Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 2, 2783 – 2793

Analyzing the Cyber Threat Information to Consolidate the Security Posture of an Application

Shantanu Mukherjee[1], Dr. Sandip Roy[2], Dr.Pinaki Pratim Acharjya[3]

[1]Department of Computational Science, Brainware University, Barasat, Kolkata, India
[2]Department of Computational Science, Brainware University, Barasat, Kolkata, India
[3]Professor, Dept. of Computer Science and Engineering, Techno College of Engineering Agartala, Agartala, Tripura, Pin- 799004

Abstract:

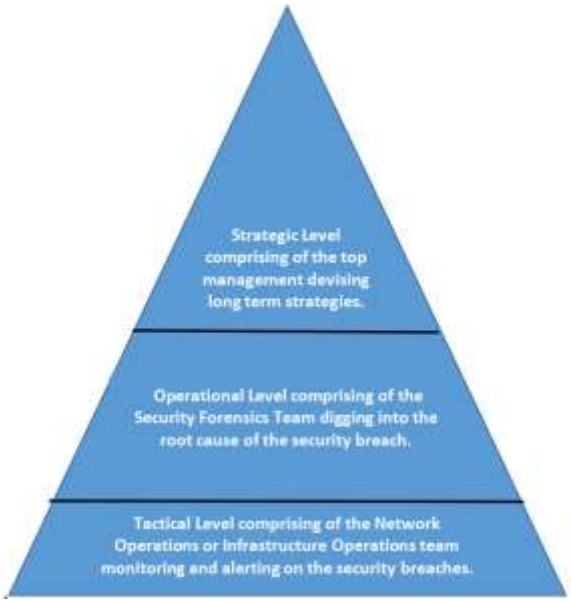
Cyber attacks have manifested drastically from what they used to be say a decade ago. The present attacking mechanisms are meticulously planned and a thoroughly concerted exercise that delays the discovery of those attacks more difficult thereby giving the attackers enough time to wreak havoc on the system. The threat landscape has changed so much that it has become important for the organizations to respond to a live attack rather than respond to a breach after the attacker has accomplished his malicious intentions. A very common response to minimize the impact of a security attack is to isolate the affected node or terminate any process running the attackers' code, however, this has a downside also that the attackers become aware that they have been detected and they go underground leaving no trace so that it can be determined which security aspect got compromised in such attacks.

Keywords: Cyber Attacks, VUCA Framework, Threat Indicators, Preparedness Index, Cyber Intelligence, Cyber Risks, Cyber Exploits

Introduction:

Security defence mechanism is multi pronged. The starting point is to identify the adversary. This is necessary because if the attackers are identified correctly then their attack tactics can be explored further and a potent defence ring can be created to protect your security infrastructure from the cyber espionage agents. This step is further supported by appropriate prioritization of which assets are to be secured [1]. This step is very important to ensure that your data is safe even if your security perimeter is intruded. The practice is not to save and salvage everything but prioritize the information assets that cannot be compromised. These assets could range from confidential customer data to intellectual property assets [2]. This is a continuous iterative process which encompasses the previous two steps discussed earlier. The idea is to learn from previous experience. Thus whatever information is available serves as a knowledge-base for future study, analysis and dissemination and with every iteration the knowledge-base becomes more enriched thereby providing a more intelligent insight into the potential cyber threats and their possible remedies [3][4].

In order to safeguard the security infrastructure we have executives working at various levels. I prefer to define these levels not in terms of job roles but in terms of policies and strategies. It may be called the security pyramid where the Network Operations or the Infrastructure operations team works at the tactical level inputting threat parameters into security tools, thereby contributing to the threat knowledge-base. Their daily job includes monitoring for security breaches and upgrading and patching susceptible systems. At the middle of this pyramid we have got the security forensics team and the fraud detection team working at the operational level to determine the root and details of the attack and unearth any additional security breaches [5][6]. The strategic level comes at the top of the pyramid with the sole purpose of devising a long term strategy to inculcate proper learning from the past breaches and prevent their recurrence.



The VUCA Framework:

The US Army coined a term VUCA - Volatility, Uncertainty, Complexity and Ambiguity. This section focuses on the concept of the VUCA framework. The attack mechanism employed by hackers are evolving continuously, no two attack patterns are same [7]. So to understand the changing threat perception a consistent study and incremental improvements on the security aspect is indispensable. This is where the concept of VUCA gets prominence. Volatility is the assortment of all the factors that are beyond your control and may impact the security defence of your organization. Then comes the uncertainty factor, that leads to the fear of unknown, i.e. it is almost impossible to predict who can attack your security perimeter, why they will do that and what can be the impact [8]. So practically no information is available about the threat and so when it occurs it catches the cyber security staff off-guard. The third factor is complexity. Complexity can be termed as an effect of growing application and the data size or in other words it can also be said that the complexity of an application is directly proportional to the size of the data housed in it [9]. So understanding the complexity at even an abstract level amounts to a enumerating and managing a huge inventory of IT assets and then analyzing how deep could be the impact and how widely it may spread. Although theoretically preached that reducing the attack surface will result in increased prevention against cyber attacks but the gap between theory and practice is much wider than can be actually conceived. The uncertainty part of the VUCA framework was looking for answers to questions like who would attack and why they would attack, but the ambiguity part is assuming that attacks cannot be prevented and sooner or later attacks will occur but it is trying to look into the situations, how that attacks may occur. The attackers may infiltrate the payloads through social engineering or malicious attachments and since, this field is always evolving so there could be ways that may come up in future but are currently unknown to the defenders managing the cyber security [10][11].

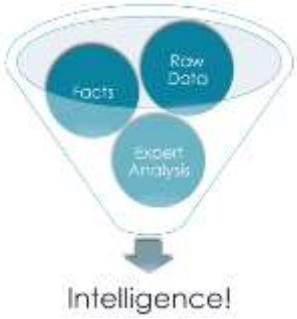
The Continuous response methodology to prevent attacks:

There is no magic wand that defends your organization against all security drawbacks. The defensive mechanism has to be targeted towards the identified adversaries. A thorough knowledge about your opponents should be employed to construct an appropriate defense mechanism. This will help better analyse the risky assets such as data, intellectual property, and other computing resources [12][13]. Threat management is not just about researching on raw threat data. It also involves removing those indicators that may create false positives, identifying the vulnerabilities in terms of their severity and patching them on priority. An analysis of a best case and a worst case scenario should be performed to be better equipped with the gravity of the situation and be able to perform a wider and in depth investigation into the attackers intentions and methods [14][15]. Thus, the focus of the analysis should be to

- Visualize, identify and scrutinize the appropriate threat source.
- Filter the data to ascertain the most important intelligence and summarize it in the right level of detail so as not overwhelm the user with information overload.

The Cyber Intelligence:

What is the primary difference between data and information - data is the raw material and information is the intelligence derived from that raw material. Flooded with terabytes of data on cyber crime will not serve any purpose unless it is churned to derive the necessary information[16].



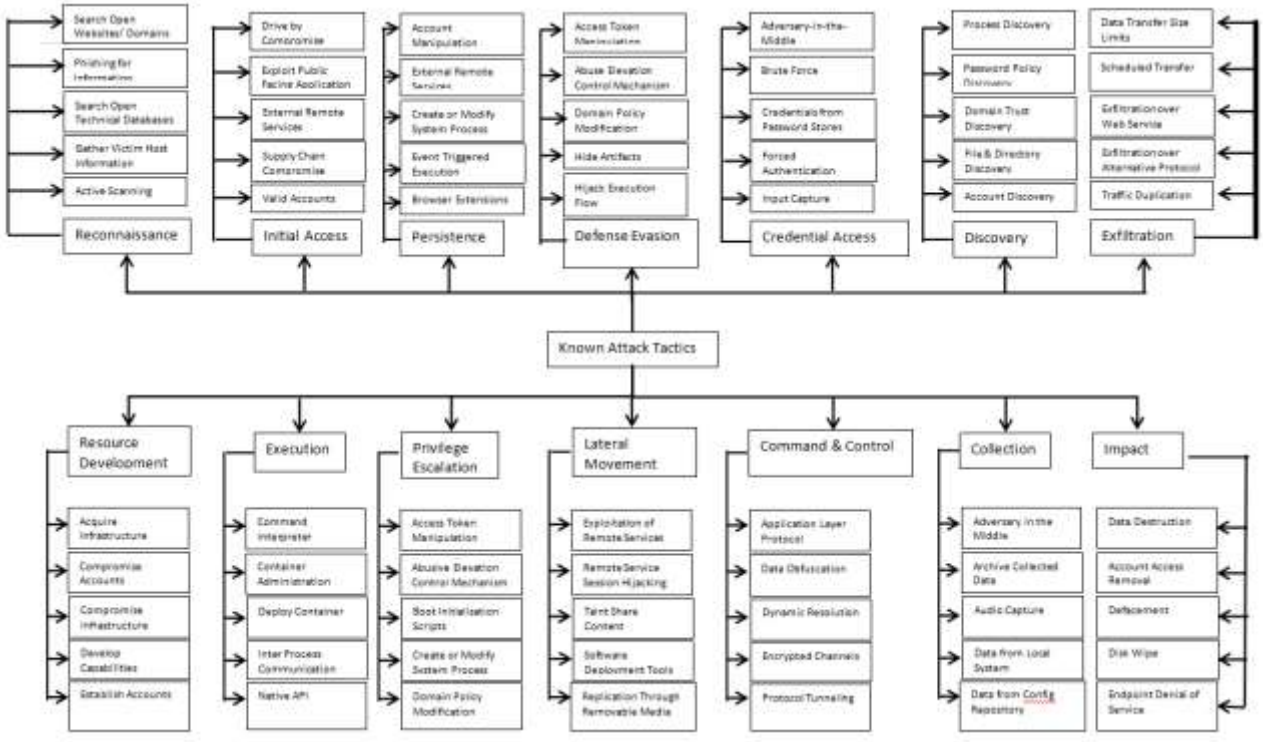
The Figure below groups the cyber threat categories into three categories:

	Threat Indicators	Threat Data Feeds	Strategic Cyber Threat Intelligence
Content	File hashes and reputation data	Statistics, trends, survey data, and analyses of malware	Information on adversaries and their motivations, intentions, tactics, techniques, and procedures
Key Uses	Increase the effectiveness of blocking technologies and generate alerts	Help SOC and IR teams identify patterns associated with attacks	Help IR and forensics teams analyze attacks, hunt for breaches, and remediate; help managers improve defenses and invest strategically
Primary Sources	Honeypots and scanners on networks	Statistical analyses of indicators, surveys, and sandboxing products	Hacker web forums, underground marketplaces, and personal contacts

Reference: Definitive Guide to Cyber Threat Intelligence, by Jon Friedman and Mark Bouchard

The Preparedness Index:

The known attack tactics that broadly cover the whole gamut of threats are shown in the figure below:



The table below is used to determine a company's preparedness or its ability to deal with cyber exploits and breach incidents that may handle the threats listed in the above figure[17][18][19]. Each attribution is rated using the following adjective scale.

Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree

Attributions used to evaluate the preparedness to respond to cyber attacks: [20][21]

- Budget allocation to protect the data assets.
- Acquisition of the required security technology to protect the data and the IT infra.
- Training need analysis and appropriate upskilling from time to time to protect the data assets.
- IT Security is placed high up in the priority pyramid
- Security is treated as an inherent feature and not as a compelling requirement.
- The IT Team is at liberty and equipped with the necessary resources to bolster the security posture from time to time.
- A strategic push to examine and adopt new technologies like machine learning, automation, orchestration, Analytics and/or artificial intelligence tools.
- Threat sharing with other companies and government and preparing learning outcomes from those are done sincerely.
- The entire supply chain is duly evaluated for security risks before any integration with a third party tool .
- Security education is given due weightage and the employees are always encouraged never to let their guards down.
- The security is cast into the SecOps model and is continually evolving [22][23].
- The security functions are formed in adherence to the data protection and the privacy requirements.
- High interoperability, scalability and agility parameters are factored in the security facet[24].
- Mock drills, regular assessments and/or audits should be embedded in the schedule to identify the security risks [25][26].
- Proper implementation of countermeasures (such as honeypots) to gain intelligence about the attacker are carried out when required[27].

Scoring the Preparedness Index: Each attribution is equally weighted and scored using the following heuristic:

Strongly agree = 10 points

Agree = 7.5 points

Unsure = 5 points

Disagree = 2.5 points

Strongly disagree = 0 points

The average of all scored attributions is a numerical value between 0 and 10 points, with a theoretical mean of 5 points. The higher the score is above 5 indicates higher is the preparedness and similarly a score below 5 indicates the opposite.Following are the ranges and color coding used for interpreting the results:

Range	Colour	Interpretation
7.6 to 10 points		Very favorable, unambiguous results
5.1 to 7.5 points		Favourable, with mixed results
2.6 to 5 points		Unfavourable, with mixed results
0 to 2.5 points		Not prepared, unambiguous results

The following ten questions can be used to evaluate the threat index relating to the actual experiences of companies over the past 12 months.

The table below shows the first six questions that are scored using a five-point numeric scale.

Table: Recent history of cyber exploits and breaches [28][29]
The count of separate data breach incidents involving the loss or theft of customer records over a period of past twelve months?
The number of data breach incidents involving the leakage of information assets over a period of past twelve months?
The number of cyber attacks that infiltrated the organization's networks over a period of past twelve months.
An approximate probability that the organization may encounter a data breach of customer records within the next twelve months.
An approximate probability that the organization may encounter a data breach involving the leakage of information assets (e.g., intellectual property) within the next twelve months
An approximate probability that the organization may encounter one or more cyber attacks infiltrating the networks within the next 12 months

Table below shows Q7, which is a list of 13 data types from a risk perspective (rated using a 5-point adjective scale from very high to very low).

Table: Data types that increase cyber risk [30]
Following are data types that may be at risk of loss or theft within your organization. Please rate each data type using the following 5-point risk scale: Very high risk (10), high risk (7.5), moderate risk (5.0), low risk (2.5) and very low risk (0).
Analytics (data models)
Attorney-client privileged information
Business communication (email)
Company-confidential information
Consumer data
Customer accounts
Financial information
Human resource (employee) files
Operational information
Product/market information
R&D information
Source code

Trade secrets

Table below shows Q8, which is a list of 19 cyber threats from a risk perspective (rated using a 5-point adjective scale from very likely to no chance)

Table: Cyber threats that increase cyber risk [31] Following are cyber threats that may be experienced by your organization within the next 12 months. Please rate each threat using the following 5-point likelihood scale: Very likely (10), likely (7.5), somewhat likely (5), not likely (2.5) and no chance (0).
Advanced malware
Advanced persistent threats (APT)
Botnets
Clickjacking
Cross-site scripting
Denial of service (DoS)
DNS-based attacks
Fileless attack
Login attacks
Malicious insiders
Man-in-the-middle attack
Phishing and social engineering
Ransomware
Registration spamming
Root kits
Server side injection (SSI)
SQL and code injection
Watering hole attacks
Web scrapping

Table below shows Q9, which is a list of 9 negative consequences that arise from cyber threats (rated using a 5-point adjective scale from very likely to no chance)

Table: Negative consequences of cyber threats [32][33] Following are negative consequences that your organization may experience as a result of a cyber attack or breach within the next 12 months. Please rate each negative consequence using the following 5- point likelihood scale: Very likely (10), likely (7.5), somewhat likely (5), not likely (2.5) and no chance (0).
Lost revenues
Lost intellectual property (including trade secrets)
Stolen or damaged equipment
Disruption or damages to critical infrastructure
Productivity decline
Regulatory actions or lawsuits
Reputation or brand damage
Customer turnover
Cost of outside consultants and experts

Table below shows Q10, which is a list of 16 areas of the IT infrastructure from a risk perspective (rated using a 5-point adjective scale from very high to very low)

Table: Areas of the IT infrastructure that increase cyber risk [34][35] Following are 16 areas that may present security risks within your IT infrastructure today. Please rate each area using the following 5-point risk scale: Very high risk (10), high risk (7.5), moderate risk (5), low risk (2.5) and very low risk (0).
DNS server environment
Data centers
Within operating systems
Across 3rd party applications
Desktop or laptop computers
Mobile devices such as smart phones
IoT devices and applications
Network infrastructure environment (gateway to endpoint)
Malicious insiders
Negligent insiders
Shortage of qualified personnel

Cloud computing infrastructure and providers
Virtual computing environments (servers, endpoints)
Mobile/remote employees
Lack of system connectivity/visibility
Organizational misalignment and complexity

Score	Number of incidents	Likelihood of occurrence	Risk	Likelihood of occurrence	Likelihood of occurrence	Risk
0	None	No chance	Very low	No chance	No chance	Very low
2.5	1 to 2	Not likely	Low	Not likely	Not likely	Low
5	3 to 6	Somewhat likely	Moderate	Somewhat likely	Somewhat likely	Moderate
7.5	7 to 10	Likely	High	Likely	Likely	High
10	More than 10	Very likely	Very high	Very likely	Very likely	Very high

Scoring the threat Index: Each one of the 10 items/questions are equally weighted and scored using the following heuristics:

The average of all 10 scored questions is a numerical value between 0 and 10, with a theoretical mean of 5 points. An average value above 5 points indicates a high cyber threat environment, and a value at or below 5 points indicates the opposite. Following are the ranges used for interpreting results:

Range	Color flag	Interpretation
7.6 to 10 points		Not prepared, unambiguous results
5.1 to 7.5 points		Unfavorable, with mixed results
2.6 to 5.0 points		Favorable, with mixed results
0 to 2.5 points		Very favorable, unambiguous results

Conclusion:

The security landscape has become so dynamic that the security teams need to identify the motives and the attacking techniques of their adversaries. This information has to be combined with technology to rein in the cyber attacks these days. It is important to collect and analyze information about the threat actors and deriving near accurate predictions about their attacking strategies, their motives and the extent of damage they may cause. Preventing an attack is certainly paramount but so is immediate incident response to arrest the spread and severity of the attack. Cyber Intelligence is the way moving forward since it is based on the assimilation of the gather information and suggesting the next best course of action.

References

[1] Gill, J., Okere, I., HaddadPajouh, H., Dehghantanha, A.: Mobile Forensics: A

Bibliometric Analysis. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 15, p. in press. Springer - Advances in Information Security series (2018)

[2] Homayoun, S., Ahmadzadeh, M., Hashemi, S., Dehghantanha, A., Khayami, R.: BoTShark: A deep learning approach for botnet traffic detection. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 7, p. in press. Springer - Advances in Information Security series (2018)

[3] Riesco, R., Villagrá, V.A. Leveraging cyber threat intelligence for a dynamic risk framework. Int. J. Inf. Secur. 18, 715–739 (2019). https://doi.org/10.1007/s10207-019-00433-2

[4] Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R.: Towards a maturity model for inter-organizational cyber threat intelligence sharing: A case study of stakeholder's expectations and willingness to share. In: Proceedings of Multikonferenz Wirtschaftsinformatik (MKWI 2018), pp. 6–9. Springer, Heidelberg (2018)

[5] Wiem Tounsi, Helmi Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks, Computers & Security, Volume 72, 2018, Pages 212-233, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.09.001. (https://www.sciencedirect.com/science/article/pii/S0167404817301839)

[6] Florian Menges, Günther Pernul, A comparative analysis of incident reporting formats, Computers & Security, Volume 73, 2018, Pages 87-101, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.10.009. (https://www.sciencedirect.com/science/article/pii/S0167404817302250)

[7] Li, Han; Luo, Xin (Robert); and Chen, Yan (2021) "Understanding Information Security Policy Violation from a Situational Action Perspective," Journal of the Association for Information Systems, 22(3), DOI: 0.17705/1jais.00678 Available at: https://aisel.aisnet.org/jais/vol22/iss3/5

[8] Hamidreza Shahbaznezhad, Farzan Kolini & Mona Rashidirad (2021) Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter?, Journal of Computer Information Systems, 61:6, 539-550, DOI: 10.1080/08874417.2020.1812134

[9] Inho Hwang, Robin Wakefield, Sanghyun Kim & Taeha Kim (2021) Security Awareness: The First Step in Information Security Compliance Behavior, Journal of Computer Information Systems, 61:4, 345-356, DOI: 10.1080/08874417.2019.1650676

[10] He Li, Sungjin Yoo & William J. Kettinger (2021) The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches, Journal of Management Information Systems, 38:1, 222-245, DOI: 10.1080/07421222.2021.1870390

[11] Yuchong Li, Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 2021, Pages 8176-8186, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.126. (https://www.sciencedirect.com/science/article/pii/S2352484721007289)

[12] Bhol SG, Mohanty JR, Pattnaik PK. Taxonomy of cyber security metrics to measure strength of cyber security. Materials Today: Proceedings. 2021 Jun 24.

[13] Kaur, Jagpreet, and K. R. Ramkumar. "The recent trends in cyber security: a review." Journal of King Saud University-Computer and Information Sciences (2021)

[14] Tavares, Joao & Dutta, Paramartha & Dutta, Soumi & Samanta, Debabrata. (2022). Cyber Intelligence and Information Retrieval - Proceedings of CIIR 2021. 10.1007/978-981-16-4284-5.

[15] Tavares, Joao & Dutta, Paramartha & Dutta, Soumi & Samanta, Debabrata. (2022). Cyber Intelligence and Information Retrieval - Proceedings of CIIR 2021. 10.1007/978-981-16-4284-5.

[16] Murat Odemis, Cagatay Yucel, Ahmet Koltuksuz, "Detecting User Behavior in Cyber Threat Intelligence: Development of Honeypsy System", Security and Communication Networks, vol. 2022, Article ID 7620125, 28 pages, 2022. https://doi.org/10.1155/2022/7620125

[17] Ramsdale, A.; Shiaeles, S.; Kolokotronis, N. A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. Electronics 2020, 9(5), 824;

https://doi.org/10.3390/electronics9050824

[18] Yuchong Li, Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 2021, Pages 8176-8186, ISSN 2352-4847, https://www.sciencedirect.com/science/article/pii/S2352484721007289

[19] Taewoo Nam, Understanding the gap between perceived threats to and preparedness for cybersecurity, Technology in Society, Volume 58, 2019, 101122, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2019.03.005

[20] Shaikha Hasan, Mazen Ali, Sherah Kurnia, Ramayah Thurasamy, Evaluating the cyber security readiness of organizations and its influence on performance, Journal of Information Security and Applications, Volume 58, 2021, 102726, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102726

[21] Pedro Taveras, Cyber Risk Management, Procedures and Considerations to Address the Threats of a Cyber Attack, Proceedings of the ForenSecure: Cybersecurity and Forensics Conference, Chicago, Illinois April 12th, 2019

[22] Berlilana; Noparumpa, T.; Ruangkanjanases, A.; Hariguna, T.; Sarmini. Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. Sustainability 2021, 13, 13761. https://doi.org/10.3390/su132413761

[23] Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani, Vijey Thayananthan, A Survey: Agent-Based Software Technology Under the Eyes of Cyber Security, Security Controls, Attacks, and Challenges, (IJACSA) International Journal of Advanced Computer Science and Applications Vol. 10, No. 8, 2019

[24] Singh, Arunabh. (2022). Cyber Security Frameworks. International Journal for Research in Applied Science and Engineering Technology. 10. 590-599. 10.22214/ijraset.2022.39843.

[25] Bhol, Seema & Mohanty, JR & Pattnaik, P.K.. (2021). Taxonomy of cyber security metrics to measure strength of cyber security. Materials Today: Proceedings. 10.1016/j.matpr.2021.06.228.

[26] Rana Khudhair Abbas Ahmed. Overview of Security Metrics. Software Engineering. Vol. 4, No. 4, 2016, pp. 59-64.doi: 10.11648/j.se.20160404.11

[27] Alsmadi, Izzat & Easttom, Chuck & Tawalbeh, Loai. (2020). The NICE Cyber Security Framework: Cyber Security Management. 10.1007/978-3-030-41987-5.

[28] Gorecki, Andrew. (2020). Investigating and Remediating Cyber Breaches. 10.1002/9781119679349.ch5.

[29] Gorecki, Andrew. (2020). Technology Considerations in Cyber Breach Investigations. 10.1002/9781119679349.ch3.

[30] Aldasoro, Iñaki & Gambacorta, Leonardo & Giudici, Paolo & Leach, Thomas. (2022). The drivers of cyber risk. Journal of Financial Stability. 100989. 10.1016/j.jfs.2022.100989.

[31] Tankard, Colin. (2021). Quantifying cyber risk. Network Security. 2021. 20. 10.1016/S1353-4858(21)00066-0.

[32] Cam, Hasan. (2022). Cyber risk and vulnerability estimation. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. 19. 3-4. 10.1177/15485129211070058.

[33] Jamilov, Rustam & Rey, Helene & Tahoun, Ahmed. (2021). The Anatomy of Cyber Risk. SSRN Electronic Journal. 10.2139/ssrn.3866338.

[34] Badhwar, Raj. (2021). Dynamic Measurement of Cyber Risk. 10.1007/978-3-030-75354-2_40.

[35] Woods, Daniel W & Bohme, Rainer. (2021). SoK: Quantifying Cyber Risk. 211-228. 10.1109/SP40001.2021.00053.