International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Cyber Insurance

Alex R Mathew

Abstract: ***The Information Technology is an essential discipline in our daily activities. We use our mobile phones often to communicate with our loved ones, research over the internet, and much more. Organizations and institutions today solely rely on computers configured over networks in their daily operations. Organizations prefer having their information backed up on virtual servers referred to as cloud computing. Cloud computing is among the safest measures to information security. We often share information either directly using storage media or over the internet. Information shared or stored over the internet is prone to attacks referred to as cyberattacks. Cyberattacks can result in total impairment of an organization's data, blockage of part or the whole information in the form of a trojan. At this point, the attacker demands payment before they grant you access to your information. Cyberattacks have thus resulted in organizations encrypting their information. However, despite the use of advanced encryption technique, cyber attackers have gone beyond this level of technology to hack into the data by gaining access to the decryption key. Researchers have thus come up with cyber insurance, which offers security to organizations' and businesses' information. Cyber insurance uses high-level algorithms that are difficult for the attackers to understand. It minimizes cases of information compromisation.***

Keywords: Phishing, Trojan, Espionage, Nash equilibrium, Encryption, Cloud Computing

I. INTRODUCTION

Cyber insurance is also known as a cyber liability or cyber risk insurance. Cyber insurance is an insurance product which is used in protecting businesses as well as individual users from internet-based risks. It mainly protects users from information technology risks. Over time, technology-related threats have considerably evolved. For instance, in the 1990s, cyber insurance policies primarily focused on online software. However, the technology, with its accompanying systems, have extensively evolved into a volatile and vibrant cyber insurance market. In the United States, for example, cybersecurity insurance policies also begun in the late 1990s. Some of the online policies covered online media, unlike others which were errors in systems that involved data processing (EDM).

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Alex R Mathew*, Ph.D. in Computer Science and Engineering, India.

Therefore, the new cyber insurance policies critically evolved as a result of liability policies for media and software risks. In addition, it is in the early 2000s that cyber insurance policies commenced covering network security, unauthorized access, data loss, and other virus-related issues. Generally, cyber risk insurance policies have had several exclusions.

These exclusions include regulatory claims, rogue employees and fines and penalties. Initially, the actual drafting of these insurance policies neglected to encompass first-party coverage. It is in the mid-2000s that these particular policies began to address the first-party coverages. In this case, the updated policies commenced covering policies like cyber extortion, network asset damage and cyber business interruption as well. The evolvement of software-related systems enhanced the addition of HIPAA liability. Notably, it is in 2003 when the insurance policies became enacted in the California Security Information and Breach Act. The enactment influenced other states to pass similar laws which had prudent effects on the private sector. Thus, various cyber insurance organizations started to embrace authentic first-party coverages. Public relations, IT forensics, customer notifications and credit monitoring were significantly adapted during this era. Also, business organizations began to notify civilians affected by an unauthorized party's data manipulation.

II. METHODOLOGY

Methodology describes how cyber insurance will be achieved within organizations around the globe. The game theory. This theory is regarded as the science of strategy. The theory tries to suggest logically and mathematically the actions which should be taken by players to guarantee themselves the best outcome. Historically, the game theory was established by a mathematician, Jon Von Neumann in the year 2004. Initially, the emphasis was put on games which involved pure conflict while other games, on the contrary, were considered to be in a cooperative form. Games are always different from the decisions which are made in a neutral environment. A game player should still recognize his interaction with other purposive and intelligent people so as to ensure his choices allow for conflict as well as possibilities of cooperation. The game theory exploits the Nash equilibrium, which refers to a stable state of a system involving different participants reacting. It further elaborates that no participant can gain or change in any way, provided that the strategies of the other participant remain unchanged.

A large-scale system, for example, an industrial control machine or a power grid or even a consumer credit reporting agency, contains various parts. These include the cyber and the physical components which need to be secured. During decision making, one needs to make reliable decisions on what to secure without forgetting the extent to which it should be secured.

The complicating part is that most large-scale systems consist of multiple owners. Interdependent companies are vulnerable to attacks.

This shows the weak links in the network, even though budgetary constraints place their limits on security measures. This theory tackles the tedious workings involved in the human decision-making process and the fact that various stakeholders are likely to act in their self-interest.

The cooperative model gives everybody the freedom to choose what is best for the system, a scenario which is quite unrealistic in the real world. In this case, people might also be unwilling to reveal their commercial secrets to other persons. Researchers have already explained how the formulation of an optimization problem enables one to efficiently find out the value every stakeholder will want to invest.

Take an example of a stakeholder, say M, is going to invest Y amount of money mainly for protecting assets A, B and C. Additionally, stakeholder N is going to invest here and there. The fact about most systems is that they are designed in a way that they are sitting ducks. In this game theory, an attacker has to keep trying now and then. However, the defender has to be successful every time. The moving-target defense attempts to change this fact and make it look like the system to be protected is not in a sitting duck position. It changes some aspects of itself from time to time to ensure that whenever the attacker attempts to attack again, chances of succeeding are minimal. The NSF-funded part is the project's game-theoretic decision-making side.

Secure systems are mostly needed for distributed platforms that use sophisticated technologies in intelligence gathering, reconnaissance and surveillance. UAVs and robots have also been deployed as decision making agents. The future complex military technologies, for example, land vehicles and UAVs will be capable of reconnaissance, surveillance and intelligence. Here, the main idea of deploying military mobile systems or UAVs on an area is to ensure that there is constant monitoring. The moment the communications with the base station is interfered with, the vehicles, on their own, can be able to function and operate in a self-organizing way accurately. In the case of some UAVs being damaged, these others should be able to work together in a self-organized network. The network needs to be too smart to avoid instances of compromisation or malfunctioning.

VANET is a sub-branch of MANET that is facing many research challenges security-wise. Vehicular Ad-hoc Network is rapidly changing and the most challenging branch of Mobile Ad-hoc Network which enables communication between vehicles and with the roadside units as well. VANET's mode of communication is through wireless medium among cars and is always expected to support a vast range of applications with high-security levels. With this capability to support an extensive range of comfort applications and road safety, it has increasingly become a very reliable component of the Intelligent Transportation System. Applications of VANET include Collision Avoiding Applications, Intelligent Transportation System, among others.

Attack Tree Diagram

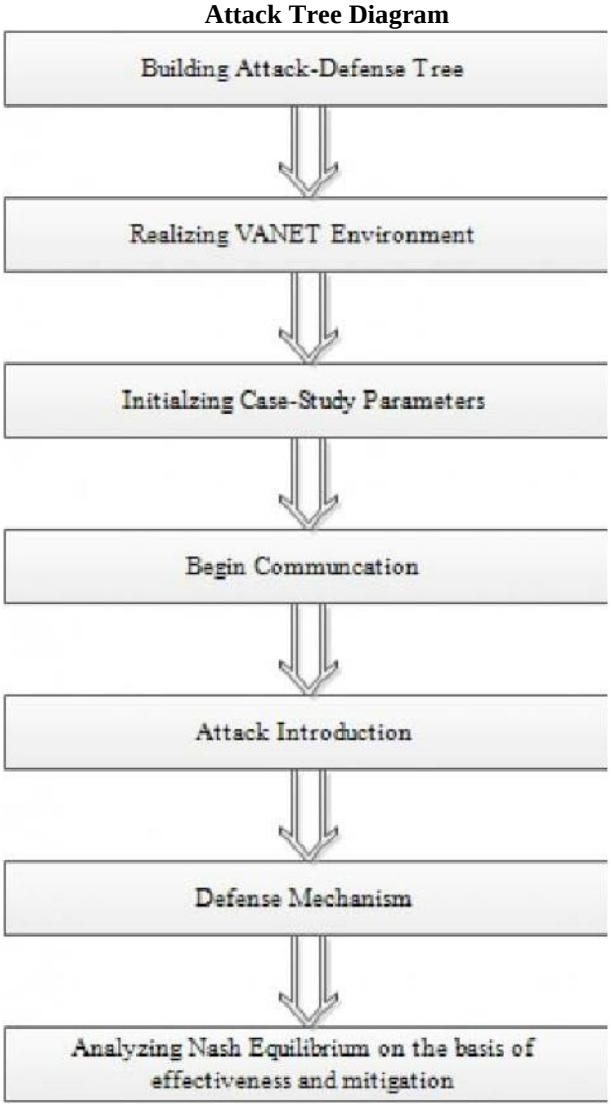

Figure [1.1] Attack-Defense Tree

III. RESULTSS ANALYSIS

An attack-defence tree, also an AD Tree is just a node-labelled rooted tree. The tree describes the possible measures that an attacker might put in place to attack a system and the defence mechanism a defender puts in place to counter the attacker. The VANET environment should then be identified. VANETS must meet the standard security requirements. That is confidentiality, authenticity, data integrity and many more. Case study parameters are then initialized, which state the main objective of the study. The risk of a cyberattack on a business can be calculated mathematically. It depends on factors such as the impact of the risk, probability that the risk will happen and the cost. That is,

Risk = (Impact * Probability) /Cost per hour.

Moreover, there are specific steps in insurance policy development, which include:

a) Identify need

Develop an insurance policy depending on the anticipation of demand and the response to the actual needs as well.

b) Find out who to take the lead responsibility.
Assign responsibilities to a person, staff members, working group or sub-committee as per the experience required.
c) Collect information
Do you have a legal task in this field? Do you have an accurate and up-to-date understanding? Have any other organization dealt with a similar issue? These are the kind of questions that one needs to ask themselves to ensure data accuracy.
d) Draft a policy
You to be sure that the policy's complexity is within the expectations of its implementers.
e) Carry out consultations.
Consultations should be carried out with the most appropriate stakeholders. Consulting with those affected will result in very effective policies.
f) Approve the policy
It is now the responsibility of the management committee to approve the policy.
g) Be sure of procedures requirement.
Procedures are required to support internal policies.
h) Implement the policy
The policy should the be implemented in the organization.
i) Monitor, review and revise.
Monitoring and reporting measures should be put in place to ensure the implementation of the policy is effective.

IV. ALGORITHM:

An algorithm is a specific formula or procedure used in solving a given problem. It outlines a set of specified actions to be adhered to for accurate results during the problem-solving process. In cybersecurity, for instance, a specific algorithm is preferred over the other after having put into consideration. Critical aspects like the strength of the algorithm to protect an institution against possible cyber-attacks, and the level of technology existing on the internet. Also, the complexity of the algorithm and its reliability and adaptability is considered as well. In detecting wide-ranging attacker behaviors, it will require a set of algorithms. Each appropriately designed with a technical understanding of these algorithms to be used and how they relate to each other.
Every algorithm must be designed with questions in mind such as;
a) Is this algorithm directed or undirected?
b) Is there a natural space to project the inputs from?
c) If not, will this algorithm be able to learn the feature representations, or does it allow for inputs to be used directly?
d) Are the inputs well represented as sequential or static data?
e) If the inputs are sequential, is it a labelling or classification task?
f) Are there any temporal dependencies on a given timestep?
g) Which training data is available concerning input dimensionality?

FLOW CHART

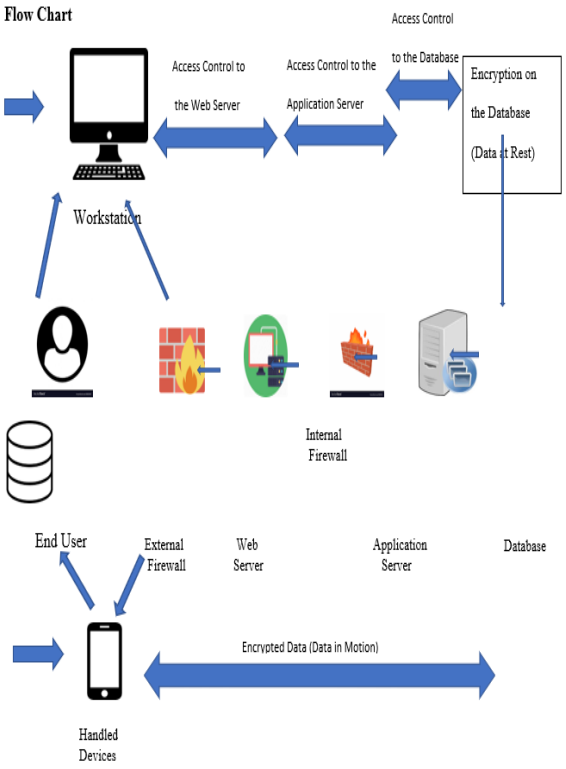

Figure [2.1] Attack-Defense Tree

ANALYSIS

Any individual or organization need to guarantee the security of the computer software and network. Network security to any network bet local or wireless, is very important as it helps in securing the environments of the working processes. Network security consists of several components including firewalls, anti-virus and even anti-spyware to block network invaders to a computer network, identify fast-spreading threats and as well as Intrusion Prevention Systems. Information stored in servers is encrypted to hinder it from being understandable by intruders if by any chance they manage to hack into it. This information can then be decrypted once it reaches the destined location using a decryption key. Firewalls are structured to protect data while being fetched from the servers.

QUANTUM TECHNOLOGY

Despite all the security attacks we are prone to, encryption is the only defensive mechanism we have in place against them. The challenge most people are facing right now is how encryption can be adapted in the whole world to the many connected information systems. An exciting development that must be considered when we take a look in the near future is how this quantum technology is likely to affect the methods to be used in encryption. Quantum computers are likely to be weakened by symmetric encryption. However, it can still be used with longer keys. The current asymmetric encryption algorithms will lose their security. Most of today's e-commerce, certification management and e-identities are based on these asymmetric algorithms. We must follow the development to ensure that these algorithms are replaced before these quantum computers become a reality.

V. CONCLUSION

With the advancing levels of technology in the world, let us try to take a look like ten years into the future and see how IT systems will be like. Cloud systems, IT systems and connected devices have their numbers increasing steadily, which is evidence of the number of connected systems in just a couple years to come. These connected systems generate large volumes of information which must be protected in one way or another. However, not all the information is sensitive to confidentiality but to correctness. We, as users want to have access to reliable information from a specified source.
Information Systems are likely to face the following threats as a result of cybersecurity. Kidnapping our essential information and then encrypting it after which they will demand payment before releasing it. This trend is mainly targeting businesses which have crucial information. Selling the information that has been found by espionage. This includes credit card key details, accounts or passwords and hospitals as well. Espionage can be used when one wants to gain access to very sensitive information. At this juncture, cases of Phishing, whereby a user over the internet sends people false email tricking them into providing their useful information, can hugely be reduced. The information obtained can later be used to gain access to users' personal or organizational data. DDoS, whereby many computers are directed to overload websites and services to block others from being able to use or access them. Intrusion which is mainly aimed at causing specific or general harm to information systems resulting in disinformation. Specific attacks aimed at blocking or hindering part of the information system from normal operations.

List of abbreviations

NSF-National Science Foundation
EDM-Enterprise Data Management
HIPA-Health Insurance Portability and Accountability
UAV-Unmanned Aerial Vehicle
VANET-Vehicular Ad-Hoc Network
MANET-Mobile Ad-Hoc Network
DDoS-Distributed denial-of-service.

KEYWORDS

1. Phishing: This is the actual fraudulent activity of sending emails to computer users purporting to come from reputable companies, with the aim of inducing the users to provide their critical information including Passwords and their Credit card numbers.
2. Trojan: this is a malware software program which can be disguised as being a legitimate software.
3. Espionage: this refers to the act of using spies especially by government to obtain military and political information.
4. Nash equilibrium: refers to a stable state of a system that involves the interaction of participants and that no participant can gain by a unilateral change of strategy if strategies of the other participant remain unchanged.
5. Encryption: refers to information protection technique that encodes the information in such a way that only authorized parties can access it by use of a decryption key.
6. Cloud computing: this is the act of storing, managing and processing information in hosted servers rather than local servers.

REFERENCES

1. Andrae, A. and Edler, T., 2015. On global Security usage of communication technology: trends to 2030. *Challenges*, *6*(1), pp.117-157.
2. Buczak A. L. and Guven E. (2019). *The Evolution of Cyber Insurance*. [online] Cyber Insurance Blog. Available at: https://www.google.com/search?q=cyber+insurance+history&oq=cyber+insurance-his&aqs=chrome.2.69i57j0l5.16226j0j7&sourceid=chrome&ie=UTF-8 [Accessed 11 Aug. 2019].
3. Garg, S. and Singh Aujla, G. (2014). *An Attack Tree that Based Comprehensive Framework for the Risk and Security Assessment of VANET using the Concepts of Game Theory and Fuzzy Logic*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/272798038_An_Attack_Tree_Based_on the Comprehensive_Framework_for_Risk_and_Security_Assessment_of_VANET_using_the_Concepts_of_Game_Theory_and_Fuzzy_Logic [Accessed 8 Aug. 2019].
4. Ismail, N. (2017). *The era of Cyber-attacks: Al's role in cyber insurance*. [online] Information Age. Available at: https://www.information-age.com/era-cyber-attacks-ais-role-cyber-insurance-123469091/ [Accessed 11 Aug. 2019].
5. Kassner, M. (2017). *How game theory and Nash equilibrium can help decide cybersecurity responses*. [online] TechRepublic. Available at: https://www.techrepublic.com/article/how-game-theory-and-nash-equilibrium-can-help-decide-cybersecurity-responses/ [Accessed 11 Aug. 2019].
6. Lindros, K. and Tittel, E. (2016). *Cyber Insurance and reasons why you need it*. [online] CIO United States. Available at: https://www.cio.com/article/3065655/what-is-cyber-insurance-and-why-you-need-it.html [Accessed 11 Aug. 2019].
7. Manz, D. and W. Edgar, T. (2017). *Hypothetico-deducitve Research*. [online] Research Methods for Cyber Security. Available at: https://learning.oreilly.com/library/view/research-methods-for/9780128129302/xhtml/chp009.xhtml [Accessed 11 Aug. 2019].
8. Ponemon, L. (2018). *Calculating and evaluating the Cost of a Data Breach in 2018, the Age of AI and IoT*. [online] Security Intelligence. Available at: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/ [Accessed 10 Aug. 2019].
9. Sadeghi, A.R., Wachsmann, C. and Waidner, M., 2015, June. Privacy and Security challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1-6). IEEE.
10. Safa, N.S., Von Solms, R. and Furnell, S., 2016. Information security policy compliance model in organizations. *computers & security*, *56*, pp.70-82.
11. Song, J., Lee, J., Park, G. and Lee, C. (2013). *An analysis of technical security control requirements for digital I&C systems in nuclear power plants*. [online] Cybersecurity. Available at: https://www.researchgate.net/figure/Data-Flow-Model-of-PPS-for-Cyber-Security-Analysis_fig6_264178211 [Accessed 8 Aug. 2019].
12. Venere, E. (2017). *Game Theory harnessed for Cybersecurity of large-scale nets*. [online] PHYS.ORG. Available at: https://phys.org/news/2017-11-game-theory-harnessed-cybersecurity-large-scale.html [Accessed 11 Aug. 2019].
13. Xu, M. and Hua Asa, L. (2017). *Cybersecurity Insurance: Modeling and Pricing*. 6th ed. Toronto: The Society of Actuaries, pp.7-26. Retrieved from https://www.soa.org/globalassets/assets/Files/Research/Projects/cybersecurity-insurance-report.pdf

AUTHORS PROFILE

Ph.D. in Computer Science and Engineering (Cyber Security)
Certified Information Systems Security Professional- CISSP - (ISC)2
Microsoft Certified Solutions Expert – MCSE - (Microsoft)
Certified Ethical Hacker – CEH- (EC-Council)
Cisco Certified Network Associate (CCNA) – (Cisco)

Computer Hacking Forensic Investigator - CHFI- (EC-Council)
IBM Certified Ecommerce Specialist
ZAP Certified Web Designer
Security+ (CompTIA)
ECSA (EC-Council)
CPSA(CREST)
Memberships:
IEEE, Cisco, EC Council, CompTIA, IBM, Microsoft, CSTA.

Alex's areas of expertise include Cyber Security, Ethical Hacking, Cyber Crimes and Digital Forensics Investigation. He is a Certified Information Systems Security Professional and the founder of several cyber security awareness initiatives in India, Asia, Cyprus and Middle East. With over 20 years' experience of consulting and training has developed a large skill set and certification set. He was instrumental initiating and organizing a number of conferences. He has 100+ publications with IEEE, ACM and Scopus Indexed International Journals. Dr.Alex has received a number of awards including the Best Professor, Best Presenter etc. He is a frequently invited speaker and panelist, reviewer at International conferences related to Cyber Security, Technology, Innovation and education. Alex's profile describes a confident and outgoing individual who enjoys the company of other people. He has a persuasive, open style with others, and develops interpersonal relationships quickly and relatively easily. His levels of self-confidence mean that he rarely doubts his abilities in a social situation, although he may find it a little harder to deal with practical or impersonal situations. Alex's communicative and open style means that he tends to be trusting of others, or at least confide information more readily than many other personality types. Because of his social orientation, however, he finds it rather difficult to deal with rejection by other people, thriving as he does on their positive attention. His current research activities are directed towards Cyber Security, Internet of Things (IoT), Security in Next Generation Networks, Smart Technologies, Cybercrimes Investigations.