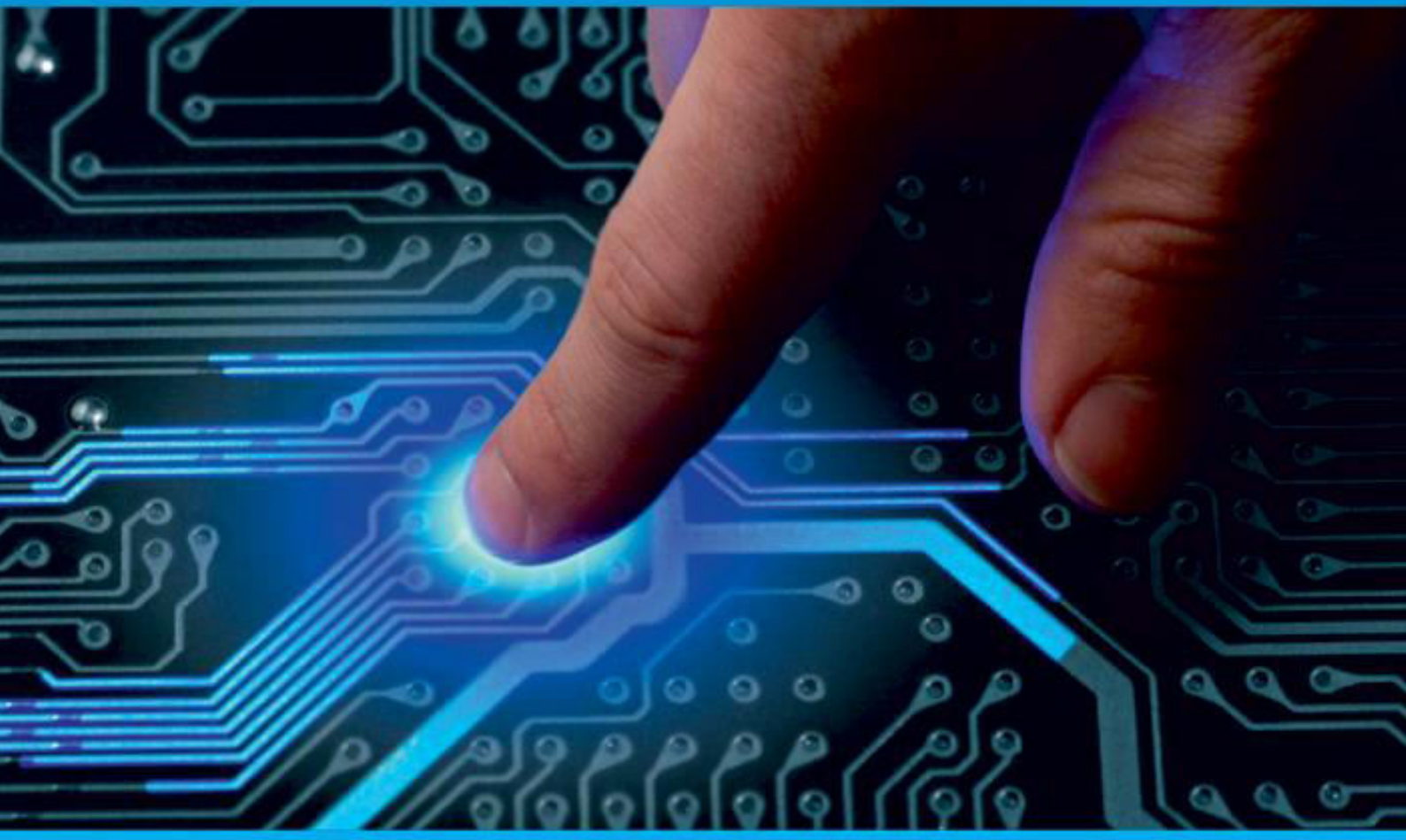
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 9, September 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009010 |

Cyber Security Good Practices and It's Socioeconomic Effects

[1]Madhusree Pramanick, [2]Shreya Dutta Banik, [3]Anirban Bhar, [4]Moumita Ghosh

[1,2] B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

[3,4]Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

ABSTRACT: An active role is accepted by cyber security in the field of information technology. In the modern era, information security has grown to be a major issue. The term "cybercrimes" comes to mind first when discussing cybersecurity, because they occur on a massive scale every day. Numerous steps are being taken by various governments and groups to stop these cybercrimes. In addition to other measures, many people continue to have serious concerns about cybersecurity. This essay focuses mostly on cyberterrorism and security. It discusses the key developments in cybersecurity as well as their effects and the role of social media in cyber security. Associations could lose billions of dollars as a result of cyberterrorism in the area of organizations. This essay primarily focuses on the difficulties that modern technology-based cyber security faces. It also emphasizes the most recent information on cyber security strategies, ethics, and trends that are shaping the field.

KEYWORDS: Cyber Security, Cyber Crime, Information Security, Cyber Ethics, Social Media.

I. INTRODUCTION

Today, anyone may send and receive any kind of information with the click of a button, whether it be a video, an email, or something else entirely, but has that person ever considered how secure that information is when it is sent to another person? Cybersecurity is the ideal response. Today, more than 61% of all industry trades take place online, making high-quality security in this sector a must for direct and successful exchanges. Consequently, cybersecurity has emerged as a pressing problem (Dervojeda, et. all., 2014). The scope of cybersecurity extends beyond simply validating data in the IT sector to other areas like cyberspace and so on. The security and economic well-being of each nation depend heavily on enhancing cybersecurity and making sure that required data systems are in place.

The improvement of new management as well as a legislative approach now depends on making the Internet safer (and protecting Internet users). A broad and secure practise is required to combat cybercrime (Gross, Canetti &Vashdi, 2017). The particular estimates alone cannot keep any crime; it is necessary that legal authorization offices be allowable to investigation and indict cybercrime efficiently. In order to prevent the loss of any crucial data, several governments and countries nowadays are imposing severe regulations on cyber safety. Each person needs to be knowledgeable about cybersecurity to protect oneself from the rising number of cybercrimes.

Both the insecurity created by and through this new environment, as well as the techniques or procedures to make it (progressively) secure, are topics covered by cyber-security (Kumar, &Somani, 2018). It alludes to numerous practises and actions, both specialist and non-specialized, that are anticipated to protect the bioelectrical state and the data it holds and transmits from all potential dangers. This study attempts to compile all available data and an overview of cybercrime, as well as historical information and reports on the data analysed from various attacks that have been widely published over the past five years. Based on the information examined, we would like to outline all the precautions that businesses may take to ensure greater security, which would aid in protecting them from hacker attacks and give a level of cyber-security that eliminates all dangers.

II. HISTORICAL BACKGROUND

Interdisciplinary, multidisciplinary, cross-disciplinary, and transdisciplinary notions were listed in a taxonomy by Cat [1]. The approach used in this review is most akin to transdisciplinarity, which views cybersecurity and economics as two distinct but interdependent systems of thought that interact in a complex socio-technical system. The interaction of various systems is the beginning point of a complex socio-technical system paradigm, which explains their relative interdependence with reference to how they interact in social and technical situations. We can capture the potentially transformative interactions between cybersecurity and economics using this paradigm.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009010 |

Information security and cybersecurity are frequently used interchangeably. Despite the fact that cybersecurity and information security have a lot in common, Solms and Niekerk contend that the two ideas are not equivalent [2]. They contend that cybersecurity extends beyond the conventional parameters of information security to encompass safeguarding other assets, such as human and cyber-physical systems, as well as information resources.

We present a definition of cybersecurity despite ENISA's conclusion that it is not necessary [3] to do so in order to minimize ambiguity over what cybersecurity comprises. When computers and other cyber-physical systems carrying important data are linked to the internet, standard procedures including people, processes, and technology in an organization, a group, or a stand-alone setting are called "cybersecurity." Cybersecurity is concerned with the various practices that safeguard assets to create a secure environment. An asset is everything that has value to a company, in accordance with ISO/IEC 27002 [4]. According to their ability to be converted (current and non-current assets), physical existence (tangible or intangible assets), and utilization (operating or non-operating assets), assets can be divided into various categories [5]. Some assets have a relational component. These assets are the product of investments made by one or both partners to promote a certain relationship [6].

Cyber risk management and cybersecurity economics have debated the value of these assets and the risks of loss or harm. Depending on the assets' cost [7], market [8], and usefulness [9], several valuation techniques are used. With the quick advancement of information technology, digital assets are now understood to be essential components of businesses. Cybersecurity does not only apply to digital assets, though. The rise in cyberattacks over the past ten years against physical assets and vital infrastructures has shown that cybersecurity is now a significant physical and cyber threat for businesses and governments.

Strategic planning, capital budgeting, and effective asset protection all depend on an accurate asset assessment. This is why if bad decisions have been made or are being made, the process is modified. The economic assessment of the assets and determining the ideal degree of security investment in organizations to safeguard those assets have occupied a large portion of the published research on cybersecurity economics [10][11]. However, cybersecurity economics is concerned with how a digital ecosystem and its operational agents work and behave, as well as whether an organization is spending enough to secure its assets and whether the security budget is allocated to the proper security measures and controls [12][13].

Additionally, cybersecurity economics focuses on the effectiveness of choices made as a result of incentives and regulations that are intended to optimize profit and environmental trust [14].

There isn't now agreement on what the word "cybersecurity economics" means. Their definitions, which were developed by numerous investigations, are typically wide. The area of cybersecurity economics that is focused with offering the greatest level of asset protection at the lowest possible cost is perhaps the one that is most widely acknowledged [15][16]. Rathod and Hämäläinen, on the other hand, took a broader approach to the economics of cybersecurity based on long-term, strategic thinking that incorporates economics right away [14].

Studies on cybersecurity economics cover factors that influence stakeholders' investments in cybersecurity services, market and regulatory systems, as well as environmental, institutional, and distributional effects of the social decision-making process. The investigations also look into the motivations, tools, and interest of actors in today's shadowy markets, as well as the economics of cybercrime.

III. CYBER SECURITY TRENDS

Some of the trends that are significantly affecting cyber security are listed below.

Web hosts:

Web application attacks that aim to extract data or disseminate harmful code continue to pose a hazard. Through genuine web servers they have infiltrated, cybercriminals disseminate their malicious code. However, assaults that steal data pose a significant threat as well and are frequently covered by the media. We now need to put more of a focus on safeguarding web servers and web applications. Particularly effective platforms for these cybercriminals to steal data are web servers. In order to avoid becoming a victim of these crimes, one must always use a safer browser, especially during important transactions.

The cloud and its services:

These days, cloud services are being gradually adopted by all small, medium, and large businesses. In other words, the earth is gradually encroaching upon the clouds. Due to the ability of traffic to bypass conventional points of inspection, this most recent trend poses a significant problem for cyber security. In order to prevent the loss of important data, policy controls for web applications and cloud services will also need to change as the number of

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009010 |

applications available in the cloud increases. Even though cloud services are creating their own models, security concerns are still a major concern. Although the cloud may offer tremendous benefits, it is important to remember that as the cloud develops, security problems also do.

APTs and targeted attacks:

A new class of cybercrime software is called a "APT" (Advanced Persistent Threat). For years, network security tools like web filtering and intrusion prevention systems (IPS) have been crucial in spotting such targeted attacks (mostly after the initial compromise). Network security must interact with other security services to detect assaults as attackers become more brazen and use hazier tactics. Therefore, we must enhance our security measures to stop new risks from emerging in the future.

Mobile Networks:

Thanks to modern technology, we can connect with anyone, wherever in the globe. Security, however, is a very serious worry for these mobile networks. Nowadays, firewalls and other security measures are getting more permeable as more people use devices like tablets, phones, PCs, and other similar ones, all of which again need additional security measures in addition to those found in the programmes being used. We must always consider how secure these mobile networks are. Additionally, mobile networks are quite vulnerable to these cybercrimes, thus extreme caution must be used in the event of any security difficulties.

IPv6:New Internet Protocol:

IPv6 is the new Internet protocol that will eventually replace IPv4 (the previous version), which served as the Internet's and our networks' main skeletons. It takes more than simply migrating IPv4 capabilities to protect IPv6. While IPv6 is a complete replacement in terms of expanding the number of IP addresses available, there are some very basic modifications to the protocol that security policy must take into account. Therefore, it is always preferable to migrate to IPv6 as soon as feasible to lower the dangers associated with cybercrime.

The practise of encrypting messages (or other information) so that prying eyes or hackers cannot read them is known as encryption. An encryption algorithm is used in an encryption technique to transform the message or information into an unintelligible cypher text. An encryption key, which determines how the message is to be encoded, is typically used for this. At its most basic level, encryption safeguards both the integrity and privacy of data. However, greater encryption use creates more cyber security challenges. Additionally, encryption is used to secure data that is being exchanged across networks (such as the Internet, e-commerce), mobile devices, wireless microphones, wireless intercoms, etc. Therefore, by encrypting the code, one can determine whether there has been any information leakage.

IV. FRAMEWORKFOR CYBER SECURITY MODELLING

At the moment, cybersecurity experts typically build the cybersecurity model based on study areas they are accustomed to. We present a common systems framework for cybersecurity modelling in this part, as shown in Figure 1. This conceptual framework identifies five crucial components:

Cyberspace's physical and virtual components are both a part of the real world. It supplies the observations for the empirical models, such as data, events, and situations, in addition to the embodiment of concepts, parameters, and equations in the mathematical model.

• Mathematical modelling is a type of theoretical strategy for converting cybersecurity system behaviour into precise formulations using mathematical ideas and terminology. The mathematical model seeks to describe the cybersecurity issue that exists in the real world and how the Cybersecurity technology changes.

• Empirical modelling is a common research strategy that was developed from observations of cybersecurity systems by evaluating the outputs of the systems, such as pertinent data, security events, or cyberattack cases. Its objectives include determining the empirical rule or characterization of the actual observation, portraying the state of network security at the moment, and determining the probabilistic direction of future trends.

• Inference describes the process of drawing conclusions using various analytical techniques and instruments. The inference is a purposeful action that is motivated by a particular cybersecurity problem and seeks to identify the best approaches and solutions for actual cybersecurity.

Practice entails the study, creation, and application of a genuine cybersecurity solution while following the recommendations of analytical findings. This is a part of the technical study that tries to apply the theoretical analysis of cybersecurity to actual cybersecurity tools and techniques in a real-world cyberspace situation.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009010 |

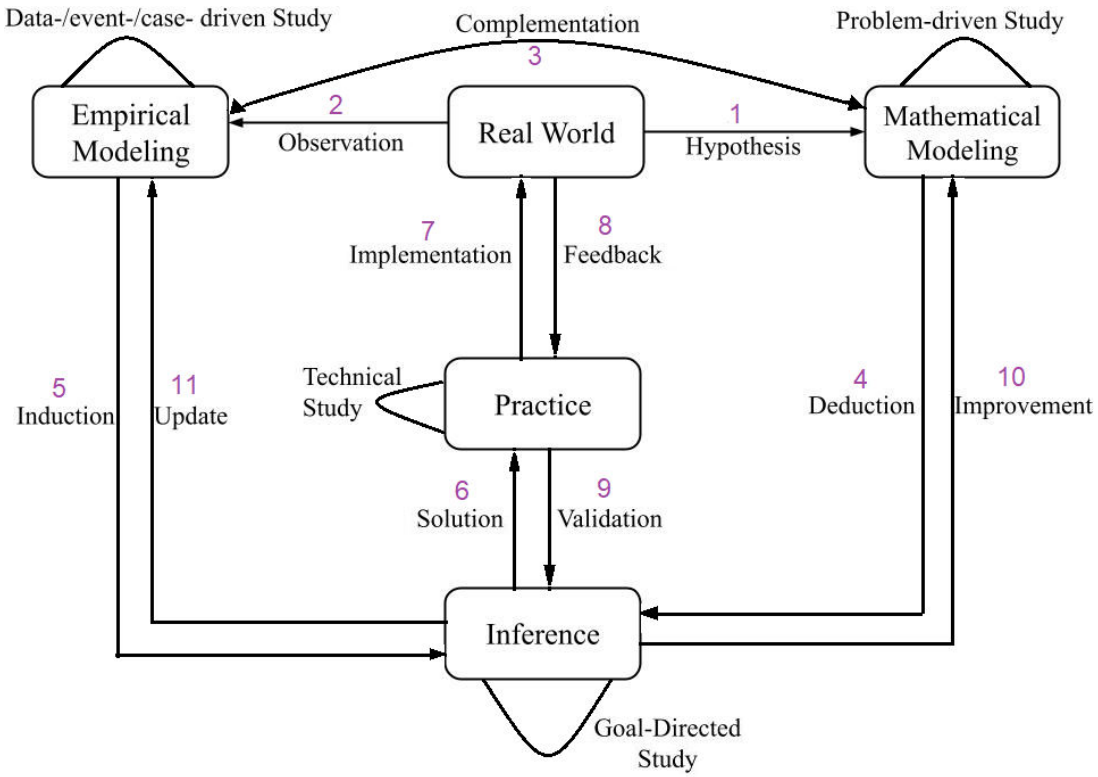


Fig.1.cybersecurity modelling approach

V. ROLE OF SOCIAL MEDIA IN CYBER SECURITY AND SOLUTION

For some people, social media has become an integral part of their lives. We use it to remain in touch, organise events, share our photos, and provide comments on recent happenings. It has taken the role of email, and using the phone takes a lot of us. But it's important to be aware of the risks, just like with anything else online. Computers, smartphones, and other devices are priceless possessions that give people of all ages the exceptional ability to interact and work with the rest of the world. People can accomplish this in a variety of ways, including by using social media or networking websites.

APTs and targeted attacks:

An entirely new class of cybercrime software is known as an APT (Advanced Persistent Threat). For years, network security tools like web filtering and intrusion prevention systems (IPS) have been crucial in spotting such targeted attacks (mostly after the initial compromise). Network security must interact with other security services to detect assaults as attackers become more brazen and use hazier tactics. Therefore, we must enhance our security measures to stop new risks from emerging in the future.

Cyberterrorism:

The term "terrorism" can refer to the unlawful use of force or violence against individuals in order to threaten a government, its citizens, or its associations, possibly in order to carry out a political or harmful purpose. The traditional framework of terrorism has given way to an innovation-supported kind of terrorism known as cyber terrorism. They continue to be important issues in today's culture.A lot of these hackers use "brute force", which is the combinations of every single imaginable letter, number, and image until they find the password Sreenu, & Krishna, 2017).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009010 |

Hacking:

The general term of all kinds of unauthorized access to any "computer system" network organize is hacking that can occur in any structure.

Computer viruses:

These are randomly distributed on a system in order to do harmful operations, such as acting as an administrative agent, generating information, or even destroying the system.

The increasing frequency of this cyber terrorism invading associations and country's information has produced a lot of issues which has resulted in loss of vitals and critical information that is typically difficult to recover.

Data intrusion:

The cyber terrorism can annihilate information honesty with the goal that the information could never again be trusted, pulverizing its classification as intruding on its accessibility.

Here are some suggestions for preventing cybercrime and cyberterrorism and there are a few methods that may be used to increase cybersecurity:

Data's Authentication: Before transferring, the documents we receive should always be verified. It should verify that it originated from a reliable source and that it has not been altered (Gade, & Reddy, 2014). The "antivirus" software installed on the devices usually verifies these records. Consequently, to protect the devices from infections, good "antivirus" software is also required.

Antivirus software: It is a computer application that categorizes, avoids, and attempts to destroy or remove harmful software programmes, such as viruses and worms. The majority of "antivirus programmes" include a "auto-update" feature that enables the programme to download profiles of new viruses so that it may check for them when they are discovered.

Malware scanners: These programmes search all of the files and archives currently stored in the system for malicious code or dangerous viruses. Trojan horses, worms, and viruses are examples of "malicious software" that are frequently assembled and referred to as malware.

Firewall: A "software application" or piece of hardware that assists in keeping an eye on diseases, worms of all kinds, and hackers that attempt to access a PC via the Internet All data that is transmitted over the internet today passes through the firewall.

Access control and Password security: The idea of a user name and password has long been a cornerstone of information security. This might be one of the initial cyber security measures.

VI. CONCLUSION AND FUTURE WORK

This article will contribute to the advancement of scientific inquiry into cybersecurity, specifically by providing a procedural response to the issue of foreseeing future data and activities that will have a substantial impact on security patterns. This study establishes the context for starting to implement regulations for all purposes as stated by the typical security concerns and solutions for data systems. This study combines a number of processes that are related to cybersecurity and may be enhanced in terms of anticipating the operational legitimacy of the methodology of assessment benchmarks. The emphasis on preventing, recovering from, and eliminating weakness is the fundamental pattern and response to the ongoing expansion of development. Over the course of the next five years, cybercrime may seriously harm information technology. The researchers claim that they have calculated a loss of about close to 6 trillion dollars. Therefore, there would be excellent opportunity for those who strive to tackle cybercrime-related difficulties and supply the necessary security measures. Since cybersecurity is the future of information technology safety, large firms like CISCO, which is entirely focused on networking technology and is among the top organizations, have millions of opportunities in this field. To protect a nation's sensitive data from cyber attackers, there are numerous opportunities in government-related industries and the defense industry.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009010 |

REFERENCES

1. Cat, J. The Unity of Science. In The Stanford Encyclopedia of Philosophy; Zalta, E.N., Ed.; Metaphysics Research Lab, StanfordUniversity: Stanford, CA, USA, 2017.
2. Von Solms, R.; Van Niekerk, J. From information security to cyber security. Comput. Secur. 2013, 38, 97–102.
3. Brookson, C.; Cadzow, S.; Eckmaier, R.; Eschweiler, J.; Gerber, B.; Guarino, A.; Rannenberg, K.; Shamah, J.; Gorniak, S. Definitionof Cybersecurity-Gaps and Overlaps in Standardisation; ENISA: Heraklion, Greece, 2015.
4. ISO/IEC27002. Information Technology–Security Techniques–Code of Practice for Information Security Controls, (AS ISO/IEC 27002:2015); International Organization for Standardization: Geneva, Switzerland, 2015.
5. Coulon, Y. Rational Investing with Ratios: Implementing Ratios with Enterprise Value and Behavioral Finance; Springer Nature: Cham,Switzerland, 2019.
6. Straub, D.; Rai, A.; Klein, R. Measuring firm performance at the network level: A nomology of the business impact of digitalsupply networks. J. Manag. Inf. Syst. 2004, 21, 83–114.
7. Moody, D.L.; Walsh, P. Measuring the Value of Information—An Asset Valuation Approach. In Proceedings of the SeventhEuropean Conference on Information Systems (ECIS'99), Copenhagen Business School, Frederiksberg, Denmark, 23–25 June 1999;pp. 496–512.
8. Henderson, S.; Peirson, G.; Herbohn, K.; Howieson, B. Issues in Financial Accounting; Pearson Higher Education: Melbourne,Australia, 2015.
9. Godfrey, J.; Hodgson, A.; Tarca, A.; Hamilton, J.; Holmes, S. Accounting Theory; Wiley and Sons: Hoboken, NJ, USA, 2010.
10. Arora, A.; Hall, D.; Piato, C.; Ramsey, D.; Telang, R. Measuring the risk-based value of IT security solutions. IT Prof. 2004,6, 35–42.
11. Bistarelli, S.; Dall'Aglio, M.; Peretti, P. Strategic games on defense trees. In International Workshop on Formal Aspects in Security andTrust; Springer: Berlin/Heidelberg, Germany, 2006; pp. 1–15.
12. Ekelund, S.; Iskoujina, Z. Cybersecurity economics–balancing operational security spending. Inf. Technol. People 2019, 32,1318–1342.
13. Anderson, R.; Schneier, B. Guest Editors' Introduction: Economics of Information Security. IEEE Secur. Priv. 2005, 3, 12–13.
14. Rathod, P.; Hämäläinen, T. A novel model for cybersecurity economics and analysis. In Proceedings of the 2017 IEEE InternationalConference on Computer and Information Technology (CIT), Helsinki, Finland, 21–23 August 2017; pp. 274–279.
15. Gordon, L.A.; Loeb, M.P. The economics of information security investment. ACM Trans. Inf. Syst. Secur. (TISSEC) 2002,5, 438–457.
16. Bojanc, R.; Jerman-Blaži˘c, B. A quantitative model for information-security risk management. Eng. Manag. J. 2013, 25, 25–37.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details