Information Systems Security Incident Response: Systematic or Ad-hoc Approach to Act

Ramin Heidari Khabbaz
(40105992)

Behnam Panjehpour
(40119593)

Yunus Emre Aydar
(4011041)

Mohammad Moazzem Hossein Khan
(40104656)

Md Sadikur Rahman Naiem
(40106537)

***Abstract*— Nowadays, we see that IT units which, are housed by various companies go through different security gaps. These security gaps are based on reasons such as the behavior of employees in companies or the weakness of the designed security system. Regardless of the cause of security breaches and vulnerabilities in any system, preparing a critical plan will help to circumvent any incident. Incident handling and response play a major role in restoring system in minimal damage during any type of cyber-attack and help companies to maintain their business without losing their global reputation in the business world.**

Incident handling and response planning involve several steps, which are preparation, detection and analysis, containment, eradication, and recovery, and post-incident activity. The goal of the incident response and handling are introduced as protecting organization, conforming with federal and local laws, reducing harmful effects that caused to public, and protecting the confidential and private information of customers.

***Keywords* – Incident Response, Incident Handling, Cyber Attacks**

I. INTRODUCTION

Nowadays by the expansion of the digital world and the power of the Internet and computer networks, regardless, how we can access everything from everywhere, or how we can process our information so fast at any time, our information becomes more vulnerable than before the digital world. There are two specific terms “Hack” and “Cyber Attack” which IT professionals and security analysts are faced with them. The cyber-attack means that attacker intends to steal information, change data or disrupt operation functions. The main purpose of both security analysis and IT security teams are protecting information and help business continuity against cyber-attacks which is called Incident Response (IR). The successful incident response needs strategy and plan by which Computer Incident Response Team (CIRT) can handle the incident step-by-step and then ensure that the same cyber-attack cannot happen again. This plan should include goals, roles and responsibilities, how to analyze and triage events, and the requirements for escalation. In other words, without having a plan, most of the times IR teams cannot respond efficacy to the attacks [1].

The goals of the incident response can be as followed:

1) Protecting an organization’s assets, information and the activities of the organization
2) Conformity with federal and local laws
3) Reduce the harmful effect of the public
4) Protect customer’s confidentiality and privacy information [1].

To achieve these goals, the National Institute of Standards and Technology (NIST) provides four phases for incident handling in NIST 800-61 Revision 2 document. These phases are Preparation, Detection, and Analysis, Containment Eradication, and Recovery, Post-Incident Activity [2]. The organizations should establish a Computer Incident Response Team (CIRT) to use incident response plan for stopping the attacks or at least mitigating the effects of attack and then recover the system [1]. It is important that all team members know their roles and responsibility.

The type of emergency action is related to the type of attack vectors. For example, the proper emergency actions for stopping ransomware and then recovering the system from attack is different from the actions for the Man-In-The-Middle attack. It means the incident response team should know various attack vectors like attacks from the web, emails, removable devices [3].

This paper focuses on emergency actions after hacking and how the IR team can recover the system based on some known attacks. In the second section of this paper, we explain the incident handling phases based on NIST 800-61 documentation (Systematic Approach). In the third section, security incident response to some attacks (Both Systematic and Ad-hoc Approach) on related works are summarized and compared. In the fourth section, we raise our controversial statement and discuss about it. The last section concludes the materials covered in this paper.

II. BACKGROUND

The emergency actions after hacking are called Incident Response (IR), which means what kinds of actions should Computer Incident Response Team (CIRT) do during an incident lifecycle. The Incident Handling and Response process follows an incident throughout its lifecycle, from the declaration to the closure [3]. This process consists of several steps with high-level goals within each step, as shown in Figure1.

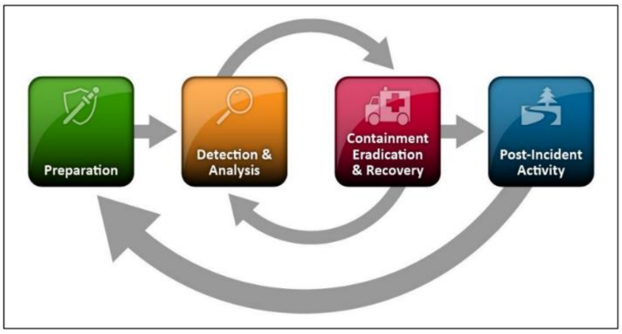


Fig.1 Incident Response Life Cycle [2]

1. **Preparation:** The incident response (IR) team should prepare some valuable tools and resources for a successful incident response handling process.

    a. **Incident Handler Communications and Facilities:** Includes the contact information of IR team members for emergency cases. For example, emails, primary and secondary phone numbers, and secure instant messaging id. Specific tracking system for incidents and secure storage for keeping the reports, log, and incident reports.

    b. **Incident Analysis Hardware and Software**: Includes software, hardware, and accessories that are useful for incident analysis. For example, a bag which contains a laptop with forensic tools, all trusted image of OS, a packet sniffer tools, blank CD and DVDs, external DVD-ROM.

    c. **Incident Analysis Resources:** A list of essential network resources and documents such as standard port numbers, network map diagram, and network schematic diagram, list of available services with their descriptions, and the hash of critical executable files which can speed up the process of incident analysis.

    d. **Incident Mitigation Software:** Access to all recovery options such as clean operating system images, backup tools, and backed up files [2].

2. **Detection and Analysis**: Determine the extent of compromise; In this step, the events should be gathered from various devices and software like firewall, antivirus software, and IDS to ensure that it is an incident. In some cases, an incident can detect by regular users and report to the IT department. For example, the user can report unexpected system behavior after connecting a USB drive to his/her computer. Before moving to the next step, all evidence related to the event should be documented by the CIRT team [2].

It is impossible to create a step-by-step guideline for each kind of attack since they are changed day-to-day, and the method of handling is different each time. However, we can categorize the incidents based on frequent attack vectors and then start the detecting phase. Common attack vectors are:

    a. **External / Removable Media:** This attack use removable devices like USB disk to autorun a malware or a Trojan behind an execution file.

    b. **Attrition:** This attack try to gain credential of services and network devices by brute force methods.

    c. **Web:** These attack targets are websites and web applications by trying to perform SQL injection or XSS (Cross-Site-Scripting).

    d. **Email:** This attack uses email service and put an infected file as an attachment. For example, most of the ransomware attacks use this method to infecting the system.

    e. **Impersonation:** This attack perform by masquerading a network device or service or one of the personnel to access to the sensitive information. For instance, a Man-in-The-Middle (MITM) attack by implementing a rogue WiFi network and capture the traffic [2].

3. **Containment, Eradication, and Recovery:**

    a. **Containment:** Limit the spread of compromise; The primary goal of this step is minimizing the damage of an attack and try to stop it. This step has three phases which should mitigate the attack and then collect the vital evidence for future prosecution if needed [2].

i. **Short-Term Containment:** Limiting the damage of an attack as soon as possible is the main purpose of this phase. For instance, isolate the compromised computer from the network or put the infected PC into the sleep mode to prevent propagating the malware.

ii. **System Backup:** In this phase, it is essential to take a backup from a compromised computer for forensic analyses with specific forensic tools such as Forensic Tool Kit (FTK) before wiping the computer disk and installing the new operating system. This backup can help to determine how the incident happened on a computer, which can be useful for lessons learned Steps.

iii. **Long-Term Containment:** The vital purpose of this phase is to back the infected system temporary to the production cycle after removing the malware and its effects, removing accounts that were created by the attacker, and installing security patches to the system.

b. **Eradications:** Remove artifacts of compromise and prevent future compromise; In this step, the malicious files and contents must be removed from the affected system entirely. The removal steps should be done correctly to ensure that the system cannot be compromised again. For example, format the hard drive bit by bit, install the trusted image of an operating system, install all critical security patches, disable unnecessary services and accounts, install antivirus with anti-malware engine detection to ensure that the malware is removed completely [2].

c. **Recovery:** Return assets to the operational-ready state; In this step, the affected system will be back to the production environment, and then it should be monitored carefully to ensure it will not compromise due to the same problem. It is essential how to monitor anomaly behavior and test the system to ensure that it is clean and fully operational [2].

4. **Post-Incident Activity:** Improve future security posture by learning from previous experiences; In the lessons learned step all documentation should be completed comprehensively and can answer all questions related to the incident like Who, What, Where, Why, and so on. The primary goal of this step is learning from the incident and preventing from happening again [2].

III. RELATED WORK

We present a summary of related work articles that are related to emergency actions after hacking and incident response. The articles are categorized based on the following eight points in section A. Then we compare those related papers in section B.

A. *Summarization of Related Articles*

1) *Organization's current practice*

There is limited number of researches related to emergency actions after hacking or how the organizations react in these terms. Most of the organizations are yet to have standard guidelines implemented regarding Incident Management. Hove, Tarnes, Line, and Bernsmed in [9] did a survey and examines current security incident management practices and challenges in three large organizations and then provides some recommendations for future study in this field though companies have Information Security Policy and Control, however, new vulnerabilities and data security occurrences happened periodically. Hence, it is evident that companies need plans and techniques to deal with security incidents when they happen. The presence of an incident reaction capacity in a company can help them in quickly recognizing occurrences, limiting misfortune and devastation, relieving the shortcomings that were abused, and reestablishing processing administrations [9].

This study [9] is based on a qualitative research method by extraction in-depth information from relatively few informants regarding current practice in security incident management in three different types of large organizations by conducting a literature review, qualitative review and a survey. Since source of information is small but in detail, the analysis is very thorough. Finally, rather than depend on any pre-existing hypothesis, this paper tries to derive patterns from the extracted information which gives this research an inductive approach. Organization A is a large government organization having several thousand people and manage own IT. Organization B is an independent and non-commercial organization with few thousands of employees and their main IT operations run by third party companies. Organization C is IT Service provider with several thousand employees provides IT services to customers and managing their own IT infrastructure.

Large organizations have plans and procedures for incident response in place and compliance with standards and guidelines [9]. But some of the procedures, especially reporting procedures, are not satisfactorily established. There are also some other challenges like employee awareness, reporting, communication, information collection and dissemination, and allocation of responsibilities.

i) Organization A [9] has an internal policy for incident handling, but those are not well-proven plans for incident handling. They have implemented ISO/IEC 27001 and 27002 standards, and they have implemented the ITIL framework in their incident management and security work. However, ISO/IEC 270035 has not been implemented. After an incident reporting, it will be categorized, and that is either resolved or transferred to another section. The main priority of the security manager is to resolve the issue and check whether the affected system is vulnerable to another attack rather than restoring regular operations as soon as possible. Organization A has a team and workflow regarding Incident management. They have contingency plans based on a set of incidents, and they are well tied up with Police. In some situation they might fill a case and don't want to investigate themselves to avoid compromising evidence. The Researched found that most of the employee is not aware of Security Incident things [9].

ii) Organization B [9] is very much concerned about the confidentiality of information, and their operations are managed by suppliers. Though they have some knowledgeable and trained people for ISO 27001,27002,270035 and ITIL security however they have not implemented these standards in their organization. Their belief is "when a crisis occurs; the most important thing is knowing what to do, not knowing what the standard says. [9]" Organization B does not have dedicated IRT. When an incident categorized as crisis, then a crisis team is formed with its supplier. They have collected all the logs, and they might seek help for Police to investigate further. Most employees are very attentive to Security incidents, and they got awareness training sufficiently [9].

iii) Organization C [9] bases all of their service management processes on the ITIL framework. They have implemented the ISO/IEC 27001 standard and have several certifications. Their incident management processes, however, are mainly built on the ITIL framework. They have not implemented ISO/IEC 27035. Organization C has the main priority to continue business operation, minimizing the business impact by proving temporary solution to the problem. They have dedicated IRT to assist major incidents. It has own IRT handbook and their incident handling things properly elaborated if incident happened. Organization C has described workflows for incidents and significant incidents respectively, based on the ITIL framework. This Organization does not have forensic experts to do forensic analysis of technical evidence. They are doing it with the help of third party and Police if needed [9].

2) *Malware attacks in industry and their responses*

The global industries are facing malware threats that can have significant or catastrophic impacts on their businesses. Dehlawi and Abokhodair, in the article [7], did a case study of the Shamoon malware over Saudi Aramco which is one of the largest companies in the world by revenue, was hit by a cyber-attack that wiped out 30,000 computers on August 15, 2012. The attack was severe enough to shut most of the company's networks for weeks, and a malware named Shamoon was the culprit. This paper sheds light on the response of Saudi Government, the primary stockholder of the company, after the attack. It also tries to benchmark its response against industry standards or best practices [7].

To understand the narrative of the incident and the nature of Aramco's security policy, this paper [7] used a comprehensive exploratory case study methodology. A variety of publicly available text sources, blog posts, and newspaper articles are used for conducting the case study. To supplement or reinforce the information found in the text sources, in-depth interview with key personals from Aramco and professionals from the cybersecurity field is also used. Based on the results of case study, the response to Shannon malware incident was done in three phases:

i. Phase 1: Disclosure; They post a message on their official website and explain what happened to Aramco's infrastructure.

ii. Phase 2: Analysis; The Aramco, asked security experts to analyze infected systems and find what the vulnerability was.

iii. Phase 3: Media Response; A large group of top media like the New York Times and Washington Post start to report this incident throughout the world [7].

A comprehensive narrative is found in [7] after collecting, analyzing, and ranking data from various sources. This narrative can be used for future reference. Interviews with IT experts can provide a basis for the development of recommendations in cybersecurity practice [7].

It is important how response to cybersecurity attacks in critical industries like nuclear power since the wrong action can have negative hazardous damage to the industrial infrastructures. Aoyama, Naruoka, Koshijima, Watanabe in their paper [17] said that with the appearance of malicious worm ‘Stuxnet’, it is proved now that cyber-physical systems are not safe and its goal is to sabotage Industrial Control Systems’ (ICS) services by modifying the program written on Programmable Logic Control (PLC). Offensive and defensive are two different sides of cyber incidents. In the case of the offense side, the penetrator tries to exploit the machine using its weakness. On the other hand, the defensive side tries to protect the system from any unwanted incidents by locating anomaly and by responding to cyber incidents in a professional manner. So, there’s an ongoing competition between these oppositions. As the uncertainty of the affairs creates high frustration inside the organization, which might lead to effect overall incident response performance, a faster action should be taken to save all the systems from spreading out of the outbreaks.

In this paper [17] a red team (offensive) – blue team (defensive) exercise was shown where the blue team is responsible for securing a chemical plant. On the other hand, the red team’s aim is to make a disruption in the flow of production. Members were distributed in two groups and they did the test for eight hours in separate locations.

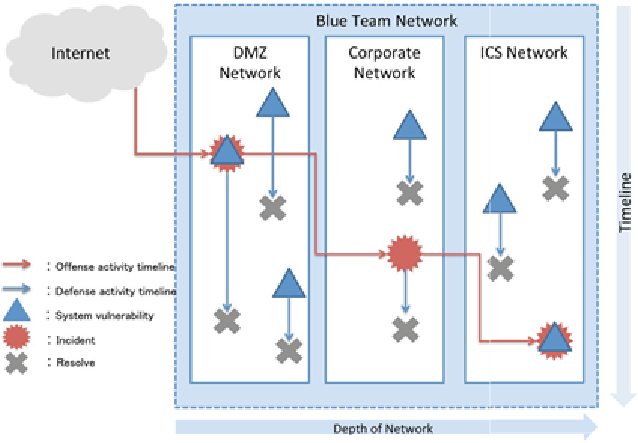


Fig. 2 Offense and defense activity [17]

As shown in Fig. 2 the red team tries to exploit the blue team’s network from outside until they get control of the production. The red team’s activity schedule is maintained by the organizer and the blue team’s activity reliant on the red team. Blue team’s reaction against the red team’s attack is the prime concern here. They are responsible for identifying the issue, enhancing security by modifying all the resources, writing report about the incident while red teams are there to look for production-related data, making interruption in the production process, and maintain secrecy of the attack.

A few managerial failures and irregularities were observed that also suggests some actions while playing the test. These include:

i) Challenge of finishing the original job that frequently gets disrupted by other occurrences,

ii) Miscommunication between the team members and the supervisors that leads to confusion and hampers in making a critical decision,

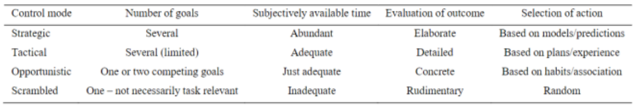
iii) There should be a proper distribution of tasks based on the priority regarding prevention, detection, and response,

iv) Risk assessment should be done to find out the most vulnerable and significant area rather than just easily visible weaknesses,

v) This test profoundly identified ambiguity of the assigned task among the participants that draws a circle of communication gap,

vi) With the growth of difficulty level, the mode shifts to opportunistic, and the management loses its capacity to predict the original objective.

However, four-level of control modes of the Context Control Model (COCOM) was operationalized by Hollnagel and Woods, and these models are strategic, tactical, opportunistic and scrambled (Fig. 3). Level of control is seen as context-specific and transitions between control modes are essential aspects of the adaptions that guarantee resilience in complex environments.



Control mode	Number of goals	Subjectively available time	Evaluation of outcome	Selection of action
Strategic	Several	Abundant	Elaborate	Based on models/predictions
Tactical	Several (limited)	Adequate	Detailed	Based on plans/experience
Opportunistic	One or two competing goals	Just adequate	Concrete	Based on habits/association
Scrambled	One – not necessarily task relevant	Inadequate	Rudimentary	Random

Fig. 3 Characteristics of the four control modes in terms of number of goals, available time, evaluation and how actions are selected [17]

Using these four-mode we can easily determine the defense team's managing measures. In the strategic manage mode, the maximum of the challenges no longer comes to the surface yet. Some irregularities may be visible as a sign of external disturbance. In tactical mode, the team adjusts the system periodically to the events. With the growth of difficulty level, the mode shifts to opportunistic. Groups are here to complete their tasks quickly. When frustration inside the team increases and the incidents exceeds the group's capability, the scrambled mode will come online which is hard to manage. Transition to this mode needs to be avoided, as the mode is infrequently workable. Hence, management obstacles should be under careful supervision.

Thereby when the management system fails to handle the occurrence, decision making has come into effect by trying with these control modes. In the view of management engineering, scramble mode should be the least popular and strategic mode is the most effective one. All incident managers should be capable of changing their control status. Hence, inside of an organization, control mode needs to be clearly defined that can act as a scale to assess management performance, and that would also train individuals regarding cyber incident management methodology. The complication of incident response could be lessening by being smart in taking urgent decisions for which responsible officials should have prior knowledge about all decision-making challenges.

3) *Zero-Day attack and response*

Organizations use different methods to defend against attacks and malware. These methods are not viable to detect when they face with zero-day attacks. Tran, Campos-Nanez, Fomin, and Wasek in the article [5] said that a zero-day attack is a malware that is difficult to diagnose and act against. There are many tools and plans developed against this attack. But these measures lose their effects day by day. They provide in article [5] a recovery model against zero-day attack and possible solutions to weak and powerful situations during recovery. They also provide more up-to-date plans and methods for zero-day attack [5].

Tran, Campos-Nanez, Fomin, and Wasek in the article [5] explain the Cyber Resilience Recovery Model (CRRM) and System Dynamics (SD) model that is derived from Susceptible-Infected-Quarantined-Recovered (SIQR) model and NIST SP 800-61 framework as recovering and analyzing plan. Those models are presented in the article that a comparison between them helps us to conceive how they are used and for what reason. Incident Response is briefly demonstrated in four stages, which are Preparation, Detection and Analysis, Containment, Eradication, and Recovery, and Post-Incident Activity. Each phase in the models guides us about spending time in some steps can be vital during recovery [5].

The paper of Tran, Campos-Nanez, Fomin, and Wasek [5] advocates that common defense methods like using firewalls, are not viable anymore against zero-day attacks. Preparing an incident response plan or designing model is feasible before the attack. Formatting and reinstalling the system has been a more feasible solution for the permanent deletion of the zero-day malware compared to other recovery methods. Besides, CRRM can be used against more attack scenarios, providing more realistic data so that can increase the resilience of the system against zero-day malware. The models can support our research about efficiency of precaution and following procedures step by step during zero-day attack.

Rashevskiy and Shaburov, in the article [6], believe that hackers are more specialized in detecting the vulnerabilities, and they try to find a way in which nobody does realize those vulnerabilities and detects system attacks. A zero-day attack is the new type of malware attack that detention of it can be challenging even for professional security analysts. The paper of Rashevskiy and Shaburov [6] focuses on special cases of Zero-day attack and traditional methods that are used for detection malware. Also, some proposed approaches for analyzing and detecting malware are mentioned in the paper [6].

The paper [6] demonstrates traditional methods of malware detection that are separated into three categories which are signature analysis, heuristics analysis, and code emulation. In addition, the proposed approaches are discussed to find doable solution for recovery. An example of an isolated environment which is a sandbox was used to test malware attacks in the system. There are five steps of analyzing possible zero-day attack: Extraction of mail, Transfering extraction of mail into sandbox , Execution of the mail, Quarantining the mail for detection purposes, and forwarding the mail. The quarantining part is observed as optional relies on suspicion in the paper [6].

Rashevskiy and Shaburov, in the article [6] suggest that security systems can be developed through isolated environments such as a sandbox. Those environments also are useful to observe behaviour of malware that can be safely executable in the environments. Extracting emails and sending them to the sandbox can be viable strategy to make system safer. Also, an environment like sandbox can lead us to achieve pioneer solutions to recover any system from dangerous malware like zero-day.

4) *Response to two different attack vectors*

The organizations have a threat of third-parties that are intercommunicating with the network of organizations and intend to make use of collected data through the network for their purpose. It would be hard to detect since the attackers conceal themselves in the communication. In some scenarios, responding to these attacks after detection is easy like running a batch file. Nayak and Samaddar in [8], said a Man-in-The-Middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. The goal of an attack is to steal personal information, such as login credentials, account details, and credit card numbers. The purpose of this paper is to explore different types of MITM attacks, their consequences, and various types of solutions as a response are available to the users [8].

Authors in the article [8] said that ARP spoofing and its effect are studied in detail to explain the methodology used in a usual MITM attack. ARP spoofing is then explained in context of various attack scenarios like DNS poisoning and HTTPS sniffing through SSL-striping. Then this paper [8] proposed a solution for IR team to handle MITM attack through ARP or cache poisoning in Linux operating systems. In this case the IR team should run a shell script which periodically sends the ARP packet to the user's gateway so that the infected user's system has the correct ARP address of the gateway in its cache. This way can stop the attack immediately, and the attacker will not be able to continue the attack [8].

A very common and old attack TYPE like MITM can be tackled with some rudimentary knowledge in shell scripting in Linux. This solution is unique in the sense that it does not require any additional appliance deployment in the environment. Even secure web connection through HTTPS is prone to consequences of MITM attack. So, a comprehensive study on ARP poisoning and DNS spoofing can help every security concern user and administrator [8].

Xiaochen, Fangqin, and Xi in their paper [10] said that Domain Name System Security Extension (DNSSE) is a standard that is developed to tackle the weakness in the DNS. But this is not always enough to provide security. So many DNS servers are vulnerable to DNS Poisoning attacks.

Authors in paper [10] mentioned the importance of emergency action after the DNS cache poisoning attack. Since the attacker can retrieve private information by changing the web URL that can lead to economic loss. After the detection phase, it is important to recover the cache of DNS servers and set up a defensive approach for them. In this stage, to ensure a clear DNS client, a command "ipconfig /flushdns" can be used that will eventually show "DNS cache refreshed successfully." Moreover, they said by extending the TTL to 7200 in the Registry setting the probability of attacks will reduce. In large portion of affected systems, these two methods can apply by Group Policy (GPO).

In the article [10], authors were calculated that the attack's success ratio was 9.09% with a TTL of 3600 seconds and bandwidth of 35Gb/s. However, it is nearly difficult to gain bandwidth like 35Gb/s in current years, so DNS Cache Poisoning Attacks are mostly impossible to succeed when TTL is 3600 seconds and above. Nevertheless, an attack can be succeeded with a reduced amount of TTL. (e.g. <60 seconds). Thus, the strategy of raising TTL numbers proved effective in minimization the DNS Cache poisoning attack.

5) *Malware and Response strategies*

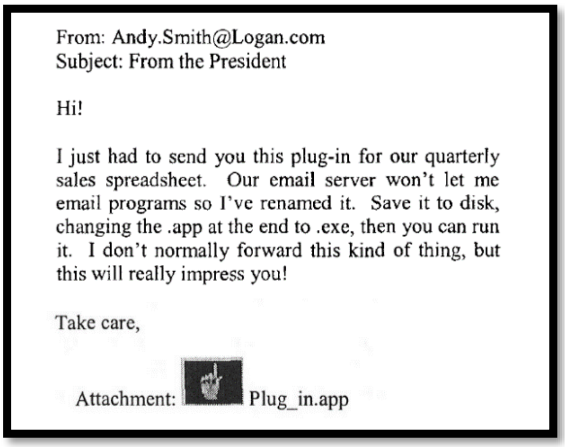
One of the essential responsibilities of the IR team is recovering the system after attack and ensure the malware is removed and the system is patched. Wael and Azer in their article [4] believe that the widespread and practical use of the Internet has led to the emergence of people who use the Internet for wrong purposes. Along with this, the danger of a security breach has begun to emerge. In particular, malware has been the result of these misuses. They mentioned in [4], this malware has as many vulnerable features as data theft, from unauthorized access to people's computers and changing the features of computer programs that are installed on people's computers. Therefore, it is necessary to take a security measure in this regard. It is worth to notice that many security tools and its variations are not able to defend the system from all of this malware. When taking the security measure, it should be kept in mind that this malware works differently in each other, and each day a new one is designed. By analyzing this malware we may recover a system after an attack [4].

According to the article [4] in the analysis of malware, the methods are divided into groups, which are behavior analysis and code analysis. Behavior analysis examines the behavior of files that are affected by malware in the system and its connection to the outside of the system. In code analysis, the design and working principle of malware are tried to be observed by using analyzing tools, executing infected files or without executing them. The use of malware forensic in this analysis is particularly effective in file and system recovery. Especially, the situation in which infected files can not be recognized or the location of the files unfound. Before initiating Malware Forensic analyzing, organizing the inspection procedure in Malware Forensic plays an active role in solving the problem for incident response and forensics investigation. In this organization, incident handling, evidence collection and analysis, incident containment, and recovery provides a faster solution as steps.

The article by Wael and Azer [4] suggests that any kind of suspicious process or image can have a dubious connection to irrelevant documents or systems. Therefore, when analyzing those files, it would be better to run infected files in isolated systems and isolated networks such as a virtual machine in isolated network. Also, utilizing a snapshot feature can be useful to make progress in identifying behaviour of malware while analyzing malware. It can also be a viable solution to the plan that consists of two different analyzes which are based on the malicious file exists and does not exist in the system.

Logan in the article [12] focuses on the recovery procedure during malicious malware attacks that many important aspects are presented to the person who was seeking to work in or study about IT department via the case study. The case study which is based on the virus attack in Logan Industries and recovery progress during the attack provides us viable and supportive information for our study and project. Furthermore, the article [12] gives us new perspective of recovery process of any system in desperate and hard periods of malicious attacks.

The article [12] presents stages of an infectious attack of which the period is divided into three days in the report of company, is followed by recovery process. First, technician visited the offices in which suspicious computers had infectious viruses due to the email, as shown in Fig. 4, and the virus had to be detected. Secondly, the technician registered virus in his system as Badboy that warn everybody and keep them alert in the company. Then, technicians in the company moved the phase that was shutting down network. Finally, the team moved to the phase that understanding behavior of virus and its etymology. The virus is associated with Visual Basic code with header that was propagating itself thorough network wise and was duplicating itself in many files of the systems. Then, they went on recovery phase. They used text search in DOS to clean infected files, and they marked the computer as green that had been fixed. After that, they reinstalled operating systems and applications in computers.



From: Andy.Smith@Logan.com
Subject: From the President

Hi!

I just had to send you this plug-in for our quarterly sales spreadsheet. Our email server won't let me email programs so I've renamed it. Save it to disk, changing the .app at the end to .exe, then you can run it. I don't normally forward this kind of thing, but this will really impress you!

Take care,

Attachment: Plug_in.app

Fig. 4 20 employees at a satellite sales office received an email from the CEO and President Andrew James [12]

The article [12] suggests responsibilities and incident handling that are key roles of surviving from dangerous cyber-attacks. Also, the steps of recovery are clarified hitherto study-case that can be doable for our project to point out critical maneuvers in incident handling. Furthermore, the article [12] highlights the impact of virus that is capable of causing security breach and harm to business environment.

The article of Vasudevan [13] concentrates on the malicious attacks that can not be detected easily. The article [13] mentions that older or vulnerable operating systems such as Windows XP and 8 that are susceptible to any unknown attacks like a zero-day attack. Vasudevan [13] advises a new framework which, is named MaITRAK, aids in reverse effects of malicious malware and to make the system getting back to a normal state. Moreover, the framework can be used to discloser undefined malware that crawls and makes worm into computer systems secretly. This framework and mentioned methods of Vasudevan can be feasible for contribution to our study and project [13].

The article [13] presents information about The Windows OS kernel system and its behavior that relates to the windows registry. The system is object-based, that every file is enclosed as an object. Also, initiation and termination of APIs are important to understand the reaction of malicious actions. According to Vasudevan [13], the methodology is divided into four steps, which are Views, Mapping, Intercepts, and Disinfection. Those steps are key roles for incident handling during undefined attack. First, critical and collective of objects are observed, such as file and configuration key in OS. Than, initiation and termination of APIs are observed to understand reaction of malicious actions in user and kernel-mode so that it can help us to understand relation between allocation of memory and APIs such as ZwReadProcessMemory or ZwWriteProcessMemory. Then, the article [13] moved to the phase of Interception. In this phase, commands of Create, Open, Delete, Close, QueryInfo, and SetInfo is observed in FSD via the windows registry. In last phase, alerting defined threats according to previous phases and try to remove them from the system.

The article [13] mentions that taking a snapshot during the attack and after recovery helps us to conceive effects of malware in the files of the system. Also, according to Vasudevan [13] analyzing the operating systems at a deep level can be various to version of operating system and its type. Therefore, incident plan and handling have to take possibilities of various systems and attacks into account in the crisis of cyber-attack.

Pan and Fung in their paper [15] said that organizations use computers and networks, and this can increase the risk of malware infection. Affecting malware with organizational systems can pose a huge risk, especially for organizations that have specific information or provide important services. In addition, malware defense programs are very weak and new malware simply breaks through the barriers and infiltrates the organization. According to research, the distance between malware control and release is very high, and this is a potential threat to corporate information. This article [15] seeks to reduce malware outbreak effect by using an Agent-Based Model to help incident responders for modeling and planning their responses. This paper also tries to compare between coordinate incident plan and non-coordinate incident plan.

Authors in [15] proposed a multi-agent system which is Agent-Based Modelling (ABM) to implement the containment phase of incident response to remove the malware from infected systems faster than the old method. The old model, which is popular is SIR. This model contains three states (Susceptible, Infected, and Recovered). The researchers' model is the Agent-based Malware Containment Modelling (AMCM) model, which uses three parameters that are constants, global variables, and scenario variables to prioritize the infected hosts and then remove the malware effect from them. The AMCM model has three agents: The malware, which is in the outbreak, the vulnerable hosts and the responders or Cyber Security Incident Response Team (CSIRT). There is also a supervisor who coordinates responders by leads them to infected hosts near them or selected hosts. The researchers attended to evaluate two stages. At the first stage they compared AMCM model with SIR, and at the second stage they tested two hypothesis responses, first increase number of responders and second prioritization of containment based on infected hosts [15].

In the article [15], at the first stage by comparing the AMCM model and the SIR model, the researchers found that using AMCM increased the rate of removal of infected hosts so responders can respond very fast to the attack by using this model, this is because using random selection from the suspicious hosts at the AMCM model instead of mathematical method which SIR used. AS shown in Fig. 5 and Fig. 6 the incident response of two models against malware attack:

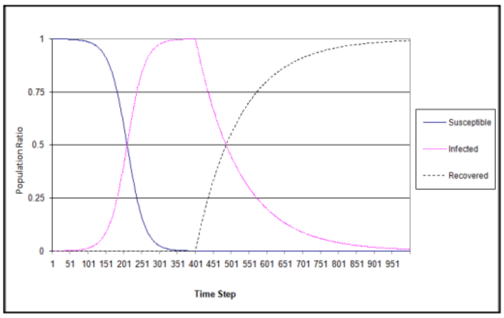


Fig. 5 SIR model output [15]

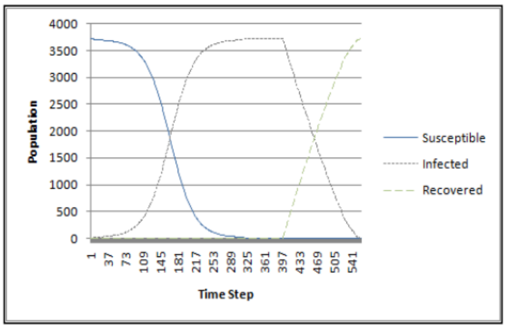


Fig. 6 AMCM Model Output [15]

In the second stage, the researchers found that the number of responders, the more achievable incident response's goals. Also, when there are oversight and coordination over responders, the time to contain Malware attacks will considerably decrease, Fig. 7 and Fig. 8 show this effect. Moreover, as shown in Fig. 9 and Fig.10 by prioritizing infected hosts for responding with oversight and coordination responders can response to malware attacks effectively.

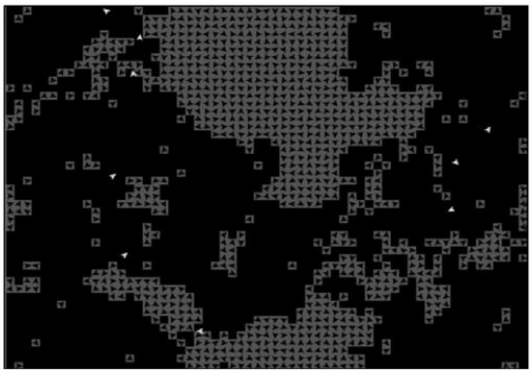


Fig. 7 AMCM Model Output Before Increase Responders [15]

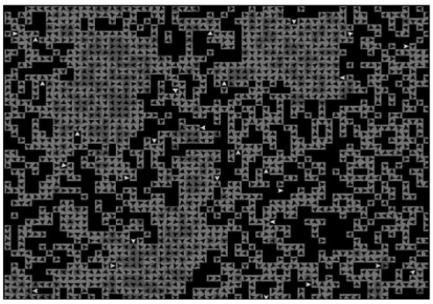


Fig. 8 AMCM Model Output After Increase [15]

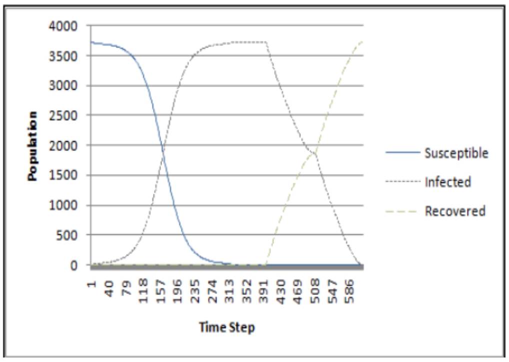


Fig. 9 Prioritization with Coordination [15]

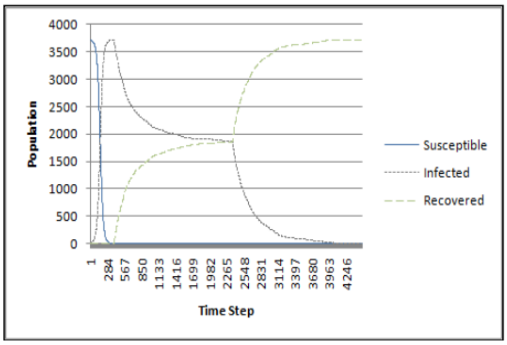
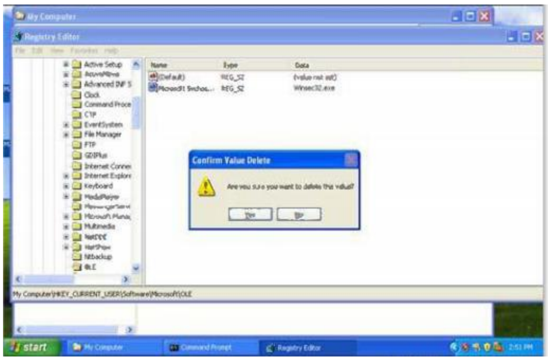


Fig. 10 Prioritization Without Coordination [15]

Authors of this paper [16] believed that since the malware can easily exploit human error and cross the line of defense, they have become an important and complex issue. Many malware containment software is ineffective, so one study found that it can only detect 20% of the software in a file. The malware can stay active even if the containment response was done. This suggests that an appropriate barrier response should be sought to counter defensive malware. This article seeks to create a containment response based on the offensive containment strategy, meaning that the response team can respond to it from the path that the malware has performed.

In paper [16] Both Windows XP and Android environments were used for this study. The reason to test the Android environment is increasing malware attacks to smartphones. The variables are the same, and the difference in the environment used is only to find out how the malware behaves. An antivirus scan was used to ensure the environment was infected. An anti-virus scan was used after the malware infection was resolved to ensure they were not present. Offensive techniques were then identified based on the gathered information about the characteristics of the Malware involved.

The goal of using offensive techniques in this paper [16] is showing that offensive techniques can be used as an incident response to remove malware from the desktop. After the Windows environment became infected with the virus, the response team use the offensive techniques for removing manual malware's process; they should use Task Manager to remove Malware's registry settings, as shown in Fig. 11.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Microsoft Svchos...	REG_SZ	Winsec32.exe

Confirm Value Delete

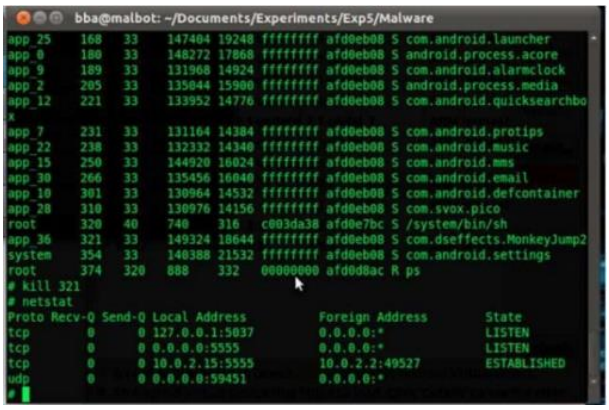
Are you sure you want to delete this value?

Yes No

My Computer\HKEY_CURRENT_USER\Software\Microsoft\OLE

Fig. 11 Remove Malware from Windows Registry [16]

This shows that the incident response team can use offensive techniques used by malware to attack to anti-malware products to response against malware attack to remove it from the system. In the Android environment, the researchers seek to show that they can get similar results from using offensive techniques in windows for smartphones. The malware in this test was the Trojan. The first step in offensive techniques used for removing malware is to find a specific listening port that malware was using. Then based on this information incident response team has to ban these ports. After that the response team should uninstall Trojan to finalize containment response part, as shown in Fig. 12.



```
bba@malbot: ~/Documents/Experiments/Exp5/Malware
app_25    168   33    147404 19248 ffffffff afd0eb08 S com.android.launcher
app_0     180   33    148272 17868 ffffffff afd0eb08 S android.process.acore
app_9     189   33    131968 14924 ffffffff afd0eb08 S com.android.alarmclock
app_2     205   33    135044 15900 ffffffff afd0eb08 S android.process.media
app_12    221   33    133952 14776 ffffffff afd0eb08 S com.android.quicksearchbo
x
app_7     231   33    131164 14384 ffffffff afd0eb08 S com.android.protips
app_22    238   33    132332 14340 ffffffff afd0eb08 S com.android.music
app_15    250   33    144920 16024 ffffffff afd0eb08 S com.android.mms
app_30    266   33    135456 16040 ffffffff afd0eb08 S com.android.email
app_10    301   33    130964 14532 ffffffff afd0eb08 S com.android.defcontainer
app_28    310   33    130976 14156 ffffffff afd0eb08 S com.svox.pico
root      320   40    740    316   c003da38 afd0e7bc S /system/bin/sh
app_36    321   33    149324 18644 ffffffff afd0eb08 S com.dseffects.MonkeyJump2
system    354   33    140388 21532 ffffffff afd0eb08 S com.android.settings
root      374   320   888    332   00000000 afd0d8ac R ps
# kill 321
# netstat
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 127.0.0.1:5037         0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:5555           0.0.0.0:*              LISTEN
tcp        0      0 10.0.2.15:5555         10.0.2.2:49527         ESTABLISHED
udp        0      0 0.0.0.0:59451          0.0.0.0:*
# 
```

Fig. 12 Stop malware remotely [16]

6) *Ransomware and Recovery Method*

The Ransomware, which is another kind malware, can destroy all data and information of an organization. This specific malware uses encryption as a method of attack, and in some scenarios, it can be impossible to stop or recover a system from attack. Richardson and North in [11] said that Ransomware is a specific type of malware that exploits security mechanisms by encrypting files and holds the key to decrypt until cryptocurrency is paid. But there are no guarantees that users will get those data decrypted even if they pay the ransom. Crypto ransomware and locker ransomware are the two most common types of ransomware where crypto-ransomware encrypts files, and locker ransomware locks the machine making it unusable. However, the first ransomware called the AIDS Trojan was made in 1989 that used simple symmetric cryptography to encrypt file names and JavaScript-only ransomware was discovered in January 2016.

This paper [11] believes most of the enforcement law agencies urge not to pay ransoms, as it will only encourage the hackers to make more ransomware which is not beneficial for the whole world. Once the attack occurs, emergency action needs to be taken to resist its replication over the network connection. As per antivirus company AVG, three steps can be taken. Firstly, running a complete scan on the infected PC to identify the ransomware. Then, copying all the infected data in a USB drive to decrypt this data in an unaffected machine. Using a tool to decrypt all the encrypted files. Before utilizing any ransomware decryption tool, the victim needs to ensure to removal of the infection from system with an updated anti-virus. Before using the decryption method, the victim first needs to know by which ransomware his system is infected. When recognized, IR team can use the tool that explicitly made to manage that particular ransomware. Generally, the warning message contains this information. Besides, each ransomware decryption tool has its own user guide [11].

Ransomware encodes exploited people's documents or information utilizing a wide range of cryptographic techniques, at that point informs the people in question that their records have been encoded and requests a payment to unscramble [11]. Some ransomware uses dynamic geographical pricing. There are hundreds of types of ransomware out there, but cybersecurity researchers are working around the clock to break the encryption that at least some of them use. Despite this, there are numerous other cryptoware strains that are not that well coded and which experts were able to crack. Backing up data, avoiding phishing emails, patching and implementing security policy can be used as a precaution. However, there are a few well-known ransomware decryption tools that can be used to get the data back [11].

7) Phishing attack and Response Management

Attackers use different ways to propagate the malware into organizations' infrastructure. One of their favorite methods is sending phishing content to the organizations' email addresses. Then, tempting users to click on the link and download the malware. Hus ́ak and Cegan in their paper [18] said phishing is one of the popular forms of social engineering attacks. Previously, phishers always use this technique to gain financial information but now they are also looking for social and professional information such as the students' accounts, employee information of a company. Lack of awareness among users made it easier for attacker to get confidential information. With the development of cloud-based services companies customers relies more on personal data and consequently security has gained a major concern.

Now if we look at the example written in this paper [18] we will find that writers used a university mailing system where there are thousands of users of different departments using the mailing system. Hence, to lessen the time of handling an incident it is important to have something that can automate the incident handling process. A tool, namely PhiGARo (Phishing: Gather, Analyze, React, and Distribute) was introduced to monitor the event that can stop further replication. PhiGARo stores the information whenever an event is identified. This helps to resist the user in replying to phishing emails or clicking on any link by informing immediately. Incidents reported by operators are sent by email or web form which then received by Request Tracker. PhiGARo begins with an assessment that helps it to figure out which technique to use to discover unfortunate victims. When the phishing contains a URL, network monitoring and logs from email servers are utilized. The revealed URL is analyzed to expose the genuine URL concealed up behind URL shorteners and redirections. PhiGARo is linked with a blocking and reporting module that used to block traffic between the secured network and IP address where the phishing website is facilitated. Later, all messages will be filtered from these websites [18].

In this paper [18] we can see that in 2012 and 2013 number of phishing incidents handled were 79 and 133, respectively. Using PhiGARo hundreds of hours of manual work was saved and it is not important for incident handlers to have complete knowledge of phishing incident and it is independently manageable. Thereby, PhiGARo proved useful to locate the phishing victims automatically using network monitoring and system logs from mail servers. It also helps in blocking phishing messages and phishing websites. Sufferers were noticed by e-mail and the incident is documented and kept for additional inquiry.

8) Agile Principle and Practice in Incident Management

The motivation behind the security incident response team is to address information security attacks and data breaches and reduce the impacts of an incident as well as to make sure the return of the organization's security posture to an acceptable state. Grispos and Glisson, in their paper [14] believed that Early research in the security incident response field mainly focused on the traditional best practices of the incident response management. But agile principles and practices of the incident response process is not widely studied among researchers. Recent commercial deliberations argue that the traditional approach in incident response is not fast, not more useful and cannot provide deep picture into the incident. This paper [14] addresses those issues and proposes agile principles and practices for the security incident response process as a workable technique of efficient incident response process for an organization.

In the paper [14] authors start with finding current practice among various industries as well as scholars to tackle security incidents and the challenges they are facing while responding to those incidents.

Then the agile process and its requirements have been discussed and it has been showed that security incident handling methods are main contenders for the incorporation of agile practices into the procedure. Finally, the authors of this paper present arguments for agile principles and practices to mitigate the security incident response challenges and concludes with some recommendations for future research works [14].

In the paper [14] Organization tried to recovery from lacking in security controls by implementing security IR actions to detect, respond to, and recover from the incident. But these steps are not flawless, and a better method is needed to tackle the issue. The incorporation of agile principles and practices can be one of the approaches and organizations can improve practical security incident handling in more well-organized way by iterative and incremental security handlings. [14].

B. Comparison

We have analyzed 15 papers related to emergency actions after hacking. It was difficult for us to compare those papers since each paper is unique in nature regards to incident response. However, we tried to distinguish those papers in three criteria which are briefly described in Table 1:

TABLE I

Papers Comparison

Criteria **Papers**	**Category**	**Does it comply with any standard or guideline?**	**Which technique is followed?**	**Which kind of attack vector can be addressed?**
Cyber Resilience Recovery Model to Combat Zero-Day Malware Attacks [5]	Zero-Day attack and response	Yes	Cyber Resilience Recovery Model (CRRM)	Zero-day Malware Attack
Protection System from '0-Day' Malware Transferred via SMTP-protocol, based on Open-Source Software [6]	Zero-Day attack and response	No	Signature Analysis, Heuristics Analysis, and Code Emulation	Zero-Day Malware Attack
Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident [7]	Malware attacks in industry and their responses	No	A Comprehensive Exploratory Case Study	Shamoon Malware
How management goes wrong? – The human factor lessons learned from a cyber incident handling exercise [17]	Malware attacks in industry and their responses	No	Context Control Model (COCOM)	Malware
Different flavours of Man-In-The-Middle attack, consequences and feasible solutions [8]	Response to two different attack vectors	No	shell script in Linux	Man-in-The-Middle (MITM)
Recovering and Protecting against DNS Cache Poisoning Attacks [10]	Response to two different attack vectors	No	Running a batch file in Windows	DNS Cache Poisoning Attack
Information Security Incident Management: Identified Practice in Large Organizations [9]	Organization's current practice	Org.1 Yes Org.2 No Org.3 Yes	Literature Review, Qualitative Review and Survey	All Kind of attacks
Ransomware: Evolution, Mitigation and Prevention [11]	Ransomware and Recovery Method	No	Manual scripting and deletion of malware	Ransomware
Malware Incident Handling and Analysis Workflow[4]	Malware and Response strategies	Yes	Behavior Analysis and Code Analysis	Malware
Bitten by a Bug: A Case Study in Malware Infection [12]	Malware and Response strategies	No	Manually shut down the system and then reinstall the OS and APPs	Malware

MalTRAK: Tracking and Eliminating Unknown Malware [13]	Malware and Response strategies	No	Used own API in windows platform	Malware
An Agent Based Model to Simulate Coordinated Response to Malware Outbreak Within An Organization [15]	Malware and Response strategies	No	Agent-based Malware Containment Modelling (AMCM)	Malware
An Offensive Containment Strategy Based on Malware's Attack Pattern [16]	Malware and Response strategies	No	Find the malware running path	Malware
Rethinking Security Incident Response: The Integration of Agile Principles [14]	Agile Principle and Practice in Incident Management	No	Agile principles and practices	All Kind of attacks
PhiGARo: Automatic Phishing Detection and incident Response Framework [18]	Phishing attack and Response Management	No	PhiGARo	Phishing Attack

IV. CONTROVERSIAL STATEMENT

Based on our research cyber incident can happen to all organizations and it is not related to how much they pay for their security services like firewalls, antiviruses and malware detections, intrusion detection and prevention. The Attack may happen even though organizations have proper security policy and enough hardware for Cybersecurity, hence we should have incident response plan in place and compliance with standards and guidelines like NIST 800-61, ITIL, and ISO 270035. What is the worthiness of having such plans and procedures? Without incident response plan, can we handle security breach issue? We cannot give a specific answer in a simple way for that. Some organizations believe that when the crisis occurs, then knowing what to do is essential, what standard says is not essential. There are some pros and cons we may observe for having and implementing incident management plan.

Pros:

1. Organization Security people could act immediately since the activity is properly defined in the Incident Management Plan.
2. Proper logs collection and monitor can be done and Security people could make some statistics and trends based on attack happened.
3. Roles and responsibilities of Team are clearly defined and hence no collision between the team.
4. Trust and Transparency can be built throughout the Organization.
5. Keeping data for evidence and forensic analysis for future investigation.
6. If the Incident Response plan is absent, then it will be challenging to act immediately and appropriately. Organization people will be in vitaldark if attack happens. Hence service restoration or any decision-making delays.

Cons:

1. Need the initial investment to implement standard and guidelines which Stockholder may not convince.
2. Much formal, hence, it might take more time to address the issue.

3. The organization might be scared to disclose the things and to inform the Police for legal matters.
4. Time and Money may be a matter for an organization to implement Incident management plan according to Guidelines and Standards.

We may try to automate the security incident response using Artificial Intelligence (AI) and Machine Learning (ML) to achieve the CIA triad which are Confidentiality, Integrity, and Availability in a timely manner.

The methods that we found in reviewed articles can be used in organizations and industries to handle cybersecurity incidents.

1- Making an incident response plan based on standards and guidelines
2- At least create an incident response playbook which covers minimum action points if any security breach or attack happened
3- Make a CSIRT team to handle the organization's security incident dedicatedly.
4- The organizations should raise IT security awareness among their personnel to reduce the risk of security threats.

V. CONCLUSIONS

We have studied different articles regarding computer security incident response. From our research, we have observed that some were followed recommended standards and guidelines based on IT security Incident management (Systematic Approach), and some were developed new methods or tools to handle the Security Incident (Ad-hoc Approach) against some attack vectors. Moreover, during our study, we have observed that people having misconception about security incident related matters, and they are thinking that IT security incident only belongs to IT related people. Sometimes management also thinks that it is nothing but expenditure and it reduces the organization's profit. However, they are not much aware of how the organization may impact if an incident happens. They may lose million-dollar business, and sometimes organizations are bound to close their business due to IT security issues. Hence, most of the organizations should have proper plan related to security incident management like incident reporting, communication, distributed responsibilities, logging, and auditing system logs, raising awareness among employees. Finally, experience is a more valuable factor not only in IT security but also in every sector of technology. Hence, we would say if organizations have proper planning with expert people, they can react cyber-attacks immediately and professionally in timely manner.

REFERENCES

[1] E. C. Thompson, Cybersecurity incident response : how to contain, eradicate, and recover from incidents, New York, NY, 2018.

[2] T. M. T. G. K. S. Paul R. Cichonski, "https://www.nist.gov/publications/computer-security-incident-handling-guide," 06 08 2012. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-61r2.

[3] P. Kral, "https://www.sans.org/reading-room/whitepapers/incident/paper/33901," 21 02 2012. [Online]. Available: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.

[4] D. Wael and M. A. Azer, "Malware Incident Handling and Analysis Workflow," in *14th International Computer Engineering Conference, ICENCO 2018*, Giza, Egypt, 2018.

[5] Hiep Tran ,Enrique Campos-Nanez, Pavel Fomin, James Wasek, "Cyber Resilience Recovery Model to Combat Zero-Day Malware Attacks," *Computers & Security,* vol. 61, no. August 1, 2016, pp. 19-31, 2016.

[6] R. B. Rashevskiy and A. S. Shaburov, "Protection System from '0-Day' Malware Transferred via SMTP-protocol, based on Open-Source Software," in *IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference, EIConRusNW 2016*, Saint Petersburg, Russia, 2016.

[7] Z. Dehlawi and N. Abokhodair, "Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident," in *IEEE International Conference on Intelligence and Security Informatics*, Seattle, WA, 2013.

[8] G. Nath Nayak and S. Ghosh Samaddar, "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions," in *3rd International Conference on Computer Science and Information Technology*, Chengdu, 2010.

[9] C. Hove, M. Tårnes, M. B. Line and K. Bernsmed, "Information Security Incident Management: Identified Practice in Large Organizations," in *Eighth International Conference on IT Security Incident Management & IT Forensics*, Munster, 2014.

[10] X. Yu, X. Chen and F. Xu, "Recovering and Protecting against DNS Cache Poisoning Attacks," in *International Conference of Information Technology, Computer Engineering and Management Sciences*, Nanjing, Jiangsu, 2011.

[11] R.Richardson, M.North, "Ransomware: Evolution, Mitigation and Prevention," *International Management Review,* vol. 13, p. 5, 2017.

[12] P. Y. Logan, S.W. Logan, "Bitten by a Bug: A Case Study in Malware Infection," *Journal of Information Systems Education (JISE),* vol. 14, pp. 301-306, 2003.

[13] A. Vasudevan, "MalTRAK: Tracking and Eliminating Unknown Malware," in *24th Annual Computer Security Applications Conference, ACSAC 2008*, Anaheim, CA, United states, 2008.

[14] G. Grispos, W.B. Glisson, T.Storer, "Rethinking Security Incident Response: The Integration of Agile Principles," in *20th Americas Conference on Information Systems (AMCIS 2014)*, Savannah, Georgia, 2014.

[15] J.Pan and C.C. Fung, "An Agent Based Model to Simulate Coordinated Response to Malware Outbreak Within An Organization," *International Journal of Information and Computer Security,* vol. 5, pp. 115-131, 2012.

[16] J. PAN, eH. e.H. FUNG, "AN OFFENSIVE CONTAINMENT STRATEGY BASED ON MALWARE'S ATTACK PATTERNS," in *International Conference on Machine Learning and Cybernetics*, Tianjin, 2013.

[17] T. Aoyama, H. Naruoka, I. Koshijima, K. Watanabe, "How management goes wrong? – The human factor lessons learned from a cyber incident handling exercise," in *6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015*, Nagoya, Japan, 2015.

[18] M. Hus ́ak, J.Cegan, "PhiGARo: Automatic Phishing Detection andIncident Response Framework," Brno, Czech Republic, 2014.

Names	Articles and Books	Tasks
Ramin Heidari Khabbaz (40109552)	NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide	- Write Background - Revise Introduction, Paper 5, 7, 8 - Write Comparison - Write Controversial Statement - Create final version based on IEEE style
	Cybersecurity Incident Response - How to Contain, Eradicate, and Recover from Incidents	
	Crafting the Infosec Playbook	
	SANS Institute: Incident Handler's Handbook	
	Recovering and Protecting against DNS Cache Poisoning Attacks	
	Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions	
	Ransomware: Evolution, Mitigation and PreventionRonny Richardson and Max North	
Behnam Panjehpour (40119593)	NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide	- Write Introduction - Summarize paper 12 and 13
	Cybersecurity Incident Response - How to Contain, Eradicate, and Recover from Incidents	
	Crafting the Infosec Playbook	
	AN OFFENSIVE CONTAINMENT STRATEGY BASED ON MALWARE'S ATTACK PATTERNS	
	An Agent Based Model to Simulate Coordinated Response to Malware Outbreak Within an Organization	
Yunus Emre Aydar (4011041)	Malware Incident Handling and Analysis Workflow	- Write Abstract - Summarize paper 1,2,3, 9, and 10 - Fix Citation
	Cyber resilience recovery model to combatzero-day malware attacks	
	MalTRAK: Tracking and Eliminating Unknown Malware	
	Bitten by a Bug - A Case Study in Malware Infection	
	Protection System from “0-Day” Malware Transferred via SMTP-Protocol, Based on Open-Source Software	
Mohammad Moazzem Hossein Khan (40104656)	Saudi Arabia’s Response to Cyber Conflict: A case study of the Shamoon malware incident	- Write Comparison - Write and revise the Controversial Statement - Write Conclusion - Summarize paper 4,5,6, and 11 - Prepare Presentation
	Information security incident management:Identified practice in large organizations	
	Mainly focuIncident Response: The Integration of Agile Principles	
	NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide and CSIRT Handbook [SEI, Carnegie Mellon University]	
	Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions	
Md Sadikur Rahman Naiem (40106537)	Ransomware: Evolution, Mitigation and Prevention Ronny Richardson and Max North	- Summarize paper 7, 8, 14, and 15
	Recovering and Protecting against DNS Cache Poisoning Attacks	
	PhiGARo: Automatic Phishing Detection andIncident Response Framework	
	How management goes wrong? – The human factor lessons learned from a cyber incident handling exercise	