Social Science Journal for Advanced Research
ISSN (Online): 2583-0074
Volume-3 Issue-1 || January 2023 || PP. 1-5 DOI: 10.54741/ssjar.3.1.1

Cyber Security Evolution and Conceptualization

Zouqiong H
Assistant Professor, Department of Information System, Chengdu University of Technology, Sichuan, China

Corresponding Author: 897040928@qq.com

Received: 03-12-2022 Revised: 23-12-2022 Accepted: 11-01-2023

ABSTRACT
Cyber security is concerned with matters of cyber-ethics and cyber-safety. The idea of cyber security should be introduced to and ingrained from a young age. Security countermeasures aid in preserving the confidentiality, availability, and integrity of information systems by preventing or lessening asset losses brought on by cyber security threats. An intrusion detection system (IDS) application analyses what happens during an execution and searches for indications that the computer has been mistreated. Numerous metaphors, including those relating to biological processes, healthcare, markets, three-dimensional space, and the preservation of tangible goods, were taken into account. These in turn sparked the investigation of a wide range of prospective tactics for advancing cyber security in the future. The concepts of "Heterogeneity," "Motivating Secure Behaviour," and "Cyber Wellness" were employed to define these tactics. Cyber security plays an important role in the development of information technology and Internet services. Our attention tends to gravitate toward "Cyber Security" when we hear about "Cyber Crimes." Therefore, how well our system handles "Cyber Crimes" is the first factor we take into account when talking about "National Cyber Security". This newsletter focuses on expanding trends in cyber security in light of the widespread adoption of cutting-edge technologies including mobile computing, cloud computing, e-commerce, and social networking. In the research, it is also covered how challenges are exacerbated by a lack of coordination between security organizations and crucial IT infrastructures.

Keywords: *cyber safety, metaphors, internet engineering task force, intrusion detection system*

I. INTRODUCTION

"In China, we went directly from having no telephones to having the most cutting-edge mobile technology." The same is true for internet-connected PCs. They sprang out of nowhere, and nobody was given even the most fundamental information on cyber security. China is ranked fifth globally among nations that are impacted by cybercrime. Nevertheless, it should be noted that these numbers are extrapolations. Widespread computer illiteracy and easily pirated equipment account for a large portion of its vulnerability. One of the most rapidly developing areas of technical infrastructure is the internet. Disruptive technology like cloud computing, social computing, and subsequent-technology mobile computing are considerably altering how companies use records technology for on-line records trade and alternate in modern-day corporate weather. More than eighty% of all industrial transactions are actually carried out online, as a consequence this enterprise wished a high degree of security for the most reliable and obvious transactions. The scope of cyber protection encompasses now not best the safety of IT systems in the organization but also the larger digital networks, such as the internet itself and essential infrastructures, upon which they depend. In the development of facts generation and Internet offerings, cyber protection is critical. Each nation’s protection and monetary health depend on improving cyber safety and safeguarding vital data infrastructure.

When setting up, maintaining, and using computers and the Internet, people's actions and decisions have an impact on cyber security. Cyber security includes the physical defence (hardware and software) of confidential data and technological assets against unwanted access obtained through technological means. The remark "Problems cannot be solved with the same level of knowledge that produced them" is attributed to Albert Einstein. More generation cannot cope with the give up-user mistakes trouble; as a substitute, a collaborative attempt and collaboration between the information generation network of interest and the bigger commercial enterprise community, as well as the important backing of senior control, is required.

The entire spectrum of human endeavors, including enterprise, banking, healthcare, power, enjoyment, conversation, and national defense, have all grown to rely on cyber networks. According to recent research findings, public problem over privateers and personal statistics has grown since 2006. Exploring the metaphors we employ in the field of cyber security may be able to enhance our thinking and conversation in four different ways. First, by mapping concepts from other domains into the realm of cyber security, we may better appreciate the value and limitations of those notions. Second, experimenting with novel or uncommon metaphors could inspire academics and policymakers to think creatively. Thirdly, metaphors that are exceptionally effective may be expanded into brand-new conceptual frameworks or models for tackling cyber security issues. Fourth, a metaphor performs a heuristic function by helping non-specialists understand abstract cyber security topics in domains they may be more familiar.

II. CURRENT IT SECURITY STRATEGIES

The majority of IT security management techniques use checklists to help decision-makers create a coverage plan; they typically amount to little more than a triage method for classifying threats. In an effort to deal with risk analysis qualitatively, models have been developed. In eBook The Executive Guide To Information Security, Mark Egan (then Symantec's CTO) proposed a notably truthful tabular paradigm that allows customers to classify hazard severities into one among three classes/columns (low, medium, and excessive), after which to average throughout columns. Although insightful, this trustworthy triage approach to subjective hazard impact evaluation is noteworthy for shooting machine uncertainty. OCTAVE, a machine created with the aid of Albert's and Dorofee, additionally evaluates threat using qualitative records. Others have experimented with quantitative methods for IT safety risk analysis.

2.1 Stress Test for China

A proposed national cyber-security strategy is being debated. China places little value on online privacy, and as a result, data control is frequently disregarded. Another justification for phishing and other scams is this. The government is using a two-pronged strategy that focuses on capacity building and teaching best practises to stop attacks. China has been spending a lot of money on cyber security because it is conscious that cybercrime hurts its reputation as a place where international investors may conduct business. China's current biggest problem is judicial system and enforcement of law, especially outside of major cities like Bangalore, Delhi, and Mumbai. According to Bajaj, training needs to be expanded to include the entire nation. At DSCI, we have created a police officer training and investigation guidebook. We have given more than 9,000 members of the court and local educational administrations cyber security training.

III. SECURITY RISKS FOR CYBERSPACE

Cyber-attacks and cyber exploitation are two broad categories that can be used to classify threats to cyber security. Cyber-attacks target and aim to harm or destroy cyber systems, while cyber exploitation aims to use the infrastructure for illegal or harmful purposes without harming or compromising it. Cyber exploitation includes the use of the Internet and other cyber systems for unlawful purposes, such as fraud, theft, the recruitment and training of terrorists, infringement of copyright and other laws governing the distribution of information, the transmission of polarizing messages (such as political and "hate" speech), and the sale of child pornography or other illegal materials. The following list of new online dangers.

3.1 Cloud Computing

Regarding cloud computing, data filling has been outsourced for 40 years. The spatial distribution of this storage is novel. A brief, on-demand community to a shared pool of computer assets is the definition of cloud computing provided with the aid of the National Institute of Standards and Technology (NIST). These are essentially server hangers; they are now not the stratosphere. Many businesses are already embracing outsourcing for computing and information garage since it results in massive price reductions. All of the predominant corporations, which include Amazon, eBay, Google, Facebook, and others, outsource compute to the cloud. According to Rohozinski, cloud computing entails dividing the contents in a way that did not previously exist. Our rules governing territorial security and copyright are distorted. The price of processing power and bandwidth, as well as the general issue of net neutrality, are a few more concerns brought up by cloud computing. But Luna issues a warning that these new storage facilities raise issues with jurisdiction and security. Who will you file a lawsuit against if there is a problem? For example, Google keeps a third of its cloud in Canada.

3.2 Security Issues with Smart Phones

Smart phones and cloud computing have brought us a whole new set of inter-connectedness related issues that call for new laws and fresh thought. Rafal Rohozinski, a Canadian specialist, claims that "the mobile internet is the transforming thing." Mobile devices, many of which are found in developing nations, will be the primary mode of connection for the next 2 billion consumers. The sheer number will probably have a similar social impact to flash mobs. There are several requests for the regulation of cyber space as well as an increase in political activity online. States are being reinvested with the power to manage cyberspace as part of the overall governance of the internet.

IV. MODERN CYBERSECURITY MEASURES

4.1 National Measures

Numerous national governments have passed legislation intended to penalise certain types of cyber-attacks or exploitation and so serve as a deterrent. However, these rules have little to no impact on those who the United States lacks or is unable to gain regulatory or criminal jurisdiction over, such as persons, groups, or nations. Nearly all of the time, US national security professionals stress the importance of taking national action to improve cyber security. They advocate for national legislation to safeguard the dissemination of threat and attack information, strategies for government agencies like the NSA to collaborate with private organizations in determining the origin and nature of cyber-attacks, and more potent defenses and countermeasures against cyber-attacks and exploitation created through government-sponsored research and coordination in accordance with cyber security plans. The GAO's report from July 2010 describes the precise roles that numerous U.S. agencies are playing in attempts to improve "global cyber-security," but it comes to the conclusion that these efforts do not form a coherent strategy that is likely to advance U.S. interests.

4.2 Individual Steps

Major roles are played by non-governmental organizations in the field of cyber security. The Web Consortium, located at the Massachusetts Institute of Technology, defines technical standards for the Web. The privately controlled Internet Engineering Task Force (IETF) develops and proposes technical standards for the Internet (including current and next generation versions of the Internet Protocol).

4.3 Global Initiatives

National governments frequently work together informally to exchange information, look into crimes or attacks, stop or prevent harmful behaviour, provide proof, or even arrange for the extradition of people to a state that requests it. States have also made official, international agreements that have an impact on cyber security either directly or indirectly. The defined criminal behaviours are covered by the international accords, even if the suspected offenders exploited cyber technology to carry them out. The UN Charter and the Geneva Conventions are just two examples of cyber security efforts.

V. CYBER-SECURITY IS ESSENTIAL

The most precious resource for an individual, business sector, state, or nation is information. Concerned regions with regard to an individual are:

1. Preventing unauthorized disclosure, modification, and access to the system's resources.
2. Security when doing online banking, stock market, and retail purchasing activities.
3. Protection of accounts from hijacking while utilising social networking sites.
4. Different missions or organizations attract various enemies with various objectives, necessitating varying degrees of readiness.
5. The need for a distinct unit to handle organizational security
6. It is important to think about capabilities, intentions, and targeting activities. Considering the state and the nation
7. When determining the type of cyber danger a mission or organisation confronts, the interaction of an adversary's
8. Protecting the data base that keeps track of all the organization's rights at the state level.
9. Securing the data comprising the results of several important surveys.

VI. SURVEY CONCERNS REGARDING CYBER SECURITY TRENDS

The research and poll on cyber security were used to create the list below:

1. Innovative Platforms and Devices
2. Protect systems rather than information
3. Networking on social media
4. Mobile Technology and Apps

VII. CYBER-ERA METAPHORS

The adoption of cyber security measures was viewed from the standpoint of the market in a second strategy called "Motivating Secure Behaviour." The fundamental idea is that a lot of the flaws in present systems may be attributed to how incentives are structured for both suppliers and consumers of information technology, which in turn shapes how people behave. The third strategy, named "Cyber Wellness," looked for parallels between initiatives to advance both individual and societal health. Its goal is to maintain the population (consisting of users and networked systems) in the best possible health, which includes being resilient to stress, attack-resistant, wary of unsafe situations, curable if ill, and able to control contagions. In general, information systems that require protection typically have three characteristics, according to the literature on cyber security:

1. Integrity - Confidence that data or computer systems have not been altered or destroyed. Loss of data integrity could manifest as instructions to the system that cause human losses, material and financial losses.

2. Confidentiality - communications and information privacy. In terms of the government, this can entail limiting access to classified material to those who are permitted. It may refer to the safeguarding of confidential information in business

3. There are two key aspects of this cyber security are metaphors and the Second, the way a problem is phrased typically suggests just particular types of answers, obviating the possibility of other types of solutions being considered. To enable further elaboration, the more recent or uncommon metaphors were then divided into a number of groups.
4. Availability is the promise that data or services will be available when needed. Interfering with availability includes denial of service attacks, which overwhelm system servers and take down websites.

VIII. COMBATING CYBER-SECURITY THREATS

8.1 Intrusion Detection System (IDS)

The problem of attacks on computer infrastructures is getting more and more serious. Any series of acts intended to jeopardise the integrity, confidentiality, or accessibility of a resource are referred to as intrusions. Therefore, intrusion detection is needed as an extra barrier to secure systems. Not only is intrusion detection helpful in identifying successful intrusions, but it also offers vital information for prompt counter measures. Misuse intrusion detection identifies intrusions using well-defined attack patterns that take use of flaws in system and application software. To identify intrusion, these patterns are encoded beforehand and compared to user behaviour. The usual usage behaviour patterns are used by anomaly intrusion detection to locate the intrusion. The statistical measurements of the system properties are used to create the typical usage patterns. Any divergence from the designed usual behaviour is identified as an intrusion when the user's behaviour is observed. In order to provide a sense of security in computer systems, Dorothy Denning suggested the idea of intrusion detection. The fundamental tenet is that incursion behaviour entails anomalous system usage. In more recent advances, several methods and procedures have been applied. Statistical methods, expert systems, predictive pattern generation, state transition analysis, pattern matching, and data mining techniques are a few of the techniques used.

8.2 Security Architecture for GPRS

The GPRS protection architecture is a collection of safety techniques used by GPRS to obtain its protection desires. The majority of those strategies have been evolved for GSM first of all, but they were altered to house packet-orientated site visitors and GPRS community additives. The number one goals of the GPRS security structure are two:

1. To thwart unauthorized access to the network, and
2. To safeguard users' privacy. It consists of the following elements:
   GPRS backbone security, Subscriber Identity Module (SIM), Subscriber Identity Secrecy, and Subscriber Identity Authentication.

8.3 Distributed Intrusion Detection System (DIDS)

In Distributed IDS (DIDS), traditional intrusion detection systems are deployed over a wide network while being incorporated in intelligent agents. IDS agents can communicate with a centralised server or with one another in a dispersed setting. The network administrators can take preventive action by early identifying planned and coordinated attacks thanks to distributed monitoring. Additionally, DIDS facilitates better network monitoring, incident analysis, attack tracing, and worm management. Additionally, it aids in the detection of new dangers posed to the network by unauthorised users, backdoor attackers, and hackers across numerous, geographically distinct locations. It is crucial to make sure that each individual IDS in a DIDS is accurate and lightweight. For a networked or distributed context, a number of IDS have been proposed. Individual distributed intrusion detection packages can work together to accomplish network intrusion detection without relying on centralised control thanks to cooperating security managers (CSM). On the local host, each CSM finds harmful activities. Each CSM will notify the CSM on the host from which the connection originated if any notable activity is noticed during the detection of suspicious activity. Only the system directly preceding it in the connection chain will be notified by the local CSM, not the other networked systems. DIDS are merely a distributed implementation of the traditional IDS superset

.

IX. CONCLUSION

The improper collection and storage of private information, problems with inaccurate private information, or improper or misused access to that information all result in human rights violations. This essay also discusses the current dangers, problems, constraints, and solutions that the IT sector in our society is currently confronting. Given the increasing frequency of cyber-attacks, developing an intrusion detection model that is reliable and performs well in real-time is crucial. Chinan inhabitants need to choose the top security features in order to safeguard the documents and systems they work with as well as the society at large. In order to increase the number of profound, securely skilled professionals working in the information sector across all industries and improve both the communication and brain compatibility abilities of both employees and employers, it will be necessary in the near future to implement cyber-protection curriculum.

REFERENCES

1. Himanshu Arora, Tanuj Manglani, Geetanjli Bakshi, & Shikha Choudhary. (2022). Cyber security challenges and trends on recent technologies. in *6th International Conference on Computing Methodologies and Communication (ICCMC)*.
2. Christos Xenakis. (2008). Security in 2.5G mobile systems. *IGI Global*.
3. Loren Paul Rees, Jason K. Deane, Terry R. Rakes, & Wade H. Baker. (2011). Decision support for Cybersecurity risk planning. *Decision Support Systems*.
4. Verma, A. K., & A. K. Sharma. (2014). Cyber security issues and recommendations. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(4), 629–634.
5. Dr. Vivekananth.P. (2022). Cybersecurity risks in remote working environment and strategies to mitigate them. *International Journal of Engineering and Management Research*, *12*(1), 108–111. Available at: https://doi.org/10.31033/ijemr.12.1.13.