British Journal of Mathematics & Computer Science
4(22): 3120-3134, 2014
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

A Comparative Assessment of Computer Security Incidence Handling

Uchenna P. Daniel Ani[1*] and Nneka C. Agbanusi[2]

[1]Department of Computer Science, Federal University, Lokoja, Nigeria.
[2]H. Pierson Associates Ltd., Lagos, Nigeria.

Article Information

DOI: 10.9734/BJMCS/2014/11874
Editor(s):
(1) Victor Carvalho, Polytechnic Institute of Cávado and Ave, Portuguese Catholic University and Lusiada University, Portugal.
Reviewers:
(1) Anonymous, Polytechnic University of Valencia, Spain.
(2) Shuai Tao, Information and Engineering College, Dalian University, China.
Peer review History: http://www.sciencedomain.org/review-history.php?iid=636&id=6&aid=5917

Review Article

Received: 08 June 2014
Accepted: 01 August 2014
Published: 28 August 2014

Abstract

Incidence response and handling has become quite a crucial, indispensible constituent of information technology security management, as it provides an organised way of handling the aftermaths of a security breach. It presents an organisation's reaction to illegitimate and unacceptable exploits on its assets or infrastructure. The goal must be to successfully neutralise the incident, such that damages are significantly reduced with attendant reduction in recovery time and costs. To achieve this, several approaches and methodologies proposed have been reviewed with a view to identifying essential processes. What is needed is referred to as incident capability mingled with collaborations. This defines a shift from response to management of computer security incidents in anointer relationship manner that foster collaboration through the exchange and sharing of incidence management details among several distinct organizations. Key step-up aspects centre on issues of enforcing and assuring trust and privacy. A viable collaborative incident response approach must be able to proffer both proactive and reactive mechanisms that are management-oriented and incorporating all required techniques and procedures.

Keywords: Incident response, incident management, incident handling, computer incidents, cyber incidents, cyber-attacks.

*Corresponding author: ucsoil@yahoo.com;

1 Introduction

Our contemporary society has witnessed a tremendous rise in cyber incidents. With the loss or damage incurred with the proliferation of this insidious activities, and given obvious facts that a great deal of these activities can hardly be put off [1], business and organisations have not relented in their efforts towards exercising controls, and management over cyber-infrastructural assets. However, unceasing developments in technology have incited greater increase in the frequency and complexity of attacks [2]. A seemingly secured end today hardly retains statuesque tomorrow. What seems a shield today could turn a hollow the next day.

Incidence response has become quite a crucial, indispensible constituent of information technology security management [1]. Incidence response provides an organised way of handling the aftermaths of a security breach. It presents an organisation's reaction to illegitimate and unacceptable exploits on its assets or infrastructure (Data, computer, network etc). As opposed to being taken unawares or caught unprepared, it is pertinent to have an on form management arrangement in place [1]. The goal must be to successfully neutralise the incident, such that damages are significantly reduced with attendant reduction in recovery time and costs.

The nature and complexity in which cyber or computer crimes thrive reveal a form of arrangement by sometimes large and well-organised groups [3]. Well thought out patterns are adopted in executing these malicious activities; and only an equal but opposite, carefully thought plan is capable of ensuring swift arrest of occurrences; all thanks to the laws of physics. A basic necessity is to be able to maintain a pre-plan that is not just able treat every security incident to its fullest through the application of suitable response methods and/or policies to minimise effect(s). Nevertheless, it should be able to lead to the actual source(s) of the incidents [4]. In broader terms, incidence response proffers a well-defined approach for detecting incidents, minimising organisational damage, fixing exploitable vulnerabilities and returning to normal operations [1]. A SANS institute survey of the relevance of Digital Forensic and Incident Response sowed that about 57% of respondents who had suffered malicious attacks noted that to be seeking for legal evidence that could hold up in court [5].

The survey underscored the need for; treating all cases with the potentials of ending up in arbitration or even legal proceedings, applying precision in the collection and management of evidence, increasing the trustworthiness so that the evidence can be defended, and ensuring sound processes that can withstand challenge under outside scrutiny [5]. This review focuses on generic computer security and incident response approaches or techniques from the year 2000 to date acquired from well-known and globally accepted professional sources like the IEEE Xplore digital library databases for conferences and journal, NIST security archives, Computer Security and Forensic books, independent systems security reviews and reports, Institutional Digital Library Archives. Literatures prior to the year 2000 are discarded due to technological relevance and evolution in trends. The methodology or approach adopted towards achieving this review is that of initial presentation and study of individual approach with a view to identifying the distinctive steps and the general advantages and weaknesses of each approach. This is followed by a comparative analysis of all the reviewed approaches and making out points of variations and similarities. Common steps are noted and outlined to make up a generic approach which through improvements and innovations could foster a better handling of computer incidences in tune with emerging trends.

2 Incident Response: Related Works

The react faster and better approach as proffered in [6] presents a three (3) tier response evaluation, escalation and management levels. All three processes are engaged transitionally from a tier 1 through tier 3 levels of the response organisation. This is similar to the state-of-the-art approach [4] to incidence response. A difference is just the exclusion of a level 0 that defines the condition where a system is in normal working order and is devoid of breach. Other researchers in the field have also proposed potential approaches leveraging different requirements and conditions all that could be utilised for effective incidence response.

2.1 Stepwise Forensic Approach

A Stepwise Forensic Approach to Incident Response and Computer Usage was proposed with the integration of two prior models; the Cyber Forensic Field Triage Process Model (CFFTPM) proposed by [7] and the Phased Investigation Methodology for Tracing Computer Usage (PIM) by [8]. CFFTPM formalises a real world investigative approach [9], affirming an onsite/field method that offers results within a short time frame without necessarily moving the suspecting/evidence media to a forensic lab for an exhaustive examination. The model emphasises a basis that; some incidences require swift and timely response, increased delay could imply greater harm to victims or assets, or better still the escape of a suspect. The PIM framework on the other hand centres on the selection of investigation targets, narrowing down the response and search to the barest minimum potential targets [9]. This allows for a prompt response to specific cases and affected systems.

The motivation for integrating these two methodologies was the need for a model that would facilitate timely and selective acquisition and response to incident data; given that most incidents tend to spread through large-scale systems that could stiffen responses and investigation. As it is, the Stepwise Forensic Process Model (SFPM) focuses on non-volatile incident data as its way of ensuring Integrity of target system. SFPM starts by categorising the data relevant for effecting trace of evidence. These include live data, file system metadata, prefetch data, registry data, web browser file and specific document file.

SFPM's five-phase (5) processes include; Case Identification, Planning, Usage Pattern Analysis, User-Files Analysis and Reporting. The process-segmentation is aimed at overcoming the problems of conventional forensic methods by efficiently choosing and responding to target systems. On the advantage, this methodology proffers a way for ensuring timely trace and response by way of extraction of incident data. In cases where a large number of systems and(or) corporations form potential targets, it ensures that a part of the systems are kept out or accorded high priority response for the sake of quick and efficient evaluation [9]; speeding up response-time and reducing resource usage. However, even though the approach does not vehemently negate traditional forensic methods, it does not yet affirm strong necessity for them as a way of ensuring and consolidating results of outcomes already acquired. On the whole, SFPM is noted to only tackle just a part of contemporary computer cybercrime incident response and handling approach. Only the forensic investigation task of establishing facts that there has been a breach, a violation to data, identity or infrastructure and establishing evidence for admissibility. The aspects of containment or elimination of vulnerabilities amongst others are not covered by this model.

2.2 Security Coordination Model

A Security Coordination Model for Inter-Organisational Information Incidents Response Forensic Process was proposed by [10]. The incident response approach leans on the basis that given certain incident complexities, most individual organisations are not able to unilaterally maintain adequate support for their computer security expert teams. Individual organisations are rarely able to maintain enough knowledge and expertise to respond to all emergent computer incidents, hence the need for collaboration with other external organisation and law enforcements. However, to remove potential threats like data privacy breaches, that are potential deterrents to this approach, the model brings to light the concept of Participant Organisation (PO) and Coordinator Organisation (CO) [11]. PO refers to individual organisation affected and that need to share information to ensure timely and successful neutralisation of an incident. The CO refers to an independent trusted organisation that would coordinate the processes of information sharing amongst POs; ensuring that rules regarding data privacy and the processes of incident response are strictly adhered to. These roles are explicitly defined in the organisational architecture of the Security Coordination model.

The model also incorporates a forensic process that extracts real-time and onsite digital evidence from monitoring systems; furnishing external organisations with the results of an analysis of such evidences, to prevent future reoccurrence [11]. Foundation blocks for this security coordination model include; real-time detection and result reporting of cyber-attacks on the part of POs, provision of online/onsite response support, propagating security events based on digital evidence collected from real-time monitoring and onsite examination of security incidents in the POs, and sharing security incident events with external organisations [11]. Greater emphasis is on communication amongst external organisations, coordination organisation and participant organisations. Global security mechanisms like hashing and digital signatures are incorporated for enhancing integrity, in addition to well documented chain of custody, incidents reconstruction for proper analysis and trace-back.

This model is noted to enhance the forensic functions of reporting and information sharing; aiding expert knowledge and skills acquisition, facilitating growth and development through collaboration. The system provides security alerting and response support based on real-time monitoring and digital forensic support based on digital evidence collected from online or onsite investigation [11].

However, if the details of an incident or threat are widely known, then such threat becomes less insidious. It is imperative to maintain role designations for specific expert levels by way of separation of duties. Such is not considered by the model. Additively, incidence response covers all that there is prior to an incident, the response and recovery to normal working order, not ruling out the pursuit of legal actions. These too are left out in the model.

2.3 Common Process Model for Incident Response and Computer Forensics

This model has been put forward as a unification of two important areas that handle computer security incidents. Incident response and computer forensics are both computer security oriented areas that are adopted for the investigation of security incidents or offences.

The investigative process of each of these areas mostly are narrowed that they are not able to yield optimum result. The well-coordinated investigative efforts that incorporate all sections of an organisation as seen in an incident response investigation might not be found in computer forensics investigation. In contrast, the adoption of scientific standards that yield objectivity and well-documented analysis in a computer forensics investigation might also give benefit to incidence response [1]. Therefore, unifying the two areas is a bid to obtain a single approach to computer security incident that incorporates the endeavours of all departments of an organisation (Legal counsel, Human Resource, Business executives), leveraging scientific standards and ensuring a well-coordinated and documented investigative process. In other words, it allows for a management-oriented approach in digital investigations while maintaining the potentials of a thorough computer forensic investigation [1].

The approach to incident response incorporated is that which was proposed in Mandia et al. [12]. It describes a seven-stage process for incident response as follows; Pre-Incident preparation, Detection of incident, Initial response, Formulation of Response strategy, Investigation of the incident and Reporting. This approach has attempted to resolve the limitations of the individual models, while introducing the concept of "*formulation of response strategy*". This presents the notion of choosing a suitable response strategy after a computer incident has been detected and initial information acquired. In the common process model, formulation of response strategy involved additional decisions, where there had to be a resolve whether to initiate a full-scale forensic analysis. Determining factors for this includes; the attacker's threat level and the potential damage to be incurred [13].

2.4 State-of-the-Art Incidence Response

The State-of-the-Art Approach to Incidence Response proffers a generic approach that leverages on the combination of a management concept and a technical concept [4]. This approach finds basis in the theory of "Escalation Level"; borne out of the established pieces of evidence, that the consequential magnitude and significance of an incident is proportional to time. Implying that greater significance is sustained if longer time ensues between the occurrence of an incident and its response. Here, incidence response has been defined based on four (4) escalation levels (0 – 3). Level 0 defines a scenario where operations are typical and no evidence has been traced. Level 1 opens up the door for discovery and initial response to identified threats. Level 2 defines a situation where threats are widening to other platforms (systems) and containment measures are being engaged. Level 3 defines the notice of higher effects in the threat, while performing containment, recovery is introduced. The processes is concluded with a post-incident analysis involving representatives of all departments and senior management to address issues of damage and impact, vulnerability removal and incident response capability procedure updates amongst other [4].

The authors of this approach asserted that when incident response capability becomes an option, then spelling out specific roles and responsibilities by organisations becomes paramount. Effective response to security incidents does not strictly dwell on the technical, experts and personnel from various departments within an organisation must actively participate in the rescue effort. Suffices to say that an explicitly-defined, simple to implement and execute management structure is essential [4]. A management schema was proposed to handle corporate incidence response. This approach to incidence response is coined from global best practices and recommendations as proposed in [14] and [15] integrated with the incident response capability (management) contacts

[4]. However, aspects of trust and compliance to procedures were not decisively covered. This implied that little attention is mated on the legitimacy of processes, activities, results and identities involved before transition to other phases.

2.5 Palantir: Collaborative Incident Response and Investigation

This framework was devised from real life practical experience in dealing with a large-scale distributed attack that occurred in 2004, popularly termed "*incident 216*" [2]. The framework became a necessity in the light of new requirements and issues that came imminent while attempting a collaborative management (information and resource sharing) of *incident 216;* a large-scale multisite attack. Comprising of a system model and a prototype implementation that facilitated partnership amongst multiple organisations and legal bodies in the response and investigation of cyber-attacks, the framework also incorporates central management by an independent trusted entity referred to as "Independent Centre for Incident Management (ICIM)" [2].

While the system model emphasises the roles, responsibilities and processes carried out by multiple organisations and law enforcement for attaining full recovery and/or prosecution, the system design cautiously tackles the security and privacy of data exchanged amongst participating organisations during the response [2]. In clear terms, this framework explores an integration of two information security areas, namely; Digital investigations and Incident response.

The framework consists of a four-phased (4) process for incident response and investigation within a localised domain which is excerpted from the recommendations of NIST [14]. It also includes another four-phased collaborative process of interactions between localised domains and the collaborative process [2]. However, it must be noted that the collaborative processes are performed at the ICIM. The four major phases of the model include; Preparation, Detection & Strategy development, Local Investigation & Recovery and Incident Closure. These processes are replicated in the collaborative process.

Central to the efficiency of this model is a collaborative workspace, which is an online platform hosted and managed by the ICIM, and made accessible to all participating member organisations for the analysis of data. This centralised approach to management was adopted for the sake of optimising security. Despite the risk to a single point of failure, the benefits of greater and better management and security were of higher priority. Thus, tools were deployed into the workspace to meet these enumerated requirements. On the advantage, this model maintains an ordered, well-defined flow of work. Several tasks abound that could be merged into a single flow for efficiency and speed. For instance, the upload and analysis of logs could be jointly simultaneously performed. The presence of such protected platform, with a surplus of useful tools no doubt makes easier the establishment of trust and engagement of collaboration among institutions in the face of cyber-attacks. This workspace allows for an extended or elongated management of collaboration against future cases, after the imminent threat is handled.

2.6 Incident Management Approach (CNSS)

This approach to incident handling was proffered by the US National Information Assurance under the auspices of the Committee for National Security Systems (CNSS). It was proposed to help organisations improve the way they detected, responded and recovered from computer or cyber incidents, when the classic six-phase approach (Prepare, Detect, Contain, Eradicate, Recover and Lesson Learned) was found to be ineffective due to the emergence of weak elements [16].

Incident management approach emerged out of the necessity to respond to the evolving threats and risks caused by computer security incidents to organisations. The need was for an improved incident handling capability that would yield better the management of incidents. This revealed a shift from response to management broadening emphasis to incident prevention, model component integration, and real-time improvement to processes. The conventional, classic approach aided consistent and sound incident response procedures that minimised the impact on business, however, the approach was yet characterised by a narrowed focus on individual stages that were perceived to be most important by the Computer Security Incident Response Team [16]. In contrast to the linearly skewed classic approach to incident handling, the incident management model presents a recursive approach that centres on combining incident-related services into a single, comprehensive program management approach; a bid to reducing disruptions to organisations [16]. The incident management model articulates a proactive position through constant monitoring and program enhancement activities, rather than a reactive stance focused on individual incidents. Vulnerability management concepts and enterprise approach to patch management are also incorporated. A continuous lesson learned process is introduced that ensures that appropriate parties are included in the policy and procedure creation, validation and maintenance. As a holistic approach, the Incident management model scheme ensures that a change in one program component is supported by other program components. Preparation and Prevention form the core and also aid appropriate interactions amongst all parts of the program component.

This Incident management model leverages the principles of planning, communication and evaluation. Planning involves the building of strategies and goals, gaining support from senior management, creating and organisational approach to incident handling and ensuring that these approaches are well integrated into the organisation's security program. Communication facilitates the exchange of information amongst internal and external audiences for better response. Evaluation encompasses feedbacks, lesson learned and gathering metrics that could help discover way of improving the process [16]. The concept of information sharing is considered very much important since most incidents usually spread to multiple organisations. This step will help mitigate the risk of harm to a larger unaware community.

2.7 Cyber Forensics Incident Response Approach

A Cyber Forensics Incident Response approach is proposed in [17]. The model is geared towards helping organizations, businesses and industries guard against intrusions, worms, automated attack against their systems. It would help towards exerting specific controls, plan of action for responding to attack or computer incident which can greatly reduce the resultant cost and also saving for bad publicity, loss of public confidence and loss of business. The proposed model aimed at addressing the problems in both incident response and cyber forensics and its distinctiveness is seen in the requisition of systematic documentation and corrective control measures. Incident response always commence with an on-going phase of pre-incident preparation that takes place even before an occurrence of the incident [17].

The model classifies incidents into two parts; the temperament of information and the nature and intricacy of the system involved. This is dependent on the type of compromised systems, to enable the variety of expertise needed to tackle the matter and eventually decide on the forensics approach to be proffered whether live or imaging or duplication or in other cases. The model emphasizes control through isolation of the affected system which may include but not limited to network termination, disabling interface at operating system level, disabling switches and or hubs and quarantining of the affected computer or just removing the network cable [17].

The proposition leans on the realization that cybercrime has become a global phenomenon needing global cooperation, legislative harmonization and technological implementation if control has to be achieved. With this model, the concept of round-the-clock cyber-surveillance to equip security/forensic officials with expertise to enable them collects legally unassailable digital evidence that will endure legal scrutiny and subsequent successful prosecution.

2.8 Incidence Response Approach

The School of Medicine, Washington University, St. Louis presented an approach for handling incident response that comprised of the four (4) steps. These include; Incident determinations (occurrence), Containment, Eradication, Recovery Process and Follow-Up [18]. As noticed, this approach bore similarity with some already mentioned approaches, and also presents the fitting together of distinct procedures like Recovery and Follow-Up. These too are very necessary for the attainment of an effective incidence response capability.

2.9 Cerebro: A Platform for Collaborative Incident Response and Investigation

Cerebro is a prototype framework/system for a Collaborative Incident Response and Investigation. The model presents a dais that allows collaborators to isolate and label illegal information. This information, collected at a granularity level, allows collaborators to specify the scope to which they desire to stake information: at a group level, an organizational level, or with all participants of an organization [19]. The approach presents a six-phase process an incident responder/assessor in the face computer crime/incident. These include; site assessment, site aggregation, site analysis, collaborative investigation/correlation, policy/rule application, and site incident strategy.

By way of generality, the cerebro model projects a systematic collection and analysis of data in a trusted cloud-computing platform, which allows for large-scale data storage while concurrently manipulating the data for evidence identification and classification. The system is proposed to be hosted on a large-scale data analysis platform on a hype security mode with forensic (extraction, logging, analysis and storage) process capabilities [19]. It employs a two-factor authentication process: role-based and signature-based, a way of ensuring that information circulates only among intended audience, an incentive-based approach for trust establishment where organizations learn more about vital watch-list information and obtain access to tools and resources to respond to and recover from attacks.

The authors asserted that the concept of collaborative incident response had become necessary in the wake of large-scale distributed cyber-attacks envisioned to exploit the principles of least privilege from a role-based access control medium. It has become typical to encounter adversaries who target communication and information exchange among experts and administrators to disrupt the effectiveness of incident responses. The model caps it all with the reliance on organizational access policies; organizations providing value in the identification and response process can collectively define important pieces (IP addresses, type of attack, pattern identification) of an investigation [19].

3 Analysis and Discussions: Unifying the Approaches

Given the upsurge of security incidents, it is needful to maintain effective response procedures. Although, it might be impracticable to stop all breaches, attempt must be made to adequately respond and manage threats.

However, the need for an organisation that provides the precise structure for handling incidents cannot be over-emphasised. Good focus on objectives, clear reporting and flexibility in investigative directions are all there to be guaranteed. A Computer Security Incident Response Team (CSIRT) is required to assume the goal of responding to cybercrime incidences [1,2] and [4]. However form the incidence appears, the group ensures a well-coordinated response, yielding a capability that allows for full recovery and patching; to avert service degeneration. They also collaborate with law enforcement when necessary to pursue criminal prosecution [2]. The services of such teams cover a proactive, reactive and security quality management perspective [20]. The proactive service helps to prepare, protect and preserve systems against potential attacks. Efficiency of this usually mitigates greatly the number of future incidents. Reactive services are activated by event requests or report of the compromise of a host, vulnerability in software or the alert by an intrusion detection system. The security management services support existing services that are independent of incident handling; by so doing assist in improving the overall security of organisation [20].

Incidence response or handling is indeed a critical aspect of computer and information security for most systems and organisations. All of the approaches proffered have in varied ways offered solutions for handling potential threats to digital information systems. Despite the variances in steps, modes and applications, all of the reviewed approaches bear one unified motive; the primary objective of discovering and halting computer threats and their attendant effects.

Close looks at the individual models reveal similarities in some of the steps. Although some of the models are environment-dependent and (or) case-specific in nature, the emergent of re-occurring steps re-emphasises significance in incident handling. It implies that any potential approach to incident handling should not be completely devoid of these processes. These processes include; preparation, detection, and formulation of response strategy/planning, containment/preservation, eradication, recovery and lesson learned/reporting/follow up and incident closure. These processes are modelled in Fig. 1 below. All of these processes should be managed in a collaborative manner given the distributed nature of modern-day threats.

3.1 Preparation

This process has been noted to be a very important aspect of an incident response methodology. The goal is to aid an organisation into a ready state for the quick and effective handling of computer incidents. Activities here include; setting and training of incident response teams, definition and adherence to proper security policies and practices including a legal framework, deployment of necessary security mechanisms (antivirus software, firewalls, Intrusion Detection

& Prevention system, Audit log consolidation, backup and recovery software). All these, are considered proactive measures to the handling of computer incidents.

3.2 Detection/Identification

This process is of crucial importance. It bothers on identifying the commencement of what is termed a "threat" in a system; for which critical decisions are required. At this process, confirmations are required about the occurrence of an incident. A system must be in place (manual or automated) for initiating alerts and reporting of incidents, ensuring that the right channel of issue to the right personnel is achieved. One very important point here is that time is of great essence; hence, detection must be in real-time to achieve best results.

3.3 Formulation of Response Strategy/Planning

The goal of this step is to determine the most suiting approach or strategy of handling the incident. This is achieved by performing an initial analysis of the scope of the incident and seeking counsel from all appropriate parties sometimes it could include the development of containment, eradication and recovery strategies.

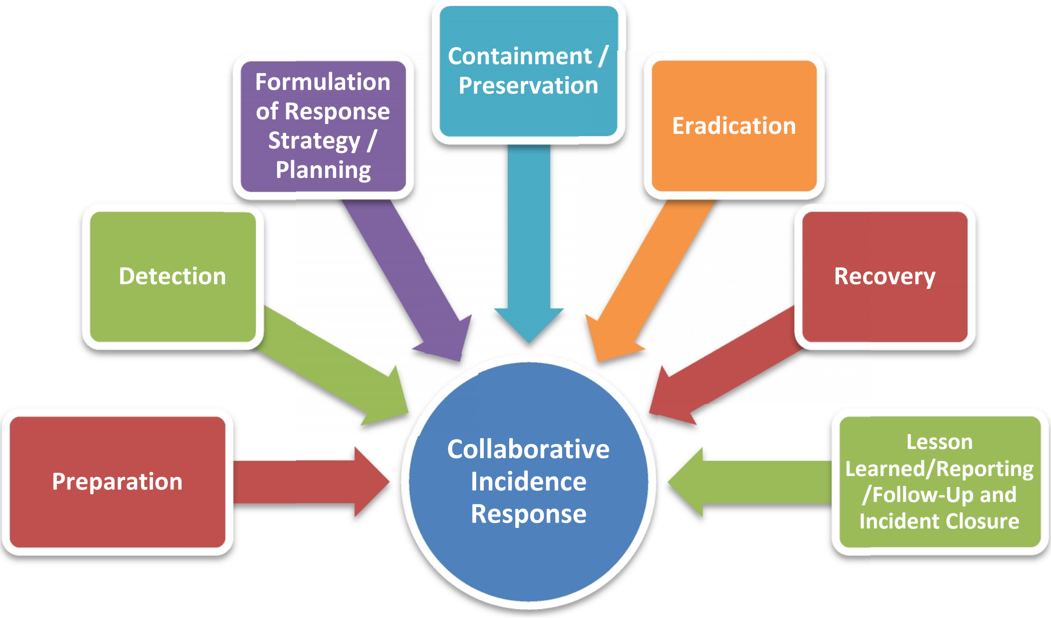
Formulation of Response Strategy / Planning
Containment / Preservation
Eradication
Detection
Recovery
Preparation
Collaborative Incidence Response
Lesson Learned/Reporting /Follow-Up and Incident Closure

Fig. 1. Collaborative incidence response

3.4 Containment/Preservation

This process is aimed at ensuring instant and interim solutions to an incident. This establishes an attempt to prevent further damages to the system. Actions could include the disabling of services, disconnection of compromised system, changing password and disabling account or at the extreme, doing a temporal shut down. This preserves the state of the system, with allowing increased compromise. Evidence collected should be preserved in a forensically sound method.

3.5 Eradication

This is similar to containment. It however focuses on the long term elimination of threats. It ensures that the system is no longer vulnerable to the threat. Activities include policy updates and independent security audits.

3.6 Recovery

This explains the process of restoring back lost or damaged information or the restoration or the restoration back to normal working order of an affected system. In the case of normal operations actions could include restoration through backups, system re-configurations and fresh installations.

3.7 Lesson Learned/Reporting/Follow-Up and Incident Closure

This combined stage involves assessing damages incurred and lesson learned from the incident. This is done a convened meeting of senior management executives and technical experts. Such lessons might require the update of security policies and guidelines. A comprehensive detail of the incident is maintained for record and referencing against future occurrence.

There are open issues that required attention if the best is to be achieved in computer security incident response. First, a correlation abounds between incident response and computer forensics. At some points both areas bear similar process and same tools. It has been observed that most organisations tend to focus on fixing breaches and getting back to normal work operations; less attention is given to lessons learned or tracing sources and taking legal actions. There is however, a need for these processes for incident handling to be whole.

Most attacks have been noted to be distributed in nature, and span across several systems and corporations; the intent is aimed at being able to gain or acquire as much leverage as possible. The complexities of these threats usually go beyond the knowledge and expertise of an individual organisation. There is the need for collaboration amongst organisations affected. Organisations by way of collaboration need to exchange information and share ideas about threat significance, potential solutions and patching methods. This must be done with great consciousness to the potentials for data privacy breaches and financial loss that could abound as a result of information sharing. Trust and assurance of organisational safety, data protection and reputation must be duly catered for in the whole process of sharing information about security threats and vulnerabilities.

There is also the issue of trust. An efficient and convincing way of proving trust for the safety of data and identity needs to be articulated if collaboration is to be maintained. Proven scientific approaches and popularly acceptable standards must be used to prove integrity of evidence that support the occurrence of a security incident.

4 Incident Response Fissures

Despite the vast efforts that have been underway towards ensuring that tolerable responses are matted to computer incidents, several fissures still exist that need to be addressed for incident response to be considered absolute. These too must be noted while planning the setup of a potentially effective response strategy [6].

4.1 Greater Focus on Prevention at the Expense of Monitoring and Response

Most companies are noted to focus greatly on prevention; relying heavily on their defensive security tools rather than ensuring a balance amongst prevention, monitoring and detection. An outcome of this is resource disproportion, which yields breach in the monitoring and alerting infrastructure with less adequate resources for response.

4.2 Weakly Structured Escalation Options

Building appropriate, smooth and well-ordered escalation path to the right entities and resources is a key inventiveness in incident response. An even response structure does not favour effective escalation. A better approach is to establish tiers that are based on factors of expertise and geography.

4.3 Excesses of the Wrong Kind of Information Too Early

Organisations tend to kick-off response processes at every alert; analysing all data available at the initial. However, without undermining the significance of audits, logs and monitoring, it is more beneficial to prioritise and filter data so as to ensure correlation.

4.4 Insufficiency of the Right Kind of Information Too Late

It has been noted that having too much of the wrong details pretty early is not beneficial. However, too little of the right information too late or early is certainly no better cure. It is advised that multiple levels of data collection be maintained. This should begin by first determining what can be collected continuously and then ascertaining the much that would be required to discover the root cause of an incident.

4.5 Knowledge-less Response

This defines a situation of responding to incidents with little or no insights and intelligence. In most circumstances, and most assuredly; this places the attacker always one step ahead the target; implying more damaged. A prerequisite is to endeavour to gather as much information speedily, and such that is enough to initiate coordinated decisions that is able to stop the attack.

These gaps have advocated for better and faster approaches to incident handling. Being able to discover timely the existence of an incident and initiating an efficient response procedure is a necessity. These might include but not restricted to collecting the right kinds of data at the right time, continuous monitoring of the system and incident level, engaging in full packet capture, and collecting as much relevant data as possible [6].

5 Conclusions and Future Work

Computer incident threat landscape and attack spaces are evolving by the day. An effective response approach yesterday might not seem same today. A good technique today could as well be unworkable the next day. The solution is; an incident handling approach that is continuously evolving. A model where processes and activities; are refined to suite potentially emanating threats.

Advanced security policies such as separation of duties could offer a better outcome. Usability, trust and security aspects of collaborating environments need to be re-emphasised and improved. Additively, contemporary forms of attacks have been seen to leverage human intelligence and the exploitation of human factors. An effective solution could tend towards such human intangibles, by proffering technological ways of implementing the conceptual world aspects of trust and privacy. There should also be a well-defined legal framework for the storage and processing of personal data; most precisely preferring ways of handling digital identity-related breaches need to be resolved into security standards. However, it must be noted that no collection of tools and techniques completely substitutesa team of skilled incident investigators and handlers. The bottom line is that the right people are required, the right procedures established and the right tools utilised. Incident response and handling of computer security incidents should maintain both a proactive and reactive stance that is management oriented and incorporating all required techniques and procedures.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Felix C. Freiling, Bastian Schwittay. A common process model for incident response and computer forensics, in Internation Conference on IT-Incidents Management & IT-Forensics - IMF 2007, Germany. 2007;19-40.

[2] Himanshu Khurana, et al. Palantir: A framework for collaborative incident response and investigation, in ID trust '09 Proceedings of the 8th Symposium on Identity and Trust on the Internet, New York. 2009;38-51.

[3] Donn B. Parker. The dark side of computing: SRI international and the study of computer crime. IEEE Annals of the History of Computing. 2007;29(1):3-15.

[4] Sarandis Mitropoulos, Dimitrios Patsos, Christos Douligeris. On incident handling and response: A state-of-the-art approach. Elsevier Journal of Computers and Security. 2006;25(5): 351-370.

[5] Jeffrey Isherwood. Evidentiary Integrity for Incident Response (EIIR), in Cyber Security Division 2013 Principal Investigators meeting. 2013;1-12.

[6] Securosis. React faster and beter: New approaches for advanced incident response. Netwitness, Report; 2011.

[7] Rogers K. Marcus, James Goldman, Rick Mislan, Wedge Timothy, Debrot Steve. Computer forensics field triage process model, in conference on digital forensics, security and law; 2006.

[8] Lee Seung Bong, Bang Jewan, Lim Kyung-soo, Kim Jongsung, Lee Sangjin. A stepwise forensic methodology for tracing computer usage, in The Fifth International Joint Conference on INC, IMS and IDC (NCM 2009); 2009.

[9] Kyung-Soo Lim, Seung Bong Lee, and Sangjin Lee. Applying a stepwise forensics approach to incident response and computer usage analysis, in 2nd International Conference on Computer Science and its Applications, 2009. CSA '09. 2009;1-6.

[10] Donn J Parker. The dark side of computing: SRI International and the Study of Computer Crime, IEEE Annals of the History of Computing. 2007;29(1): 3-15.

[11] Kimoon Jeong, Junhyung Park, Minsoo Kim, Bongnam Noh. A security coordination model for an inter-organisational information incidents response supporting forensic process, in Fourth International Conference on Networked Computing and Advanced Information Management. 2008;143-148.

[12] Kevin Mandia, Chris Prosise, Matt Pepe. Incident response & computer forensics, 2nd ed. California, USA: McGraw-Hill; 2003.

[13] Eoghan Casey. Digital Evidence and Computer Crime, 2nd ed.: Academic Press; 2004.

[14] Grance T, Kent K, Kim B. Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology. NIST, NIST Special Publication 2004;800-61.

[15] Patsos D. A strategic approach to incident response, Royal Holloway University, London, London, M.Sc Thesis; 2002.

[16] National Information Assurance, "National Information Assurance (IA) Approach to Incident Management (IM), Committee on National Security Systems, Security Recommendatons; 2007.

[17] Virginiah Sekgwathe, Mohammad Talib. Cyber forensics: Computer security and incident response, International Journal on New Computer Architectures and Their Applications (IJNCAA). 2012;2(1):127-137.

[18] Washington University, "Information Security Plan," Washington University School of Medicine, St. Loius, Security Plan; 2013.

[19] Anne Connell, Tim Palko, Hasan Yasar. Cerebro: A platform for collaborative incident response and investigation, in IEEE International Conference on Technologies for Homeland Security, Waltham, MA. 2013;241-245.

[20] Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek. Organisational models for Computer Security Incident Response Teams (CSIRTs), Carnegie Mellon Software Engineering Institute, Pittsburgh, Handbook; 2003.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=636&id=6&aid=5917