Enhancing Cyber Security in the Philippine Academe: A Risk-Based IT Project Assessment Approach

Michael Francis M. Aquino and Marvin I. Noroña
School of Industrial Engineering and Engineering Management
Mapúa University, Manila, Philippines
mfmaquino@mapua.edu.ph, minorona@mapua.edu.ph

Abstract

Cybersecurity devices such as anti-virus, intrusion detection, and prevention system, firewall, network access control, are reactive responses to cyber-attacks because it is based on the known signature. However, security analytics and security information, and event manager are devices, that can gather data about the historical behavior of attacks and correlate it to one another. The significance of this research is to precisely predict if an attack were about to happen, many industries only act if an attack was already happening inside their network or has done significant damages already to the business. This research would significantly help industries, to gain insights on the security events on their network. Artificial Intelligence can instantly predict and suggest if a person can potentially harm based on people's record of good behavior. This can be related to a computer's normal pattern of behavior in the network and once an anomaly happens an unusual behavior can be detected. Hence, the best application of Artificial Intelligence in Cyber Security is to put out a fire before it spread out, preventing data breaches that can cause damages to people's lives and material assets.

Keywords
Cybersecurity, artifical intelligence, data breaches, network access control

1. Introduction

Cybercrimes have a big impact on industries where human lives and properties are at risk, like the banking sector and smart cities (Kehrli, 2017). One perfect example (Kehrli, 2017) is the Bangladesh Bank heist that happened on February 5, 2016, which was almost considered a perfect crime, because of its perfect timing. The hackers launched the virus through phishing email in January 2015, the malware was embedded on the emails, once click by an unsuspecting victim it will rapidly spread on the bank's network, it stayed there for 1 year to gather username and password. The malware also gathered information about the Bank's money transfer system called the SWIFT network. The hackers have ample time to study how the money transfer system works, by falsifying transmission on SWIFT's network. It was February 5, 2016, a long holiday in Bangladesh, when the hackers launched the attack, no one was there to monitor the transaction on the network. 35 transactions were made through the SWIFT network but 30 were blocked in the US Federal Reserve due to suspicion, but 5 transactions were able to go through, 1 in Sri-lanka and 4 in the Philippines. 81Million US dollars were laundered in Philippine casinos (Kehrli, 2017). The lack of law for investigation on money laundered in Casino has indeed helped the success of this crime.

Many types of cybercrimes that are committed by cybercriminals; (Hemraj, Rao, Panda, 2017) classified as crackers that break into other people's computer, bypass passwords and remove a limitation on licenses; hackers that break into systems to steal, change and destroy data; pranksters who play practical jokes or do mischievous act using computers; career criminals, who earn a little and steal a little on their jobs, then find another job and repeat the process; cyber terrorists who use the Internet to promote their ideology and political view. They mainly use the Internet as a propaganda channel to seek terror and chaos; and cyberbullies who harass people through the use of the Internet; and, Salami attackers who do small to bigger attacks, causing a denial of services, bitcoin mining, stealing an unnoticeable amount of money in banks servers.

The phases of a cyber-attack are reconnaissance, scanning, gaining access, maintaining access, and covering tracks (Ayrour, Raji & Nassar, 2018): Cyber attackers follow the sequence of (a) identifying vulnerabilities in the web server using the Internet; (b) Exploiting the system weakness and control devices to download massive information, and using them for illegal purposes; and (c) selling data, proliferating crimes, and terrorism; doing collateral damage to the organization (Bradbury, 2014).

In the academe, Students and Employee records, Business Records, Financial and Intellectual property are always at risk, because of evolving cybersecurity threats. One cybersecurity incident that had occurred on one university in the Philippines is related to a browser add-on, named Gumshoe, which when installed on the browser, collects any keystroke entered while surfing the Internet; are also the credentials entered by the users. In another cyber-crime incident in said university, a hacker has already uploaded a file in the Server, and have posted it on the Internet, to tell the hacking community of the university's loophole. These hacking and vulnerability incidents in the Academe posed a great threat to the education systems to the student's peril.

Artificial Intelligence can be used as a tool to improve the processing and interpretation of data faster, because of its capability to learn and differentiate based on the normal and unusual behavior of the network and the number of hosts attached to it. Academic networks are very vulnerable to attacks that can result in severe damage on employees and students like database are being manipulated by hackers. For example, hackers can edit the student's database compromising the integrity of the system, and students where about are being monitored by hackers, resulting in compromised safety, and invasion of privacy. Previously, other methods to protect a Network are Blockchain Encryption (Sharma & Park, 2018), Intrusion Detection Prevention System (Aloqaily et al., 2019), Big data analytics (Saraladevia, et al., 2015), Software Defined Networks (Rego et al., 2018) and Firewalls (Saraladevia, et al., 2015), Honeypots (Singh, et al., 2019).

The objectives of the study are: 1.) To identify the type and conditions for cyber-attacks in the Academe, and to assess them according to their damage and impact on the digital infrastructure. 2.) To determine and prioritize vulnerability factors that can significantly predict potential cyber-attacks on the academe infrastructure. 3.) To recommend the most effective artificial intelligent system with its integral components, to establish a vulnerability index that will specify priorities and protocols in preempting cyber-attacks and preventing infrastructure damage.

The significance of this research is to precisely predict if an attack were about to happen, many industries only act if an attack was already happening inside their network or has done significant damages already to the business. This research would significantly help industries, to gain insights on the security events on their network.

The scope of the study covers the academe in the Philippines, specifically in selected Universities/Colleges in Metro Manila. Limitations due to data privacy and sharing may be encountered. However, the similarities in the campus network set-up may help in the discussion of important research topics as the focus of this study.

2. Methodology

Cyber-attacks happened when there are weaknesses in people, processes, product/technology, and partner/supplier of an organization. The so-called 4P's of IT service management, as illustrated in figure 2.1. 4P's focus on organizations on critical success factors for a successful ITIL implementation. People's human errors contribute to 90% of cyberattacks, especially when people cut corners on processes. Products/Technology software security bugs are weaknesses in coding and hardware, and Partners unsecured access contributes to cyber-security breach.

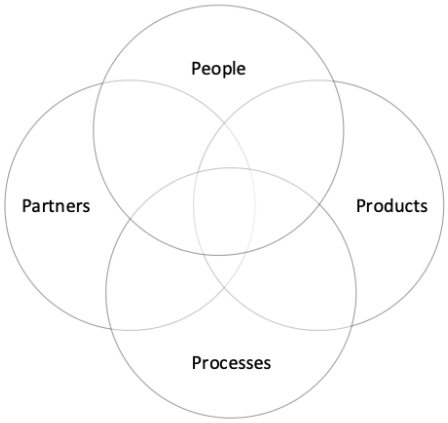

Figure 2.1 4P's of ITSM (ITIL v4, 2019)

2.1 Research Framework

According to Panimalar, Pai, and Khan (2018), artificial intelligence, with its feature of interference detection, can adequately detect zero-day threats before it spreads and attacks the IT service system. This paper takes on this logic that cyber-crimes attack the weakness of the 4P's of IT service management and that artificial intelligence can be a detector and mitigator of cyber-crimes pre-attack, full blown attack, and damage. Thus, the paper will adopt the following conceptual framework as shown in figure 2.1.1.

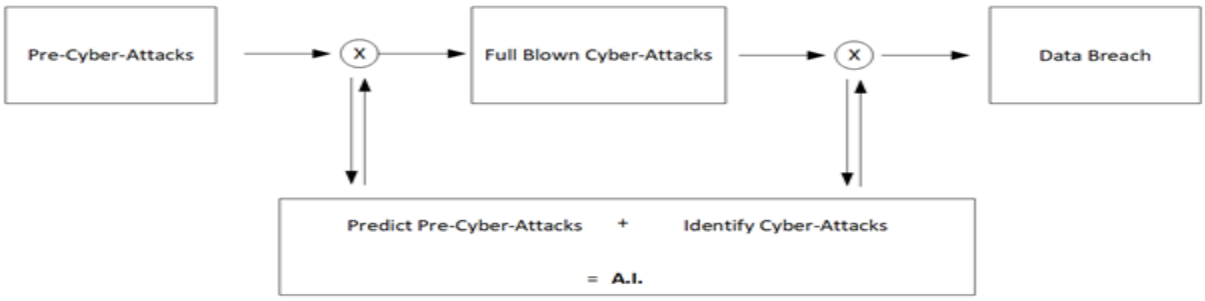

Figure 2.1.1 Conceptual Framework

To effectively predict an attack is going to happen, A.I. must identify what is normal and unusual behavior. The conditions of unusual behavior will be gathered by A.I.; Artificial Intelligence system must Identify, Protect, Detect, Respond, this will aid the human counterpart in analyzing thousands of logs on hundreds of systems 24/7. The Recovery portion will be done manually by people (Mahn ,2018) including reputation build up after the cyber-attack aftermath. Figure 2.1.2 represents the operational framework of A.I. for this study.

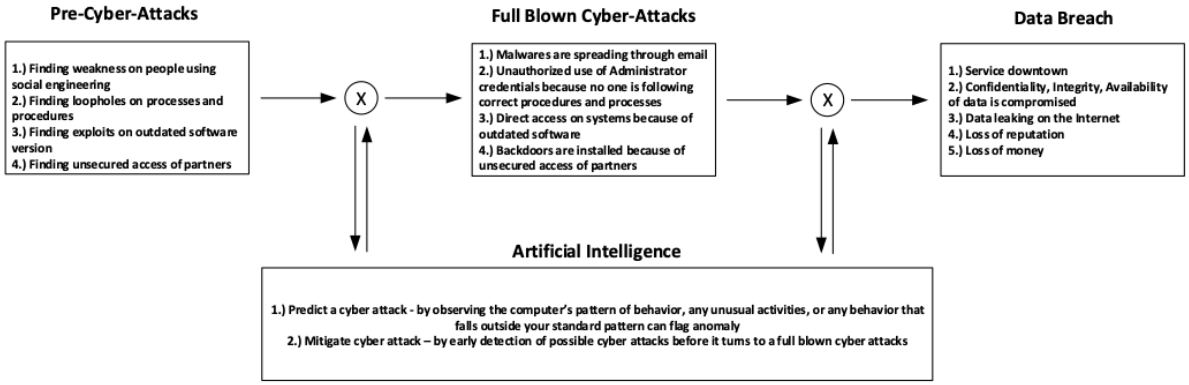

Figure 2.1.2 Operational Framework

2.2 Research Design

Figure 2.2.1 represents the I-P-O diagram which illustrates the first objective of this study. Objective 1 is to identify the type and condition of the cyberattack and assess its damage and impact. The source of the data are computers such as servers, endpoint, IoT devices; the type of quantitative data is an average volume of data flowing, source and destination IP address, source and destination ports, source and destination domain, and time stamp. The software tools to use are Python programming, Wireshark traffic sniffer, Big data Hadoop/Spark, Fireware cloud tools. On the other hand, the analysis tools are, classification for data labeling, regression for prediction, decision trees for supervised learning, and clustering for unsupervised learning as shown in figure 2.2.2.

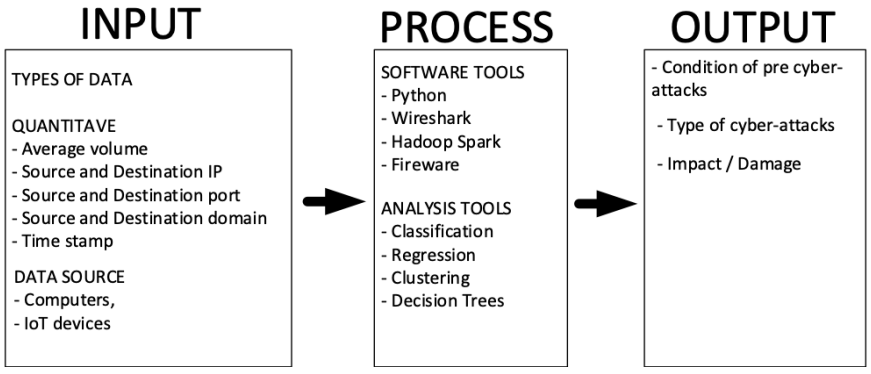

Figure 2.2.1 I-P-O diagram illustrating objective no. 1

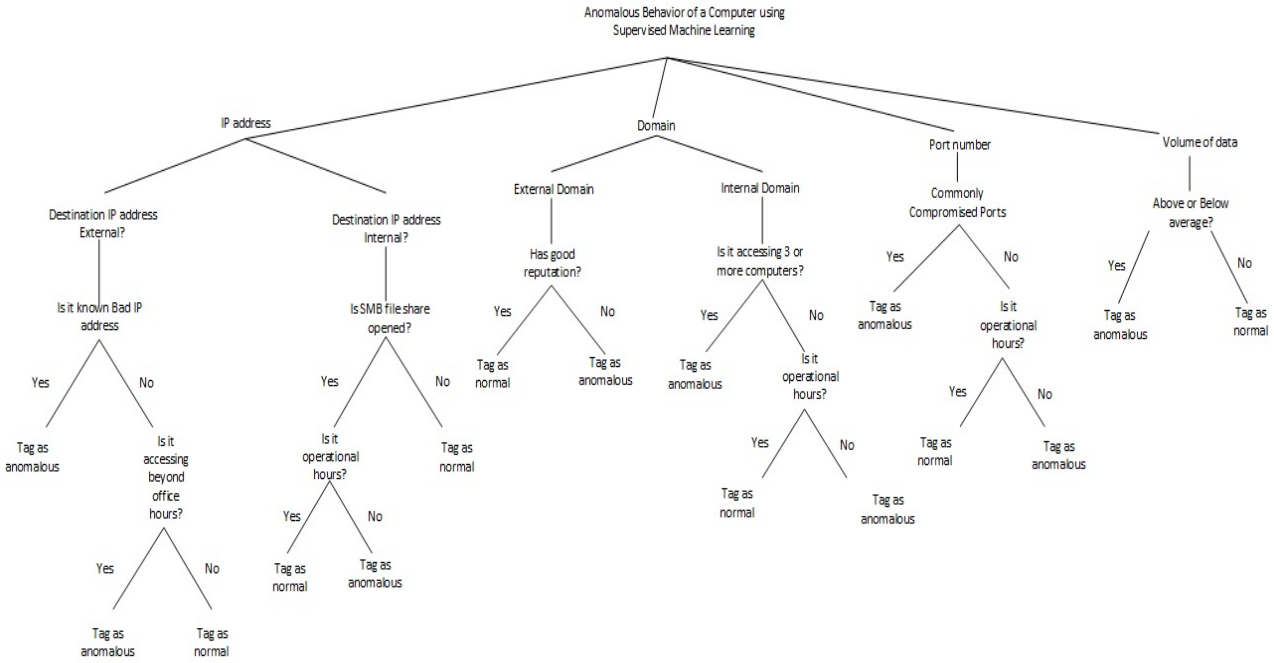

Figure 2.2.2 Classification and Decision Tree Analysis for Supervised Learning

To accomplish objective 2, which is to predict cyber-attack and to determine and prioritize based on the impact of cyber-attack, we scan the suspected computer with OpenVAS scanning software to reveal the software vulnerability of the computer, the software will automatically yield the common vulnerability scoring system. Figure 2.2.3 represents the I-P-O diagram which illustrates the objective 2.

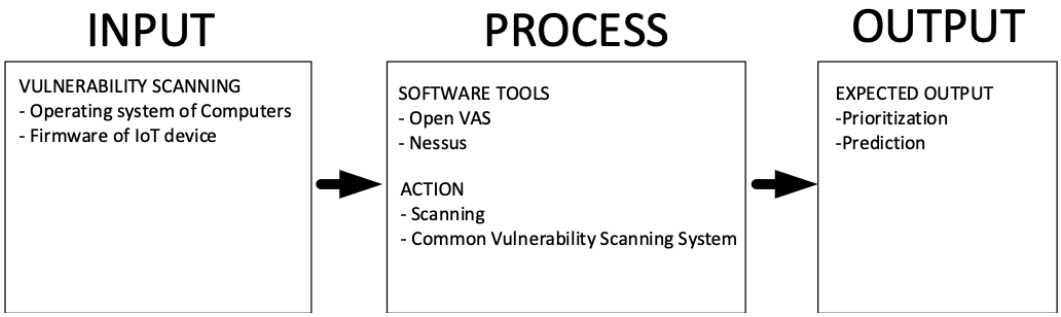

Figure 2.2.3 I-P-O diagram illustrating objective no. 2

By using common vulnerability scoring system, risk priority level can be determined from Critical to Low. Below is the manual computation of CVSS base score:

$$\text{CVSS} = (0.6 * \text{Impact}) + (0.4 * \text{Exploitability}) - 1.5 * \text{f(Impact)}$$

When:

$$\text{Exploitability} = 20 * \text{Access Vector} * \text{Access Complexity} * \text{Authentication}$$
$$\text{Impact} = 10.41 * [1 - (1 - \text{Confidentiality Impact}) * (1 - \text{Availability Impact})]$$
$$\text{f(Impact)} = 0 \; if \; Impact = 0, 1.175 \; otherwise$$

Table 2.2.1 represents the risk priority level that will be based on the computed CVSS base score or the vulnerability factor.

Table 2.2.1 Risk Priority Number

CVSS BASE SCORE OR VULNERABILITY FACTOR	RISK PRIORITY LEVEL
< 4.0	Low
> 4.0 and < 6.0	Medium
> 6.0 and < 10.0	High
10	Critical

Following figure 2.2.4 which represents the I-P-O diagram for objective 3, objective 1 and objective 2 are needed to recommend an effective A.I components, that will prioritize pre-empt cyber-attacks and prevent infrastructure damage.

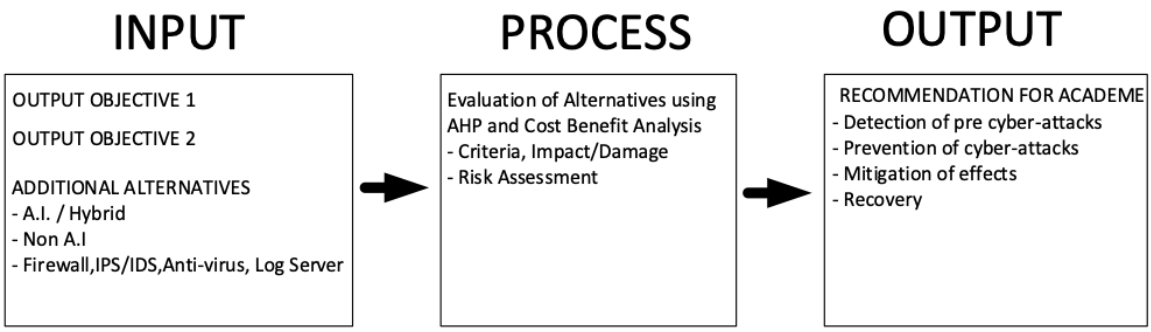

Figure 2.2.4 I-P-O diagram illustrating objective no. 3

Using the analytical hierarchy process as shown in figure 2.2.5, when there are no cyber-attacks, the security insights feature gives an idea of what is the current risk exposure of the whole system. For impending cyber-attacks, (e.g. attacks that are about to happen) the attack prediction feature gathers data, observes, scans for vulnerability, and gives off a recommendation. For onset cyber-attacks (e.g., detection of attacks) that are already happening, identifies what type of attacks are used. For massive attacks or severe attacks, the alternatives can block access to all networks preventing further damage to the system.

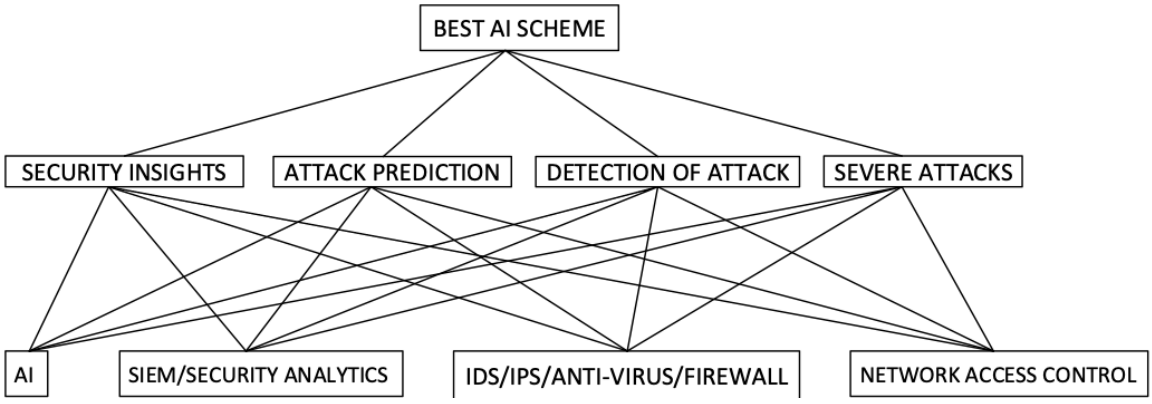

Figure 2.2.5 Analytical Hierarchy Process Model

3. Results and Discussion

The cases below were collected in different businesses as a part of the research in artificial intelligence such as manufacturing, transport, telecommunication, computer, etc., to find the most effective A.I system which can be applied in the field of academe, to prevent and mitigate cyber-attacks using objective 1 and 2.

Case 1: An internal computer device was monitored making regular HTTP connections, over 2,000 has been established to "moonbitcoin[.]cash". A.I. detected that the regular communication to the known crypto mining site has been identified as a beaconing-type pattern. Beaconing activity on the network has been profiled as a potentially malicious behavior in the network with external communication to outside servers, accomplishing objective 1, which is to identify the condition of a cyber-attack.

Moonbitcoin[.]cash has been known to offer free bitcoin in exchange for tasks such as watching ads, captcha completion, playing games. Regular connections to these types of sites have been tagged as a compromised endpoint.

Case 2: A.I have detected several endpoints making an external connection to differentia[.]ru, the website is associated with Andromeda botnet. This behavior is an indication of a widespread infection, accomplishing objective 1, predicting the condition on which a widespread infection is going to happen

Case 3: A.I. has monitored that the internal server has been receiving shared file connection over 39,000 SMB from an external endpoint. Endpoint with a public IP address 114.143.161.182. Normally shared file connection is done internally. External shared access connection is susceptible to man in the middle attack and can exploit the opened port on the endpoint. A.I. recommends verifying the identity of the external endpoint, accomplishing objective 1.

Case 4: A.I. has detected a computer that frequently connects to an external server using HTTP protocol and downloading a malicious executable file. The file was analyzed by A.I. that it contains malicious software that could potentially extract user information or open a backdoor for a hacker to enter the network. The behavior of this single computer has been flagged anomalous as compared to its peer computers, accomplishing objective 1 which is to determine the impact of an onset cyber-attack.

Case 5: A server has received multiple remote management connections from an external endpoint. Exploiting remote management can provide an attacker an initial control to a server once gained access. Exposing remote desktop protocol or RDP to the internet creates a weakness in the network user credentials can be brute-forced by an attacker. The security administrator should check whether the activity is valid, accomplishing objective 1 which is to identify and condition of cyber-attack.

Case 6: An end-user desktop has been observed connecting using the Hola VPN application. VPN services can encrypt the packets and bypass security monitoring and gain access to restricted content. Third-party VPNs are used to leak data from corporate networks. Since Hola is a peer-to-peer VPN, it is susceptible to malicious activity by peered threat actors and can perform Denial of Service without the knowledge of the user. The security team should investigate how did the user be able to install the prohibited software on the computer, accomplishing objective 1 which is an impending cyber-attack.

Case 7: A desktop computer was detected conducting a network scanning activity, resulting in large internal connection attempts. Scanning the network activity is used to gather information about open ports, active host, type of OS, and type of hardware. This type of activity is a prelude to an attack. All network scanning activities are subject to verification, an ordinary end point should not conduct this type of activity and is subject to further investigation, accomplishing objective 1 which is a prelude to a cyber-attack.

Case 8: A.I. has monitored that an internal computer desktop has executed windows remote management on another computer in the network. It was the very first time that the computer has executed this type of service. WinRM is occasionally used by network administrators because it is built internally in windows. Windows remote management has been known to be used by an attacker to move back and forth in the network and disguised as legitimate network administration. Since the behavior was the first time to the end computer, the security team may wish to investigate this activity to ensure that the activity is legitimate accomplishing objective 1 to identify cyber-attack

Case 9: A.I have monitored a large SMB delete request that has been successfully executed. Mass deletion of shared resources has been tagged as anomalous behavior by A.I. and an indication of a breach. A.I. recommends further investigation, accomplishing object 1 which is to assess the impact of cyber-attack.

Case 10: It is common for some IoT devices to connect regularly to servers on the Internet owned by some vendors and manufacturers. To site a few reasons some connections are for software updates, remote support or analytics, etc. A recent discovery has been found that some connect to anomalous servers. One example is a DVD player regularly using HTTP connections to an unregistered external server for updates. If the server were to be compromised the DVD may act as a gateway to the inside network of the company. This will accomplish our objective 1 identifying the condition of a cyber-attack

Case 11: A.I. has detected a Sharp TV making external connections to the Internet using the HTTP protocol. This type of connection is susceptible to man in the middle attacks. Other details revealed the type of manufacturer, mac address, and IP address accomplishing objective 1 identifying the condition of a cyber-attack

Case 12: A.I. has detected an IP security camera making external connections using HTTP protocol that contains a visible username and password. The device was regularly connecting to an external server in China in June 2017 and is associated with NetEase also known as 163.com, a Service provider in China. When attempting to access the server using a browser, the default operational message began to appear. The URL contained local IP, ports, and log details all is visible, accomplishing object 1 identifying the condition of a cyber-attack

3.1 AHP Analysis

By using AHP, we arrived at the following data as shown in table 3.1.1, security insights are the most favorable criteria to achieve objective 1, which is to identify the condition of pre cyber-attacks; Attack prediction achieves objective 2 which is to predict impending attacks; it also covers the severity of attack; Detection of onset attacks achieves objective 1. By combining objective 1 and 2, an effective A.I. system can be achieved which is objective 3.

To achieve objective 3, the following features for A.I are as follows (a)Security insights is a feature that gives an idea on what is the current risk exposure of the whole system (b) Attack prediction is a feature that gathers data, observes, scans for vulnerability, and gives recommendation (c) Detection of attacks are for attacks that are already happening (d) Severe attacks means the system has experience damaged and prompted the system to halt. The following table below was given by 7 people, cyber-security experts. Using the nominal group technique, they arrived at the following criteria, then they arrive at the consensus using force ranking, in creating the best A.I. system with its integral components, achieving objective no. 3.

Table 3.1.1 Comparison Matrix for A.I. Features

ALTERNATIVES	SECURITY INSIGHTS	ATTACK PREDICTION	DETECTION OF ATTACK	SEVERE ATTACK	WEIGHT
AI	1	1	1	1	4
AI + SIEM/SECURITY ANALYTICS	5	3	3	3	14
AI + IDS/IPS/ANTI-VIRUS/FIREWALL	3	5	5	5	18
AI + SIEM/SECURITY ANALYTICS + IDS/IPS/ANTI-VIRUS/FIREWALL	7	7	7	7	28
AI + SIEM/SECURITY ANALYTICS + IDS/IPS/ANTI-VIRUS/FIREWALL + NETWORK ACCESS CONTROL	9	9	9	9	36

Alternatives can be used according to the type of impact to the academe infrastructure and depending on the vulnerability factor, and how it can be prioritized. The vulnerability factor depends on the impact on the CIA triad (e.g. loss of confidentiality, integrity, availability of data). Vulnerability factor increases if each of the CIA triads is affected (ISACA, 2017).

Table 3.1.2 represents the vulnerability favtor and risk prioritization. For single loss of CIA factor (low-risk priority), A.I. only or A.I. with SIEM with built-in security analytics, or A.I. with Firewall with built-in IDS/IPS and Anti-virus can be used to signal for impending Cyber-attack. For dual loss of CIA factor (medium risk priority), A.I. with SIEM and Firewall can be used for heightened alert. For total loss of the CIA triad (high-risk priority) the most effective system is A.I. with built-in SIEM and Firewall and Network Access Control for repair, damage control, and full proof

to cyber-attack achieving objective 3. As A.I. is used now in cybersecurity, it helps identify potential sophisticated cyber-attacks with less involvement of humans (EC-Council, DEC 2019). A.I. will prioritize the high-risk system by detecting malicious behavior on the system, this will prevent attacks from happening, and will enhance the security posture of the Academe

Table 3.1.2 Vulnerability Factor (Index) and Risk Prioritization

ALTERNATIVES	IMPACT	VULNERABILITY FACTOR	RISK PRIORITY LEVEL
AI only or AI + SIEM/SECURITY ANALYTICS or AI + IDS/IPS/ANTI-VIRUS/FIREWALL	Loss of Confidentiality	1	Low
AI only or AI + SIEM/SECURITY ANALYTICS or AI + IDS/IPS/ANTI-VIRUS/FIREWALL	Loss of Integrity	1	Low
AI only or AI + SIEM/SECURITY ANALYTICS or AI + IDS/IPS/ANTI-VIRUS/FIREWALL	Loss of Availability	1	Low
AI + SIEM/SECURITY ANALYTICS + IDS/IPS/ANTI-VIRUS/FIREWALL	Loss of Confidentiality and Integrity	2	Medium
AI + SIEM/SECURITY ANALYTICS + IDS/IPS/ANTI-VIRUS/FIREWALL	Loss of Confidentiality and Availability	2	Medium
AI + SIEM/SECURITY ANALYTICS + IDS/IPS/ANTI-VIRUS/FIREWALL	Loss of Integrity and Availability	2	Medium
AI + SIEM/SECURITY ANALYTICS + IDS/IPS/ANTI-VIRUS/FIREWALL + NETWORK ACCESS CONTROL	Loss of Confidentiality, Integrity and Availability	3	High

The cost of an alternatives depends on how A.I. is mix with different system, the more system is integrated with an A.I. the higher the cost, see table 3.1.3.

Table 3.1.3 Costing for each alternatives

ALTERNATIVES	COST in PHP
AI	1,000,000
AI + SIEM/SECURITY ANALYTICS	3,000,000
AI + IDS/IPS/ANTI-VIRUS/FIREWALL	3,500,000
AI + SIEM/SECURITY ANALYTICS + IDS/IPS/ANTI-VIRUS/FIREWALL	4,000,000
AI + SIEM/SECURITY ANALYTICS + IDS/IPS/ANTI-VIRUS/FIREWALL + NETWORK ACCESS CONTROL	12,000,000

3.2 Information Risk Assessment of Critical System for Academe

Table 3.2.1 represents the summary of critical, essential, and non-essential systems for the academe. A list of a critical system is enumerated; 1.) Student data; 2.) Employee data; 3.) Enrollment system; 4.) Payment transaction system; 5.) Billing system; 6.) Treasury system; 7.) Financial system; 8.) Payroll system; 9.) Grades encoding and 10.) Backup.

Essential systems such as 1.) Communication Tools; 2.) HRIS system; 3.) Security in and out system; 4.) Laptops and Computers 5.) Online classroom and laboratory are said to have impacts of interruptions are significant, and short durations are acceptable.

Non-essential systems are as follows 1.) Library system; 2.) Health e-system impacts of interruptions are tolerable for these systems, and long durations are acceptable.

Table 3.2.1 Critical, Essential, and Non-Essential Systems

ASSET CATEGORY	DIGITAL ASSET	ASSET OWNER	LOCATION
Critical	Enrollment System(Online Enrollment)	DEV,SYS AD	Datacenter
	Payment Transaction System	DEV,SYS AD	Datacenter
	Billing System (Online Payment)	DEV,SYS AD	Datacenter
	Treasury System	DEV,SYS AD	Datacenter
	Financial System	DEV,SYS AD	Datacenter
	Payroll System	DEV,SYS AD	Datacenter
	Grades Encoding	DEV,SYS AD	Datacenter
	Student (Customer) Data	DEV,SYS AD	Datacenter
	Employee Faculty Data	DEV,SYS AD	Datacenter
	Backups	DEV,SYS AD	Datacenter
Essential	Communication Tools	SYS AD and NET AD	Datacenter
	HRIS	DEV,SYS AD	Datacenter
	Security In/Out System	SECURITY	Gate
	Network Devices	NET AD	Datacenter
	Employee / Student Attendance	DEV,SYS AD	Datacenter
	Laptops and Computers	RESOURCE	Datacenter
	Online Classroom	ACADEMIC	Cloud
	Online Laboratory	ACADEMIC	Cloud
Non Essential	Library system	LIBRARY	Datacenter
	Health-e System	DEV,SYS AD	Datacenter

Critical hardware systems where the data reside are as follows 1.) Active Directory; 2.) Domain Name Service; 3.) Web server; 4.) Database server; 5.) In-house application server and 6.) File storage server they are all contained in the NUTANIX server.

Essential tools were identified as follows 1.) Email; 2.) Instant messaging; 3.) Web conference; 4.) Mobile; 5.) Landline telephones.

To identify the potential risk for these systems, vulnerability for these systems should be scanned by an open-source scanner and known threats were identified. Once the potential risk is identified, the likelihood of these threats and their impact on the academe field should be rated. A risk matrix is used to identify the risk rating as shown in table 3.2.2, once rated the risk with the highest rating are prioritized.

Table 3.2.1 Risk Matrix

THREAT	VULNERABILITY	POTENTIAL RISK	LIKELIHOOD	IMPACT	RISK RATING	RISK RESPONSE	CONTROL IN PLACE	PEOPLE	PROCESS	TECHNOLOGY	LEVEL OF PROTECTION
NATURAL DISASTER											
Earthquake	Philippines is situated in the ring of fire	Datacenter destruction	Low	High	Medium	Transfer	Strong Infrastructure			Yes	1
Fire	The university is situated in congested area	Datacenter destruction	Low	High	Medium	Transfer	Fire suppression			Yes	1
Flood	The university is near Manila Bay	Datacenter destruction	Medium	High	High	Transfer	Higher floor location		Yes		1
Storm Surge	The university is near Manila Bay	Datacenter destruction	Low	High	Medium	Transfer	Higher floor location		Yes		1
Tsunami	The university is near Manila Bay	Datacenter destruction	Low	High	Medium	Transfer	Higher floor location		Yes		1
Typhoon	Philippines is located in the Pacific	Datacenter destruction	High	High	High	Avoid	Higher floor location		Yes		1
Astronomical phenomenon	N/A	Datacenter destruction	Low	High	Medium	Transfer	None				0
Vulcanic Eruptions	Philippines has 7.33 % of active volcanoes	Datacenter destruction	Low	High	Medium	Transfer	Far away location		Yes		1
Man-made disaster	N/A	Datacenter destruction	Low	High	Medium	Transfer	None				
MAN MADE											
Civil disorder	Philippines has rebels	Can't go to site	High	Medium	High	Avoid	Back up location		Yes	Yes	2
Labor Dispute	Philippines has labor	Can't go to site	low	Medium	Low	Accept	Back up location		Yes	Yes	2
World War	Philippines has low level of military protection	Datacenter destruction	low	High	Medium	Reduce	Back up location		Yes	Yes	2
Terrorism	Philippines has high number of terrorist attacks	Datacenter destruction	High	High	High	Avoid	Back up location		Yes	Yes	2
Activism	Philippine has a high number of activist	Can't go to site	High	Low	Medium	Reduce	Back up location		Yes	Yes	2
POWER INTERRUPTION											
Water depletion	Philippines suffer water shortage during summer	No power in the datacenter	Medium	High	High	Avoid	UPS and back up generator			Yes	1
Sabotage	Power lines are still using poles which are susceptible thieves, and weather disruption	No power in the datacenter	Low	High	Medium	Avoid	UPS and back up generator			Yes	1
Due to Natural Disaster	Philippines has typhoons, earthquake that can cause power disruptions	No power in the datacenter	High	High	High	Avoid	UPS and back up generator			Yes	1
TELCO DOWNTIME											
Fiber cut	Government and privately owned telco's are not coordinated to each other	access the services inside the data	High	Medium	High	Avoid	Redundant Telco			Yes	1
Labor problems	Philippines has contractuals which are susceptible to labor problems	support from Telco during downti	High	Medium	High	Avoid	Redundant Telco			Yes	1
Merging of business	Philippines has two only two major competitors	Telco services are not improved	Low	Low	Low	Accept	Redundant Telco			Yes	1
PANDEMIC											
COVID 19		Can't go to site	Medium	High	High	Avoid	Remote Access			Yes	1
Spanish flu	Health insurance is fair	Can't go to site	Medium	High	High	Avoid	Remote Access			Yes	1
LAWS AND REGULATION											
Data privacy law	N/A	Penalty if no compliance	Medium	Medium	Medium	Avoid	Compliance	Yes	Yes		2
GLOBAL ECONOMY											
Degrading market condition	Going down economy has an effect on parents income	ible support problems from suppl	Low	Medium	Low	Accept	Student loans		Yes		1
Decreasing Economy	Possible recession	No support engineer available	Low	Medium	Low	Accept	Student loans		Yes		1
HARDWARE FAILURE											
End of support devices	Some network devices such as access switches have no warranty	Network downtime service	Medium	Low	Low	Accept	Warranty		Yes		1
IT RISK (TECHNICAL)											
External Cyber Attack											
Malware	The university uses Windows operating system	Operational issues	High	High	High	Avoid	Firewall, Anti-virus,NAC		Yes	Yes	2
Phishing	The university hasn't conducted full awareness program yet	Data breach	High	High	High	Avoid	Firewall, Anti-virus, Training	Yes	Yes	Yes	3
DDos attacks	Routers has no intrusion prevention	Service denial	High	High	High	Avoid	Firewall, Anti-virus		Yes	Yes	2
Drive-by attack(planting of scripts, then redirect to)	The university didn't have Web Application Firewall	Service denial	Medium	Low	Low	Accept	Firewall, Anti-virus		Yes	Yes	2
Password attack(Sniffers,social engineering,key logger)	The use of old password is still in effect	Data breach	Medium	High	High	Avoid	Firewall, Anti-virus		Yes	Yes	2
SQL injection	No code review yet and no databases are not frequently done	Data leak	Medium	High	High	Avoid	None				0
Cross site scripting (XSS) attack	No code review yet	Data leak	Medium	High	High	Avoid	None				0
Reconaissance Attack	No pentest yet are conducted on the firewall and routers don't have IPS	Possible bigger attacks	High	Low	Medium	Reduce	Firewall			Yes	1
Spam	Some employees have no awareness training	Service denial	Medium	Low	Low	Accept	Anti-Spam			Yes	1
Remote code execution	No dedicated IT personnel to monitor this type of attack	Operational issues	Medium	High	High	Avoid	Anti-virus			Yes	1
Web shell attack	No code review yet	Operational issues	Medium	Low	Low	Accept	None				0
Sim hacking	Some employees have no awareness training	Operational issues	Medium	Low	Low	Accept	None				0
Ssh attack	No equipment to monitor SSH attack on the network and servers	Operational issues	High	Medium	High	Avoid	Firewall			Yes	1
Internal Cyber Attack											
Eavesdropping attack	Network access control is not yet fully implemented	Data leak	Low	High	Medium	Reduce	None				0
Data leakage	DLP is not implemented	Data leak	Medium	High	High	Avoid	None				0
Man in the middle	No equipment to monitor man in the middle attack	Data leak	Low	High	Medium	Reduce	None				0
Reconaissance Attack	No equipment to monitor recoinassance attack	Possible bigger attacks	High	Low	Medium	Reduce	Firewall			Yes	1
Unauthorized configuration changes	No equipment to monitor configuration changes	Operational issues	High	High	High	Avoid	Change Management	Yes	Yes		2
Account sharing	No equipment to monitor multiple login of credentials	etermine who is the cause of the p	Medium	Medium	Medium	Reduce	Audit	Yes	Yes		2
Key logger	No inventory for software installed on the PCs	Unauthorized access	Low	High	Medium	Reduce	None				0
Screen grabber	No equipment to monitor network activity of the users	Privacy issues	Low	High	Medium	Reduce	None				0
Command and Control	No equipment to monitor connections and dedicated IT staff	Unauthorized access	Low	High	Medium	Reduce	Anti-virus			Yes	1
Crypto Mining	Servers are prone due to untested anti-virus	Slow resources	High	Medium	High	Avoid	Anti-virus			Yes	1
Fraud and scams	Some employees have no awareness training	an give up confidential informatio	High	Medium	High	Avoid	Audit		Yes		1
Proxy Bypass	No dedicated IT personnel to monitor this type of attack	No online protection	High	Low	Medium	Reduce	Firewall			Yes	1
Zero day	No sandboxing was implemented on the network	Data corruption	High	Medium	High	Avoid	None				0
Fake antivirus	NAC was not yet implemented on the network that would force users to have anti-malware	Operational issues	Low	Low	Low		Anti-virus			Yes	1
Credit card cloning	No work place inspection and bag inspection while entering the campus	Financial and Reputational loss	Low	High	Medium	Reduce	CCTV			Yes	1
Plain text attack	Encryption are not yet implemented by the university	Privacy issues	Low	Low	Low	Accept	None				0
Black mail, Prank calls	The university hasn't conducted full awareness program yet	Operational issues	Medium	High	High	Avoid	Awareness training	Yes			1
Active X	The university is still using Windows xp	Operational issues	Low	Low	Low	Accept	Anti-virus			Yes	1
Javascript	No web application firewall installed yet	Operational issues	Low	Low	Low	Accept	Anti-virus			Yes	1
Plugins for browsers	No visibilty was implemented for this type of attack	Compromised credentials	High	High	High	Avoid	Disable feature, Per request			Yes	1
Popups	Windows operating system are used by the university	Operational issues	High	Low	Medium	Reduce	Anti-virus			Yes	1
Drive-by download	Windows operating system are used by the university	Operational issues	Low	Low	Low	Accept	Anti-virus			Yes	1
Cross-site request forgery	The university hasn't conducted full awareness program yet	Financial loss	Low	Medium	Low	Accept	Firewall			Yes	1
Unvalidated redirects and forwards	Browsers doesn't have plugin for antivirus	Operational issues	Low	Low	Low	Accept	Firewall			Yes	1
Insecure direct object references	No code review yet	Operational issues	Low	Low	Low	Accept	Firewall			Yes	1
Malicious Apps	Some users know the administrator password for the computers, infrequent changed of credential passwords	Data leak	High	High	High	Avoid	Username and Password			Yes	1
Side channel attacks	Wireless network is not monitored due to large number of users	Operational issues	Low	Low	Low	Accept	None				0
Power glitch attacks	No maintenance testing for UPS in the data center	Data corruption	Low	Low	Low	Accept	UPS and back up generator			Yes	1
URL Link attacks	Browsers doesn't have plugin for antivirus	Operational issues	Low	Low	Low	Accept	Firewall, Anti-virus			Yes	1
Rootkit	Use of old computers sre still used in the university which prevent frequent antivirus scan	Data breach	Low	Low	Low	Accept	Anti-virus			Yes	1
Disgruntled Employee	No survey and assestment was done on the university regarding employee hapiness	Data loss and leakage	High	High	High	Avoid	CCTV			Yes	1
Unchange default configuration	use of hubs are still used in the university	Network infiltration	High	Low	Medium	Reduce	None				0
Permanent denial of service (Hardware)	No regular patching is done	Service denial	Low	High	Medium	Reduce	None				0
Cyber bullying	No clear process handling for this incident	Unhappy customers	High	Low	Medium	Reduce	None				0
Stolen password	No dedicated IT personnel to monitor password login	Unauthorized access	Medium	High	High	Avoid	None				0
Bluetooth enabled device attack	NAC is not yet fully implemented	Unauthorized access	Low	Low	Low	Reduce	None				0
Rogue Access Points	No pentest yet done on Wireless network	Service denial	Low	Low	Low	Reduce	Meraki clean air			Yes	1
Session Hijacking	Browsers doesn't plugin antivirus	Financial loss	Low	Low	Low	Reduce	Firewall			Yes	1
Third party access to devices	No dedicated IT personnel to monitor access to equipment during time off and holidays	Data breach	High	Medium	High	Avoid	Timed access		Yes	Yes	1
Servers not located in the datacenter	test servers that are not officially used in productions are in different location	Data loss	High	Medium	High	Avoid	None				0
Staffing issue	Some positions in DO-IT are still vacant	Downtime	High	Medium	High	Avoid	None				

3.3 Critical Success Factor

The critical success of this project are the following; 1.) Hiring of skilled Programmers, Data Scientist, and Cybersecurity experts; 2.) Budget allocation for high end computer hardware; 3.) Identification of critical systems to be monitored; 4.) Correlation and Risk exposure assessment algorithm; 5.) Penetration testing of system

3.4 Project Requirements

The academe field will have its operation conducted off-premises in cases of an event of a disaster. The service needed in cases where no one can go to school is to setup a virtual classroom, virtual laboratory, virtual computers, enrollment applications, billing applications, payroll applications, student records and back up, using open-source software.

The purpose of the project is to secure the operation of these online facilities. Such that the academe business can continue its operation during disaster times. The scope of the project is for the IT part of the organization. The technological challenge of this is to identify false positive alarms, sort out thousands of logs every day, and the appropriate action for each type of cyber-attacks.

3.5 Project Roadmap

Figure 3.5.1 represents the project roadmap of this study. Phase 1 assembling a team of skilled cyber-security professionals, data scientist, and computer programmers; collaboration, discussion on strategic plans, critical success factors, and implementation to attain objective and goals; Phase 2, the cyber-security professionals will conduct a risk assessment on people, processes, technology and IT assets, prioritization of risk according to impact and likelihood and assess the current security exposure of the system; Phase 3, a data scientist will formulate a strategy on how the A.I. system can learn, predict attacks and decide based on mathematical equations and formulas; Phase 4, computer programmers will devise an algorithm and create computer codes for machine learning equations; Phase 5, cyber-security professional will conduct a simulated cyber-security attack such as hacking the system; Phase 6, all team members will collaborate to evaluate the A.I. system has successfully and accurately predicted an attack.

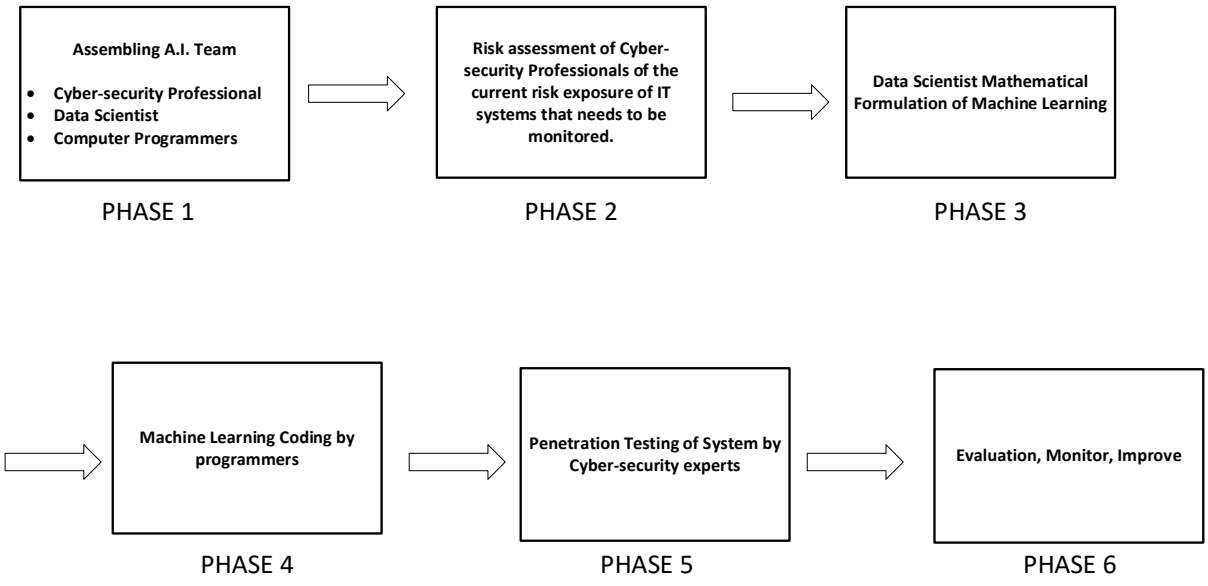

Figure 3.5.1 Project Roadmap

4. Conclusion

Cybersecurity devices such as anti-virus, intrusion detection, and prevention system, firewall, network access control, are reactive responses to cyber-attacks because it is based on the known signature. However, security analytics and security information, and event manager are devices, that can gather data about the historical behavior of attacks and correlate it to one another. To answer the research question, "what can effectively detect emerging cyber-attacks, and prevent them from happening"?

The answer is the use of vulnerability index, which considers cost, risk, features and the different cases of cyber-attacks, coming up with vulnerability index that was formulated using risk assessment, nominal group techniques, with the corresponding configuration, from options 1 to 4 it can pre-empt cyber-attacks to avoid infrastructure damage. The vulnerability index, serves as a basis on how A.I. will treat the system, the higher the risk, based on the weakness of the system; The higher the safeguards are placed on the system with high vulnerability, this will be the basis for the decision making of the A.I. application. In return, enhancing the cyber-security in the Philippine Academe.

Artificial Intelligence can give suggestions which accomplish objective 1; identifying the type and conditions of cyber-attacks, and learn based on historical data which is objective 2; to predict emerging cyber-attack, the more data it has, the better it becomes. A.I. can sort out thousands of logs prioritizing the most severe threat, according to the vulnerability index of the system, preventing infrastructure damage accomplish objective 3.

5. Recommendation

Artificial Intelligence is a great tool to help humans do their jobs efficiently and effectively. It can help humans in decision-making with augmented reality, especially in situations that go beyond human capabilities, such as sorting through thousands of security event logs that were generated by various systems and network devices daily. Sorting through and correlating all security events logs are cumbersome and very time-consuming. Before deciding to act upon a cyber-attack can be too late, because the attacker has already infiltrated the network and created damages before noticing it. Being proactive and making quick decisions based on A.I. findings, is the key to prevent cybersecurity incidents from happening. If in case, all cyber-security measure fails for people, process and technology, business continuity and disaster recovery plan should always be included in the organization, as the last resort for the business to survive during negative events.

Artificial Intelligence behavior analytics can be used primarily in premises security, malicious behavior can be monitored in airports, concerts, public gatherings, etc. In recent years the interest to improve the reliability of deception and hostile intentions detection techniques is related to the need of increasing the safety of citizens threatened with terrorist attacks. In particular, the Philippines government through its security agencies is looking for and financing research on modern lie detection techniques. There are different opinions on whether we can determine who is planning a hostile act merely by observing behavior. Some researchers are convinced that scientific methods of detecting hostile intentions, among others by detecting deception, can help to catch a terrorist and provide security.

In China, a giant screen displays the faces of pedestrians who dared to jaywalk, unaware they were being watched. But it wasn't police who caught them, it was street-side surveillance cameras equipped with the latest in facial recognition technology. For China's government, that means not only being able to identify any of its 1.4 billion citizens within a matter of seconds but also having the ability to record an individual's behavior to predict who might become a threat.

Artificial Intelligence can instantly predict and suggest if a person can potentially harm based on people's record of good behavior. This can be related to a computer's normal pattern of behavior in the network and once an anomaly happens an unusual behavior can be detected. Hence, the best application of Artificial Intelligence in Cyber Security is to put out a fire before it spread out, preventing data breaches that can cause damages to people's lives and material assets.

References

Albert Rego a, Laura Garcia a, Sandra Sendra a,b, Jaime Lloret a,*, 2018. Software Defined Network-based control system for an efficient traffic management for emergency situations in smart cities, Spain. Retrieve from: https://www.sciencedirect.com/science/article/pii/S0167739X17330364

Amy Mahn, 2014. Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework, USA. Retrieve from: https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework

Arockia Panimalar, Giri Pai, Salman Khan, March 2018. Artificial Intelligence techniques for Cyber Security,India. Retrieved from: https://www.academia.edu/36827589/ARTIFICIAL_INTELLIGENCE_TECHNIQUES_FOR_CYBER_SECUSECU

Danny Bradbury, 2014. Unveiling the dark web, Canada. Retrieve from: https://www.sciencedirect.com/science/article/pii/S135348581470042X

EC-Council, Dec 2019, The role of A.I. in Cyber-security. Retrieved from website: https://blog.eccouncil.org/the-role-of-ai-in-cybersecurity/

Hemraj Saini,Yerra Shankar Rao,T.C.Panda, April, 2012. Cyber-Crimes and their Impacts India, Retrieve from: https://www.researchgate.net/publication/241689554_Cyber-Crimes_and_their_Impacts_A_Review

ISACA, May 2018, IT Asset Valuation, Risk Assessment and Control Implementation Model. Retrieved from website: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model

Jerome Kehrli, November 15, 2017. Deciphering the Bangladesh bank heist. Switzerland, Retrieved from: https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist

Moayad Aloqaily a., Safa Otoum b., Ismaeel Al Ridhawi b., Yaser Jararweh, 2019. An intrusion detection system for connected vehicles in smart cities,UAE/CANADA/JORDAN. Retrieve from https://www.sciencedirect.com/science/article/pii/S1570870519301131

Pradip Kumar Sharma, Jong Hyuk Park, 2018. Blockchain based hybrid network architecture for the smart city. Korea retrieve from: https://www.sciencedirect.com/science/article/pii/S0167739X1830431X

Singh, Dhara, 24 June 2019. Raspberry Pi hack puts NASA in security jam, n.d, retrieve from: https://www.cnet.com/news/raspberry-pi-hack-puts-nasa-in-security-jam/

Yassine Ayrour, Amine Raji and Mahmoud Nassar,March 2018. Modelling Cyber Attacks a survey study, France. Retrieved from: https://www.sciencedirect.com/science/article/pii/S1353485818300254

Biographies

Michael Francis Aquino is a holder of BS Electronics and Communication Engineering and MS Engineering Management degrees, working as a network administrator in Mapua University, Philippines. Research interests include electronics design and microcontroller programming, network reliability and stability, and cyber-security.

Marvin Noroña is the Managing Partner and Senior Consultant of the Socio-Economic and Empowerment Development Solutions (SEEDS), Inc. and currently a faculty at the Mapua University School of Industrial Engineering & Engineering Management and School of Graduate Studies. He earned his BS Industrial Engineering and MBA degrees from University of the Philippines and is a Doctor in Business Administration candidate finishing his thesis in lean and green manufacturing. His research interests are in the areas of sustainability, supply & operations management, production & service systems improvement, strategic planning and management, lean six sigma, and design thinking.