International Journal of Advanced Research in Computer and Communication Engineering 7.11 (2018): 125-128.

[18] Galinec, Darko, Darko Možnik, and Boris Guberina. "Cybersecurity and cyber defence: national level strategic approach." Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije 58.3 (2017): 273-286.

[19] Ransford B., Kramer D., Kune D., "Cybersecurity and medical devices: a practical guide for cardiacelectrophysiologists", Pacing Clin Electrophysiol 2017; 40:913-7.

[20] Kruse C., Frederick B., Jacobson T., “Cybersecurity in healthcare: A systematic review of modern threats and trends", Technol Health CareCW Jobs (Internet). London, UK: 2016.

[21] Coronado, Anthony J., and Timothy L. Wong. "Healthcare cybersecurity risk management: Keys to an effective plan." Biomedical Instrumentation & Technology 48.1 (2014): 26-30.

[22] Loughlin S., Fu K., Gee T., “A roundtable discussion: safeguarding information and resources against emerging cybersecurity threats”, Biomed Instrum Technol. 2014; 8-17. Available online: 10.2345/0899-8205-48.s

[23] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research 1.1 (2011): 80.

[24] Martin, Guy, et al. "Cybersecurity and healthcare: how safe are we?." Bmj 358 (2017).

[25] Daniele G., Lisa M., “The cyber-risk in cardiology: towards an investigation on the self perception among the cardiologists.”

[26] Kieseberg, Peter, et al. "A tamper-proof audit and control system for the doctor in the loop." Brain Informatics 3.4 (2016): 269-279.

[27] Herring M., Willett D., “Active cyber defense: a vision for real-time cyber defense” J Inform Warfare. 2014;13 (2):46–55.

[28] Marvell S., “The real and present threat of a cyber breach demands real-time risk management”, Acuity Risk Management; 2015.

[29] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research 1.1 (2011): 80.

[30] Majhi, Santosh Kumar, Ganesh Patra, and Sunil Kumar Dhal. "Cyber physical systems & public utility in India: State of art." Procedia Computer Science 78 (2016): 777-781.

[31] Kannus, Katarinaa, and Ilona Ilvonen. "Future prospects of cyber security in manufacturing: findings from a Delphi study." Proceedings of the 51st Hawaii International Conference on System Sciences. 2018.

[32] Cardenas A, Amin S., Huang L., Huang C., Sastry S. Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM symposium on information, computer and communications, security; 2011. p. 355–66.

[33] Stamp J., Dillinger J., Young W., DePoy J.. “Common vulnerabilities in critical infrastructure control systems”, SAND2003-1772C. Sandia National Laboratories; 2003.

[34] Hahn A, Kregel B, Govindarasu M, Fitzpatrick J, Adnan R, Sridhar S, and Higdon M. “Development of the power cyber SCADA security testbed”, Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, New York; 2010. p. 21:1–21:4.
[35] Morris T, Vaughn R, Dandass YS., “A testbed for SCADA control system cybersecurity research and pedagogy”, *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, ACM; 2011. p. 27.

[36] Luallen M., Labruyere J., “Developing a critical infrastructure and control systems cybersecurity curriculum”, *46th Hawaii International Conference on System Sciences (HICSS)*; 2013. p. 1782–91.

[37] Lee J., Wells a, Jaime A., Camelio A, Christopher B. Williams b, Jules White “Cyber-physical security challenges in manufacturing systems”, *Department of Computer Science and IT, Kabarak, University – Kenya*

[38] Jaco P., Sinha S., and Basie S., “Review of Industry 4.0 Manufacturing Process Security Risks” *Kasetsart University, Thailand*

[39] Ervural, Beyzanur Cayir, and Bilal Ervural. "Overview of cyber security in the industry 4.0 era." *Industry 4.0: managing the digital transformation*. Springer, Cham, 2018. 267-284.

[40] Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak. "Security and privacy issues in wireless sensor networks for healthcare applications." *Journal of medical systems* 36.1 (2012): 93-101.