Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A survey of information security incident handling in the cloud

Nurul Hidayah Ab Rahman [a,b], **Kim-Kwang Raymond Choo** [a,*]

[a] *Information Assurance Research Group, University of South Australia, GPO Box 2471, Adelaide, SA 5001, Australia*

[b] *Information Security Department, Faculty of Computer Science and Information Technology, University of Tun Hussein Onn Malaysia, 86400 Batu Pahat, Johor, Malaysia*

ARTICLE INFO

Article history:
Received 1 July 2014
Received in revised form
22 October 2014
Accepted 18 November 2014
Available online 2 December 2014

Keywords:
Capability Maturity Model For Services (CMMI-SVC)
Cloud computing
Cloud response
Incident handling
Incident management
Incident response

ABSTRACT

Incident handling strategy is one key strategy to mitigate risks to the confidentiality, integrity and availability (CIA) of organisation assets, as well as minimising loss (e.g. financial, reputational and legal) particularly as organisations move to the cloud. In this paper, we surveyed existing incident handling and digital forensic literature with the aims of contributing to the knowledge gap(s) in handling incidents in the cloud environment. 139 English language publications between January 2009 and May 2014 were located by searching various sources including the websites of standard bodies (e.g. National Institute of Standards and Technology) and academic databases (e.g. Google Scholar, IEEEXplore, ACM Digital Library, Springer and ScienceDirect). We then propose a conceptual cloud incident handling model that brings together incident handling, digital forensic and the Capability Maturity Model for Services to more effectively handle incidents for organisations using the cloud. A discussion of open research issues concludes this survey.

1. Introduction

The pervasive interconnectivity of systems used in our Internet-connected society are potential vectors that can be exploited by actors with malicious intents, ranging from cyber criminals acting alone to organised groups of financially-, criminally- and issue/ideologically-motivated crime groups to state sponsored actors (Choo, 2011). It is not surprising that information security incidents are increasing in both numbers and the level of sophistication. For example, over 200 companies in the United States (US) reportedly experienced 122 successful cyber-attacks per week in fiscal year 2012 (Ponemon Institute, 2013). In 2013, more than 10,000 security incidents were reported to Malaysia Computer Emergency Response Team (MyCERT) (MyCERT, 2013). It was also reported by the United States (U.S.) Government Accountability Office (GAO) that 24 major federal agencies were inconsistently demonstrate effective incident handling strategies to cyber incidents based on a statistical sample of the incidents in fiscal year 2012 (U.S. GAO, 2014). The financial impacts of security incidents can be substantial. For example, the total cost of cybercrime in Australia in 2013 is estimated at AU$1.06 billion (Symantec, 2013).

Information security threats and windows of vulnerability evolve over time, partly in response to defensive actions or

* *Corresponding author*. Tel.: +61 8 8302 5876.
E-mail addresses: nurul_hidayah.ab_rahman@mymail.unisa.edu.au (N.H. Ab Rahman), Raymond.choo@unisa.edu.au (K.-K.R. Choo).
http://dx.doi.org/10.1016/j.cose.2014.11.006
0167-4048/

crime displacement, and information security is defined by the ability to manage human, process and technical imperfections, and technical solutions alone cannot provide a comprehensive information security solution Choo (2011, 2014b). Incident handling strategy is one key strategy to mitigate risks to the confidentiality, integrity and availability (CIA) of organisation assets, as well as minimising loss (e.g. financial, reputational and legal); particularly as organisations move to the cloud.

One of the challenges faced in incident handling is the cloud's organisational data that is being targeted (e.g. Intellectual Property, and unauthorised access and modification of customer and other sensitive data) as well as attempts to erase evidential data associated with current or past security incidents. As explained by Butler and Choo (2013), '[g]iven the increase in ICT in everyday life, digital forensics is increasingly being used in the courts in Australia and overseas. The concept central to digital forensic is digital evidence … [and] digital evidence is becoming more commonplace in today's digital age' for both civil litigation and criminal investigations.

Digital forensic and incident handling are usually discussed separately although the processes may overlap and are interrelated. To the best of our knowledge, there is no comprehensive survey on incident handling. For example, a recently published systematic review has been conducted by Tøndel et al. (2014) examines whether current incident management practice and experiences are consistent with ISO/IEC 27035:2011 (International Standard for Organisation, 2011) standard. This review is, however, limited in scope – only surveyed 15 publications in the context of the ISO/IEC 27035:2011 standard.

In this paper, we surveyed materials published in English over the past five years (i.e. January 2009 to May 2014). A total of 139 publications were located by searching various the websites of standard bodies (e.g. National Institute of Standards and Technology) and academic databases, including IEEEXplore, ACM Digital Library, Google Scholar and ScienceDirect using keywords such as "incident handling", "incident response", "incident management", "incident handling cloud", "incident response cloud", "digital forensic", "digital forensic cloud computing", "forensic analysis", "forensic readiness", "incident handling digital forensic", and "incident response digital forensic" — see next section. In Section 3, we discuss the role of digital forensics in incident handling, particularly in the cloud computing environment. We then outline the research trends based on the located materials and present our proposed conceptual cloud incident handling model in Section 4. The last section concludes this paper as well as identifying several potential future works.

2. Incident handling: a survey

Information security management is relatively mature, as evidenced by the number of international standards and guidelines, as well as academic literature on the topic. Despite the maturity of this area, there is a lack of consistency in describing incident management, incident handling and incident response in the literature. In this paper, we make a distinction between these terminologies, as explained in the remainder of this section (see Fig. 1).

As explained by Alberts et al. (2004), incident management is not only about responding to an incident; it also includes vulnerability handling, artefact handling, security awareness training, and other related services. Incident handling consists of incident reporting, incident analysis and incident response (Killcrece, 2003). Incident response refers to the collective actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to stop future similar incidents from occurring. Similarly, the National Institute and Standard Technology (NIST) (Cichonski and Scarfone, 2012) defines incident handling as a whole

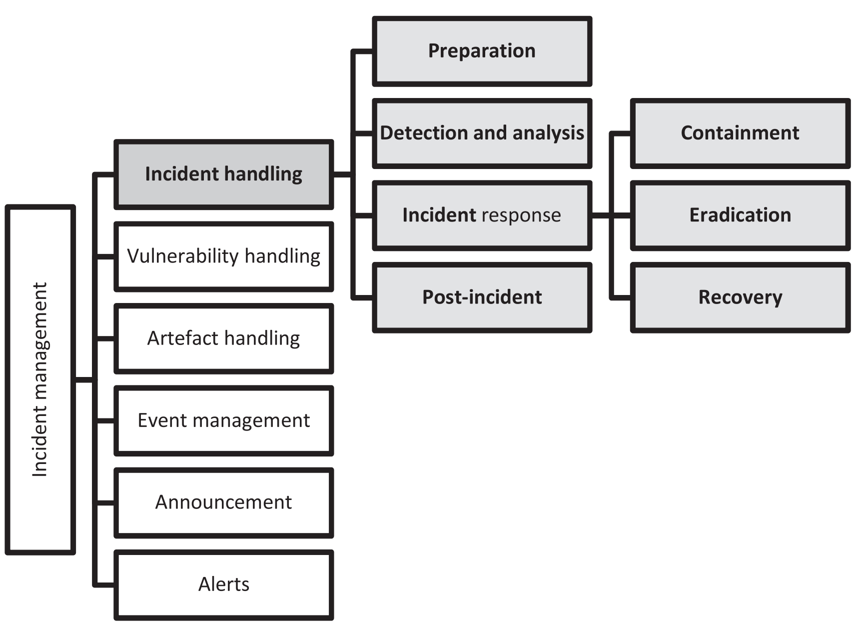

Fig. 1 – What is incident management? Adapted from: Alberts et al., 2004; British Standards Institution, 2007; Cichonski and Scarfone, 2012.

lifecycle that includes incident response. The latter relates to the ability to react to a security incident. Grobauer and Schreck (2010) further explain that response should incorporate containment, eradication and recovery phase, which is consistent with the proposed guidelines from CSIRT (Computer Security Incident Response Teams) (Alberts et al., 2004) and NIST (Cichonski and Scarfone, 2012). This is the definition adopted in this paper, namely: incident management is the 'big picture' (as presented in Fig. 1) that comprises incident handling and incident response. The grey boxes in Fig. 1 represent the scope of this study.

2.1. Standards and guidelines

This section briefly describes several key international standards and guidelines, and our reviews of existing academic incident handling models.

2.1.1. Computer Emergency Response Team Coordination Centre (CERT/CC)

CERT/CC, part of the Software Engineering Institute (SEI) located in Carnegie Mellon University (CMU), published a series of four guidelines for managing information security incidents. The Handbook for Computer Security Incident Response Teams (CSIRT) (West-Brown et al., 2003) is the main publication designed to provide specific in-depth guidance to facilitate organisation in forming and operating a CSIRT. The State of the Practice for CSIRTs (Killcrece, 2003) is designed to assist new and existing teams in understanding best practices and recommendations for handling incidents and related CSIRT services. The Organisational models for CSIRT publication (Killcrece et al., 2003) focuses on selecting the right model for an organisation's incident response capabilities. Defining Incident Management Processes for CSIRTs: A Work in Progress (Alberts et al., 2004) provides an overview of the processes and functions and supporting people, technology, and procedures that are involved in incident management.

CERT/CC discusses four phases of the incident handling process model (i.e. receiving incident report, triage, incident response, and analysing) which consists of 14 sub-phases.

2.1.2. NIST Special Publication (NIST SP 800-61)

NIST is a non-regulatory federal agency within the US Department of Commerce. The Computer Security Division of NIST publishes Special Publications of the 800 series for the computer security community. SP 800-61 (Cichonski and Scarfone, 2012) is one of the 800 series that discusses computer security handling guidelines.

This guideline outlines four incident handling phases, namely: (1) preparation, (2) detection and analysis, (3) containment, eradication and recovery, and (4) post-incident activity. In NIST's incident handling model, the second (i.e. detection and analysis) and third (i.e. containment, eradication, recovery) phases are illustrated as iterative, whereas the final phase is interconnected to the first phase.

This guideline includes a detailed description of each phase, and highlights some key points such as recommendations for conducting incident analysis, incident documentation, and the sharing of information between team members and external parties.

2.1.3. International Organisation for Standardisation (ISO)

ISO/IEC 27035:2011, an International Organisation for Standardisation (ISO) information security incident management standard, is designed for large and medium-sized organisations (International Standard for Organisation, 2011). The standard is not limited to incident handling, and covers processes for managing information security events and vulnerabilities.

Five phases are incorporated, namely: (1) planning and preparation, (2) detection and reporting, (3) assessment and decision-making, (4) responses, and (5) lessons learned. The phases are depicted as a lifecycle as each phase is connected to the following phase, including the final phase being linked to the first phase.

This standard also provides a collection of reporting form templates for information security events, incidents and vulnerabilities.

2.1.4. European Network and Information Security Agency (ENISA)

ENISA is an agency of the European Union (EU) that was established to improve network and information security in the EU. As an agency of expertise, ENISA is actively contributing to specific technical and scientific tasks.

Incident Management Guide (European Network and Information Security Agency (ENISA), 2010) is one ENISA publication that provides practical information and guidelines for the management of incident handling phases. The phases consist of six major sequence components, these being, (1) incident report, (2) report registration, (3) triage, (4) incident resolution, (5) incident closure, and (6) post-analysis. ENISA's approach closely follows the CERT/CC approach, except for the inclusion of incident closure and post-analysis in the final phase. The guideline also incorporates a formal framework for a Computer Emergency Response Team (CERT) such as roles, workflows, and basic CERT policies.

2.1.5. SANS Institute

SANS Institute is a well-known private US company that specialises in Internet Security training. In addition, SANS' research archive is publicly available, and is referred to as the SANS Reading Room. Many publications in various computer security areas can be accessed from the Reading Room, including those on incident handling matters.

SANS' Incident Handler's Handbook (Kral, 2011), a publication on Incident Handling, provides information for IT professionals and managers to create incident response policies, standards and teams for their organisation. It incorporates six subsequent phases as follows, (1) preparation, (2) identification, (3) containment, (4) eradication, (5) recovery, and (6) lessons learned. This handbook is quite brief compared to other five guidelines discussed in this section. Its contents include a checklist for the incident handler and guidelines on anomalies searching for Windows and UNIX operating systems.

2.1.6. Information Technology Infrastructure Library (ITIL)

ITIL is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the organisation. The ITIL publication consists of five volumes and each one covers an ITSM lifecycle stage.

BIP 0107:2008 — Foundations of IT Service Management Based on ITIL V3 (British Standards Institution, 2007) is a model for IT service management; incident management is one of the service management areas. It consists of five main phases, (1) incident detection and recording, (2) classification and initial input, (3) investigation and diagnosis, (4) resolution and recovery, and (5) incident disclosure. These five phases are described as a process workflow. Event management is another service area that is closely related to incident management. It is concerned with monitoring events and detecting any triggered events for the incident management process.

A comparative summary of the international standards and guidelines discussed above is presented in Table 1.

2.2. Related works

A number of academic models/frameworks (both terms are used interchangeably) have been proposed by various authors who discuss key phases and activities involved in the incident handling model.

Mitropoulos et al. (2006) proposed a framework, which draws upon principles of digital forensics and incident handling and responses. It comprises six phases, namely: (1) preparation, (2) identification, (3) containment, (4) eradication, (5) recovery and (6) follow-up. These phases are in line with the existing standards and recommendations, such as SANS (Kral, 2011) and NIST (Cichonski and Scarfone, 2012). Another more recent study (Line, 2013), based on the existing ISO/IEC 27035:2011 standard, presented a qualitative analysis that investigated current practices concerning information security incident management in the power industry.

Focussing on small-scale organisations and CSIRT, Kim et al. (2011) proposed a systematic approach for comprehensive incident handling that focused on the bot response, covering detection, analysis, and response phases. The authors noted that the other phases of incident handling (i.e. preparation and post-incident) will be expanded on by large CSIRT. The model of Khurana et al. (2009) uses a collaborative incident response and investigation mitigation strategy for multiple sites, which comprises four parallel phases at two sites (i.e. local site and collaborative centre site). The phase starts with incident preparation at both sites. It is followed by incident detection and strategy development at the local site, and in the meantime the collaborative centre starts using incident analysis once it has received an incident detection report. Both sites then conduct their investigations independently and finally close the incident collaboratively.

The emergence of cloud computing in recent years has led to several researchers examining incident handling in the cloud. For example, Grobauer and Schreck (2010) analysed the challenges and approaches that would be suitable for incident handling and response in the cloud. The challenges and approaches are examined for five common steps as follows: (1) detection, (2) analysis, (3) containment, (4) eradication and recovery, and (5) preparation/continuous improvement.

Using an OpenStack environment (Infrastructure as a Service – IaaS) as a case study, Monfared and Jaatun (2012) demonstrated that NIST incident handling guideline can be

Table 1 – Comparative summary of incident handling models in international standards and guidelines.

	Computer Emergency Response Team Coordination Centre (CERT/CC) (2003)	BIP 0107:2008	ENISA (2010)	ISO/IEC 27035:2011	SANS (Kral, 2011)	NIST SP 800-61 (Cichonski and Scarfone, 2012)
Relevant phases				Plan and prepare	Preparation	Preparation
	Reporting and detection	Incident detection and recording	Incident report registration	Detection and reporting	Identification	Detection and analysis
	Triage	Classification and initial support	Triage			
	Analysis	Investigation and diagnosis				
	Incident response	Resolution and recovery	Incident resolution	Responses	Containment, eradication recovery	Containment, eradication and recovery
		Incident closure	Incident closure post-analysis	Lessons learned	Lessons learned	Post-incident activity
Other terms used to describe incident handling		Incident management		Incident management		
Reactive/proactive	Reactive	Reactive	Reactive	Proactive	Proactive	Proactive

adapted for deployment in the cloud computing environment by introducing cloud specific strategies in each of the five phases.

The five key cloud strategies are specific cloud incident handling approaches, responsible stakeholder(s) for the approaches, service impacted, enforcement challenges, and specific platform and libraries dependencies.

A comparative summary of the six standards and guidelines, and the existing academic incident handling model is presented in Tables 1 and 2 respectively. As outlined in Table 1, the standards and guidelines of CERT/CC, BIP 0107:2008 and ENISA are reactive (i.e. services are triggered by an event or request). Both CERT/CC and ENISA incorporate incident preparation as part of the incident management framework, whereas BIP 0107:2008 discusses the issue with reference to event management (other sub-areas). This is consistent with several other published works (see Anuar et al., 2011; Yuill et al., 2000) which pointed out that incident handling is primarily reactive. On the other hand, only one academic model is reactive. This particular model, however, focuses on small scale incident. The remaining standards and guidelines in Table 1 and models in Table 2 incorporate the proactive element (i.e. provide assistance and information to help prepare, protect, and secure). This is not surprising due to the changing trend in information security and the threat landscape, which increasingly requires proactive defence and real-time incident response to defend an organisation against myriad security issues.

As mentioned earlier, incident response and incident handling were used interchangeably in the literature. Two studies in Table 2 used the "incident response" terminology to describe incident handling activities, in contrast to previous studies and recommendations (see Alberts et al., 2004; Cichonski and Scarfone, 2012; Grobauer and Schreck, 2010). Despite the use of different terminologies to describe the various phases in the standards and guidelines and academic models, four common main incident handling phases are identified in Tables 1 and 2

Incident handling generally starts with incident preparation, followed by detection and analysing of the (detected) incidents, executing response activities, discussing the incident issues in the post-incident phase and finally implementing improvements for future actions. Therefore, we conclude that the four main phases in incident handling are: (1) preparation, (2) Detection and Analysis, (3) Incident Response (includes containment, eradication, recovery), and (4) Post-Incident. We further propose that each phase requires different degrees of proactiveness, from low (or reactive) to high (see Fig. 2).

We argue that both Preparation and Post-Incident phases require high degrees of proactiveness as both phases actively incorporate mechanisms to prepare, protect and secure an organisation's assets. Incident response is mainly reactive, and the proactive degree for Detection and Analysis ranges between low and high.

2.3. The four main phases of incident handling

The four phases of incident handling are described in the next four subsections – see Fig. 3.

Table 2 – Comparative summary of academic incident handling models.

	Mitropoulos et al. (2006)	Khurana et al. (2009) Local site	Khurana et al. (2009) Collaborative centre site	Grobauer and Schreck (2010)	Kim et al. (2010)	Monfared and Jaatun (2012)	Line (2013)
Relevant phases	Preparation Identification Containment Eradication Recovery Follow-up	Local preparation Detection and strategy development Local investigation and recovery Incident closure	Collaborative preparation Incident activity analysis Collaborative investigation Incident closure	Preparation Detection Analysis Containment, eradication, recovery Continuous improvement	Detection analysis Incident response	Preparation Detection and analysis Containment, eradication and recovery Post-incident activity	Plan and prepare Detection and reporting, assessment and decision Responses Lessons learned
Other terms used to describe incident handling	Incident response	Incident response					Incident management
Reactive/proactive	Proactive	Proactive		Proactive	Reactive	Proactive	Proactive
Standard/guideline adoption						NIST SP 81-600	ISO/IEC 27035:2011

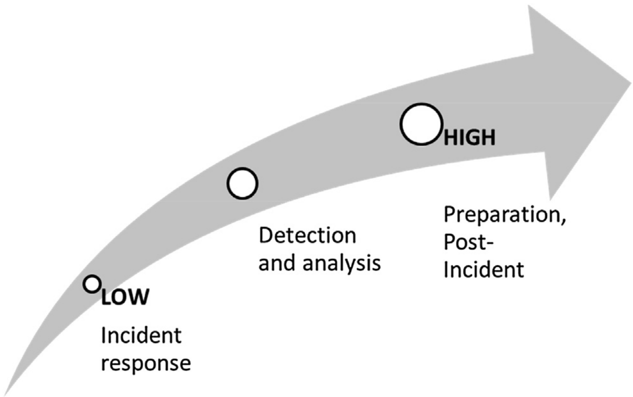

Fig. 2 – Degree of proactiveness.

2.3.1. *Preparation*

In the Preparation phase, the organisation should be in a state of readiness to minimise the impacts of security incidents and maintain business continuity (Taylor, 2013). The proactive degree in this phase should be high to ensure that unforeseen events or black swan events (i.e. events due to unexpected and highly unpredictable causes) are well-prepared for. Information Security (IS) management (e.g. IS culture, training, policy compliance) is one popular approach in pre-incident preparation, which includes establishing corporate security policies and regular updates, incident notification process, the development of an incident containment policy, creation of incident handling checklists, staff training programme, and making sure the security risk assessment process is functioning and active (Johnson, 2014).

From a technological perspective, it is crucial to address logical security control. This includes, for example, firewall implementation, malware protection, vulnerability assessment, network monitoring and data security protection (such as encryption system, authentication system). An example of a recent technology is Security Information and Event Management (SIEM), which provides real-time monitoring and historical reporting of security events captured by network, system and appliances (Anuar et al., 2010). Physical and environmental security complements the logical protection. Another key backbone in the Preparation phase is the establishment of a Computer Security Incident Response Team (CSIRT) that is responsible for determining what happened, what actions need to be taken and then undertaking the actions.

2.3.2. *Detection and analysis*

Preparation aims to minimise incident risk, yet not all incidents can be prevented. It is, therefore, necessary to rapidly detect and analyse an incident occurrence. The degree of proactiveness gradually changes from High to Medium, based on particular processes. The detection phase begins as soon as a suspicious or unusual event is detected and reported. Some examples include unfamiliar file name, unexplained new files, excessive unsuccessful login attempts, and suspicious entries in the network system account. The detection can originate from either an automated tool (e.g. intrusion detection system) and manually reported by people (users and employees). To systematically organise the flow of reports, an incident reporting model must be established in an organisation.

Incident analysis is then conducted to determine the report's validity (probably false alarm); and the potential impact(s) to the organisation's core services and assets. Risk management (including risk assessment, mitigation and evaluation) is the key to estimating the damage that such impacts can have on an organisation. Furthermore, the results of risk assessment are needed to determine incident prioritisation (if multiple incidents occur simultaneously).

2.3.3. *Incident response*

Once an incident has been detected, an effective response reaction must be undertaken. As explained by Baskerville et al. (2014), response is generally a quick and effective reaction to an event to mitigate its harmful impacts. In this phase, the proactive degree is low which suggests that reactive activities are taking place. Containment, eradication, and recovery are important actions in the incident response phase (Alberts et al., 2004; Cichonski and Scarfone, 2012). Some examples of containment and eradication action are shutting down the infected system, locking compromised accounts, blocking all incoming network traffic and changing passwords on compromised systems. Research efforts for backup and recovery are emphasised in order to improve performance, technique, and utilising advanced technologies (e.g. online backup, cloud storage).

No two crime scenes are alike. Similarly, when responding to security incidents, there is no one-size-fit-all approach or strategy. Cichonski and Scarfone (2012), for example, suggest

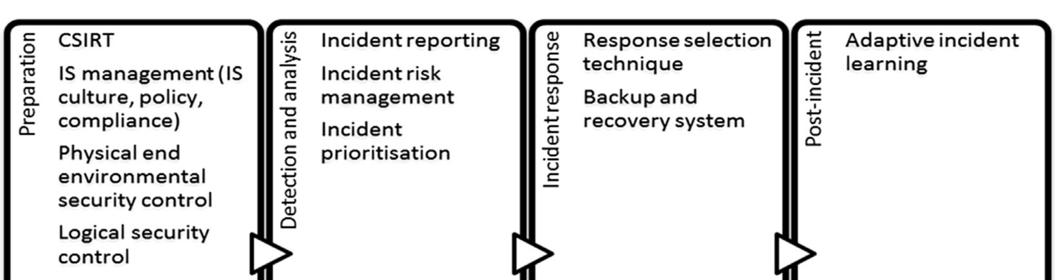

Fig. 3 – Incident handling phases and research areas. Adapted from: Cichonski and Scarfone, 2012; Grobauer and Schreck, 2010.

the following criteria to assist the formulation of an incident respond strategy.

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity and services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partial containment and full containment)
- Duration of the solution (e.g., emergency workaround to be removed in 4 h, temporary workaround to be removed in two weeks and permanent solution).

Ideally, response selection techniques should align with the particular incident scenario so that the incident response process can be rapidly deployed, say using an automated tool. One example is the automated intrusion response system (AIRS), which can be deployed as a decision-making process where appropriate response options are automatically selected to provide immediate responses (as demonstrated in the studies of Anuar et al. (2013) and Stakhanova et al. (2007b)). Researchers such as Luo et al. (2014), Shameli-Sendi and Dagenais (2013), and Zonouz et al. (2014) have also demonstrated that AIRS is able to reduce significant delay between detection time and response time especially in relation to complex and multistage attacks (i.e. significant improvement in the incident response rate).

Response selection strategies can be broadly categorised into static mapping, dynamic mapping, and cost-sensitive mapping.

2.3.3.1. *Static mapping approach*. Static model maps are a pre-specified incident alert to a predefined response (Stakhanova et al., 2007a; Krichene and Boudriga, 2008). Past response experience, particularly from CSIRT members, is one of the keys to building a static table. Krichene and Boudriga (2008) proposed probabilistic cognitive maps, a methodology for automatically determining responses to security incidents based on CSIRT members' experiences. The probabilistic cognitive map comprises a set of nodes representing concepts (can be symptoms, actions and unauthorised results) belonging to the network security field and a set of edges representing the concepts' relationship using the heuristics rule.

Ping et al. (2010) applied ontology for reusing and sharing knowledge of incident features, and case-based reasoning (CBR) to represent the decision-making process that is part of the appropriate decision response support system. The system generates the response solution using CBR once the incident ontology has been constructed.

The key benefit of the static table is that it can be easily implemented. The concept, however, enables the attacker to presume what the response action will be. As a result, the response strategy must be dynamic and this results in the dynamic mapping model.

2.3.3.2. *Dynamic mapping approach*. The selection process in dynamic mapping model is undertaken dynamically based on the context of an incident (Stakhanova et al., 2007a). In this model, more advanced and a variety of approaches in mapping incidents are deployed.

Risk assessment is a key process to minimise the performance cost, reduce response time, and ensure the trade-off between security and usability (Anuar et al., 2013; Caskurlu et al., 2013; Shameli-Sendi and Dagenais, 2013). Risk Index Model (RIM) formed the central focus of a study by Anuar et al. (2011) who considered incident prioritisation to address the issue of response time. The study adopted the Risk Index Model (RIM) to rate incidents based on two key factors, namely: 1) impact on assets; and 2) likelihood of vulnerability. In a subsequent study, the same authors presented the Response Strategy Model (RSM) for risk response planning by grouping incidents based on their priority which allows for simultaneous response (Anuar et al., 2013). The appropriate priority quadrants are assigned to the incidents based on risk ranking (Anuar et al., 2011).

In other approach to minimise response time, Shameli-Sendi and Dagenais (2013) presented perfect coordination between the risk assessment mechanism and the response system. This work incorporates adaptive response goodness (history) over time. In another approach, Mu and Li (2010) integrated the response time and response measure decision-making processes to achieve a different set of response goals by deploying a hierarchical task network planning.

Several studies (Luo et al., 2014; Zan et al., 2010; Zonouz et al., 2014) applied the Markov decision model (one of the machine-based learning techniques) to assume that future actions depend on the present state (not the past) (Zonouz et al., 2014). Machine-based learning technique consists of the ability to learn and improve over time (Patel et al., 2013). Zan et al. (2010) proposed the Hidden Markov Model (HMM) and Partially Observable Markov Decision Process (POMDP) to track and predict attack intention and identify false alerts. As highlighted by Zan et al. (2010), this approach able to improve the trade-off between response accuracy and adaptability elements, and has been applied to compute optimal response policies to maximise total response reward.

Gathering multiple opinions can obfuscate the assessment of decision-making. Integrating game theory is one suggested approach to minimise conflict of interest. For example, the Response and Recovery Engine (RRE) is a game theoretic that models the security battle between the system and the attacker as a multistep, sequential, hierarchical, non-zero sum, two-player stochastic (Markov model) (Zonouz et al., 2014). A similar concept was proposed by Kundu and Ghosh (2014) who apply Nash equilibrium strategies.

Another game theoretic approach, a Dynamic tree-based Fictitious Play (DFP), is proposed using Bayesian learning technique to describe the repeated interactive decisions of the decision-makers based on the concept of game tree (Luo et al., 2014). However, the authors also highlighted the constraint of game theory is knowledge to predict the attackers' characteristics in real time is limited.

Although the dynamic mapping model is able to address the ability to change response strategy in a dynamic environment, it does not consider damage cost and response cost. Inappropriate decisions can result in costs more expensive than the incident impact. Thus, it is necessary to compare the maximum possible damage cost with the response cost (Lee et al., 2002). This problem has motivated studies on the cost-sensitive mapping model.

2.3.3.3. *Cost-sensitive mapping approach*. Cost-sensitive response model is key to balancing damage and response costs. An appropriate response must be able to minimise values of four functions, namely: cost of implementation, the level of resources that are needed, time effectiveness, and the cost of induced modification (Fessi et al., 2014). Furthermore, the major related cost factors consist of three types (Lee et al., 2002; Zhou and Yao, 2012):

- Damage cost: The amount of damage to a target resource by an attack due to intrusion detection or prevention being unavailable or ineffective (Lee et al., 2002).
- Response cost: The cost of acting on an alarm or log entry that indicates a potential intrusion (Lee et al., 2002). Three main components that constitute response cost are response operational cost, the response history in mitigating the damage, and the response impact on the system (Strasburg et al., 2009b).
- Operational cost: The cost of processing the stream of events being monitored by intrusion detection or prevention system and analysing the activities using intrusion detection models (Lee et al., 2002).

A variety of approaches to enhance cost response and seek trade-offs has been proposed in recent years. For example, Stakhanova et al. (2007a) deployed pre-emptive (i.e. triggering the responses before the attack completes) cost-sensitive response, and an update-response option according to the response decision previously issued by the system. This approach observed intrusion pattern that made it possible to recognise the intrusion direction and, thus, trigger the correct response option. Strasburg et al. (2009b) aim to balance intrusion damage and response cost. In their study, they assess response impact with respect to resources available while incorporating security policy and properties of the affected system environment.

Kheir and Cuppens-Boulahia (2010) modelled a dependency graph consisting of services so that the cost assessment for response selection could be considered. Service dependencies refer to the relationship between confidentiality, integrity and availability (CIA) of data and the availability of IT resources. The CIA properties are employed to propagate impacts in a dependency graph with the aims of quantifying the real cost of a security incident. Each CIA vector values are subsequently updated, either by actively monitoring the estimation or by extrapolation using the dependency graph (Shameli-Sendi et al., 2012). Further analysis undertaken leads to implementing Return-On-Response-Investment (RORI) (adaptation of Return of Investment index) that considers both response collateral damage and response effects on intrusion.

Zhou and Yao (2012) in their approach applied a clustering model to reduce operating costs and optimise decision-making. Their aims are similar to that of Lee et al. (2002) but this study, however, presented a clustering algorithm to cluster the similar repeat alarms to reduce the response time.

Weighted Linear Combination (WLC), a technique proposed by Fessi et al. (2014) to deploy a multi-attribute genetic algorithm model for a multi-criteria decision-making. In this study, the response–resource causal relationship has been highlighted as the cost of each response selection will be evaluated and their impacts on the affected resources will be determined.

2.3.4. *Post-incident*

Post-incident constitutes the final phase after an incident has been resolved. The degree of proactiveness is switched to high as the relevant personnel must take the initiative to recognise and reflect new threats, and improve protection mechanisms. Information or results from this phase will be used as feedback to improve incident handling. A recently recognised feature of the Post-incident phase is transferring knowledge or experience for future actions, known as adaptive incident learning, which refers to the ability to change and learn from past experiences (Ahmad et al., 2012; Shedden et al., 2010, 2011).

Despite its importance and the impact it makes, incident learning is not widely studied compared to the technical aspects of incident handling (Shedden et al., 2010). It also appears from our literature survey that organisation learning theory has been used as the theoretical lens to examine how organisations are able to develop knowledge to guide behaviour of practicing through forms, rules, procedures and strategies. Another approach in knowledge management is ontology and it provides a formal specification of machine concepts interpretable to various domains and the relationships between them (Ping et al., 2010), which is claimed to facilitate effective learning from CSIRT to a wider audience.

Post-incident is mainly concerned with collecting information from the three previous phases for learning and improving purpose, and usually take the form of a report (Taylor, 2013). It also involves formal reporting to top management and recommending improvements in incident handling from technical and managerial perspectives. As described by Taylor (2013), a generic information content and template study would be useful to help prepare a comprehensive and informative report (particularly if the report is to be used by law enforcement agencies or in a court of law). Existing practices, however, seldom consider digital forensics despite the interconnected processes that exist between incident handling and digital forensics. We discuss the role of digital forensics in incident handling in the next section.

2.4. *The role of digital forensics in incident handling*

Digital forensic is a scientific discipline which is concerned with the collection, analysis and interpretation of digital data connected to a computer security incident (Freiling and Schwittay, 2007) as well as 'any crime that involves a digital device capable of storing electronic information' (Simon and Choo, 2014, p. 115). The discovery and acquisition process of digital evidence must be conducted in a manner that the evidential data collected is admissible in a court of law. There are several digital forensic models (see Table 3), and one widely used model is that of McKemmish (1999) that comprises the following four phases:

Table 3 – Comparative summary of digital forensic models.

	Cohen (2009)	Pilli et al. (2010)	Agarwal et al. (2011)	Martini and Choo (2012)	Wu et al. (2013)	Valjarevic and Venter (2013)	Kohn et al. (2013)	Quick and Choo (2013a)	Quick et al. (2014)
Phases		Preparation and authorisation	Preparation		Identification and preparation	Planning Processes Group	Preparation	Commence Prepare and response	Commence Prepare and response
	Identification	Detection of incident/crime	Securing the scene Survey and recognition	Evidence source identification and preservation	Identifying data sources		Incident Incident response	Identification and collection	Evidence source identification and preservation
		Incident response	Documenting the scene Communication shielding	Collection	Prioritising, preservation and collection				
	Collection	Collection	Evidence Collection			Assessment Processes Group	Physical investigation Digital forensic investigation		Collection
	Transportation Storage	Preservation Examination Analysis	Preservation Examination Analysis	Examination and analysis	Examination Analysis			Preservation Analysis	Examination and analysis
	Examination and traces	Investigation							
	Presentation Destruction	Presentation and review	Presentation Result and review	Reporting and presentation	Reporting and presentation Review results	Implementation Processes Group	Presentation Documentation	Presentation Feedback Complete or future tasks identified (second iteration)	Reporting and presentation Feedback Complete or future tasks identified (second iteration)
Forensic readiness	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Domain	Generic	Network forensics	Generic	Cloud computing	Critical infrastructure	Generic	Generic	Cloud storage	Cloud computing

- Identification — involves identification of an incident from its source(s) and determines its type.
- Preservation — involves the isolation, securing and preservation of the state of evidential data.
- Analysis — involves determination of the significance, reconstructing fragments of evidential data and drawing conclusions based upon evidence found.
- Presentation of digital evidence — involves the summary of results and conclusions.

Technological advances have spurred the need for a digital forensics model in specific domains. Pilli et al. (2010) proposed a network forensic model to deal with data found across a network connection. Wu et al. (2013) presented a forensic capability architecture with reference to critical infrastructure. The first cloud forensic framework was, probably, proposed by Martini and Choo (2012) which was subsequently validated using ownCloud (Martini and Choo, 2013) and Amazon EC2 (Thethi and Keane, 2014). Another cloud forensic framework was proposed a year later by Quick and Choo (2013a) and validated using Dropbox (Quick and Choo, 2013b), SkyDrive (Quick and Choo, 2013a), Google Drive (Quick and Choo, 2014b) and XtreemFS – a distributed filesystem supporting cloud systems (Martini and Choo, 2014). These two frameworks were subsequently merged into one (Quick et al., 2014).

The current focus of incident handling is generally on responding to incident breaches, without due consideration to collecting evidence that may provide valuable input to current investigations as well as future prosecution of the offender in a court of law. Historically, there has very little discussion of using evidence collected from the investigation of previous incidents to assist with current or other investigations. There is an opportunity to apply digital forensic processes to incident handling, and it has been noted by researchers such as Freiling and Schwittay (2007) that both incident handling and digital forensics use similar security tools such as log monitoring and data acquisition in a range of activities. For example, when a system is compromised, digital forensic process such as those of Valjarevic and Venter (2013) and techniques such as those of Quick and Choo (2013c) can be used to facilitate the collection of evidence from compromised cloud servers and client devices for analysis. This would allow subsequent reconstructing of the incident and establish facts such as.

- Where did the attack come from?;
- What vulnerability (ies) was/were exploited?; and
- What data/which systems was/were compromised?

The evidence collected can be used to inform risk mitigation strategy as well as be used in the prosecution of the offender in a court of law.

It is, therefore, not surprising that there have been recent attempts to integrate forensic practices into incident handling or vice versa. For example, Pilli et al. (2010) and Kohn et al. (2013) integrated the incident response phase into their proposed forensic model. There is increased recognition of the importance of being proactive in digital forensic investigations (e.g. forensic readiness and forensic-by-design) in recent times (see Section 3.1). Forensic readiness is a state of proactive digital forensics which is capable of determining in advance what evidence is required when an incident occurs (Pangalos et al., 2010). Conceptually, forensic readiness aligns with the proactive nature of incident handling, and seven of the nine models reviewed in Table 3 incorporate the forensic readiness phase.

The need to integrate digital forensics science and incident handling has been noted in several studies (see Cichonski and Scarfone, 2012; Freiling and Schwittay, 2007; Gurkok, 2013), and digital forensic specialists are found in most CSIRTs (see Ruefl et al., 2014).

In this paper, we integrate forensic activities (or sub-areas) in each phase of the incident handling model as illustrated in Fig. 4. For instance, findings from forensic analysis in the "Detection and Analysis" phase can facilitate the organisation to identify key assets and the vulnerabilities and threats that could be exploited to target such assets in the organisation. This will subsequently help to inform the implementation of suitable risk assessment, security controls and mitigation strategies. An appropriate and effective risk assessment and mitigation strategies can also help to ensure that the organisation is forensic ready and when an incident occurs, the investigators responding to the incident know where potential digital evidence resides in the organisation's system. This will facilitate a more efficient and timely incident response and forensic examination.

3. Discussion

3.1. *Current research trends*

The research trends concerning incident handling and digital forensics between January 2009 and May 2014 are described in Tables 4 and 5; with the total number of publications being 139. This includes three overlapping publications in digital forensic model and forensic readiness, namely: Quick and Choo (2013a), Quick et al. (2014) and Valjarevic and Venter (2013). As shown in the word cloud (see Fig. 5), "forensics" and "response" are the two most frequently used keywords in these 139 publications, followed by "security", "incident" and "management".

Table 4 summarises our survey findings of incident handling research, categorised by research areas aligned with the four incident handling phases described in Section 2.3. Risk management is the second most widely researched area and the number of publications has been consistent throughout the five years. Response selection technique, in contrast, fell sharply over the past three years. Similar to generic digital forensics model research (see Table 5), the number of publications on CSIRT and incident handling/management strategies appears to be on the decline since 2009 but specific application domains remain of interest to researchers.

There has been relatively little published work in relation to incident reporting and prioritisation in the last five years (i.e. less than 10% of publications in these two areas – see Table 4), although a number of studies on incident prioritisation were integrated with those on risk management while

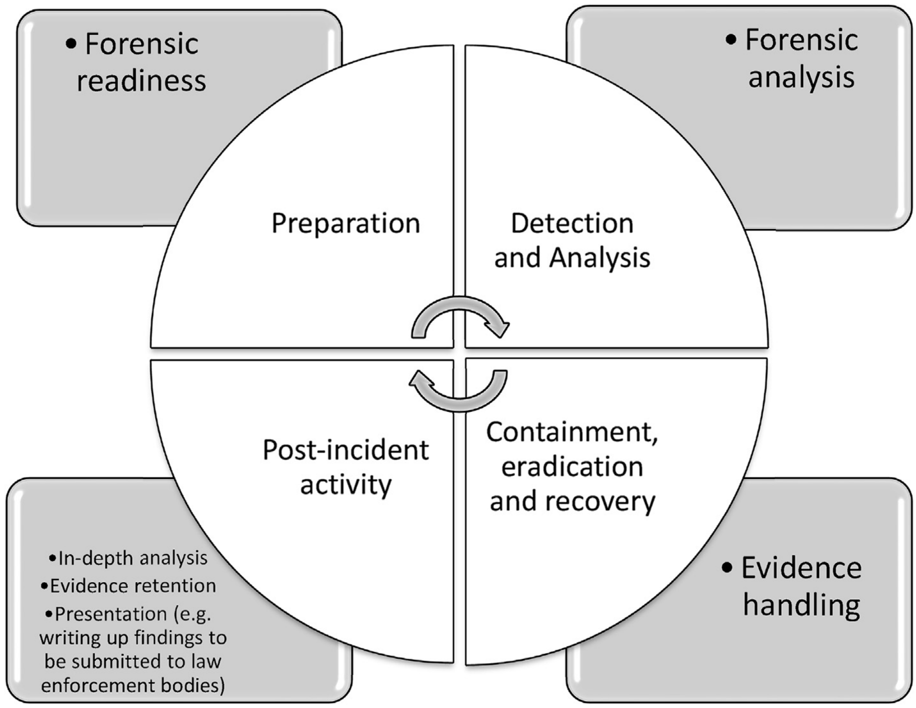

Fig. 4 – The main digital forensic activities in the incident handling.

incident reporting is mostly incorporated in incident handling strategies (Cárdenas et al., 2011; Daley et al., 2011; Shameli-Sendi et al., 2014).

Table 5 summarises our survey findings of digital forensics research, categorised by research areas. It is evident that digital forensics is a growing research area (e.g. single-digit publication between 2009 and 2010, 10 publications in 2011, 11 publications in 2012, and 17 publications in 2013) and there also appears to be growing interest in forensic readiness research. Although the number of publications on generic digital forensics model appears to have decreased after 2009, there has been interest in newer consumer technologies such as cloud computing, mobile computing and smartphone as evidenced by the fact that these three application domains and techniques improvement represent the most published topics in digital forensic research (see forensic analysis theme in Table 5). Cloud forensic is another area of increasing research focus. Research-based forensic models such as Martini and Choo (2012), Quick and Choo (2013a) and Quick et al. (2014) form the basis or foundation for more detailed practitioner-based models such as Quick and Choo (2013c). The latter is generally more detailed and platform specific (e.g. the models or processes are designed to collect evidential data from a specific technology such as cloud storage services or device type/model).

Of the 139 publications surveyed in this paper, only a small percentage discussed the role or potential of digital forensics in helping incident handling (particularly in relation to incident response) (see Kohn et al., 2013; Martini and Choo, 2012; Moser and Cohen, 2013; Pilli et al., 2010; Taylor, 2013). Considering the overlaps between both disciplines, there is great potential to integrate digital forensic practices into cloud incident handling that will influence and provide benefits to the various stages of cloud incident handling; and as an example, we present a conceptual cloud incident handling model in Section 3.3.

3.2. *Are we cloud ready?*

The adoption of cloud computing is significantly changing the landscape of incident handling, particularly between Cloud Service User (CSU) and Cloud Service Provider (CSP). CSUs may be limited in their ability to handle incidents efficiently on their sites because CSP is solely (or partly) in control of the infrastructure. Examples of CSU limitations include the inability to access log files (e.g. network log, audit log), inability to install, update or patch for vulnerability assessment (i.e. no administrative access), and inability to conduct real-time monitoring on their own. Furthermore, security incident handling is likely to be complicated by the need to involve other actors in the cloud ecosystem (e.g. cloud broker, cloud carrier, other CSUs), as compared to conventional computing which generally involves only one particular organisation. Therefore, it is foreseeable that “traditional” incident handling strategy may not be fit-for-purpose due to the cloud computing environment.

The literature suggests that the common incident handling operational procedures described in existing studies such as those of Grobauer and Schreck (2010), Gurkok (2013), Monfared and Jaatun (2012), are relevant in the cloud environment. This

Table 4 – Research areas and themes in incident handling ($n = 80$).

Incident handling			
Phase	Research area	Theme/application domain	References
Preparation	CSIRT	Automation workflow	Connell and Waits (2013); Kácha (2009)
		Establishing and coordinating CSIRT model	Daley et al. (2011); Grobler and Bryk (2010); Wiik et al. (2009a,b,c)
		Collaborative information sharing model	Murray and Ruefle (2014); Proctor (2013); Zhao and White (2014)
	Incident management/handling strategies	Model	Kostina et al. (2009); Cusick and Ma (2010); Usmani et al. (2013); Taylor (2013); Guo and Wang (2009); Line (2013); Hove and Marte (2013); Kurowski and Frings (2011); Hove et al. (2014)
		Collaborative structure	Khurana et al. (2009); Connell and Waits (2013); Bhilare et al. (2010)
		Cloud computing	Grobauer and Schreck (2010); Monfared and Jaatun (2012); Sarkar et al. (2011)
Detection and analysis	Incident reporting	Model	Koivunen (2012)
		Cloud computing	Dekker et al. (2013)
		Information exchange format	Nowruzi et al. (2012); Klein et al. (2010)
	Risk management	Model	Satoh and Kumamoto (2009); Chivers et al. (2009); Ma (2010); Shedden et al. (2011a,b); Zambon et al. (2010); Bojanc (2013); Webb et al. (2014); Caskurlu et al. (2013); Wu et al. (2009); Xinlan et al. (2010); Poolsappasit et al. (2012); Yang et al. (2013)
		Cloud computing	Zhang et al. (2010); Aleem and Sprott (2013); Albakri et al. (2014)
		Critical infrastructure	Theoharidou et al. (2011); Zonouz and Haghani (2013); Cárdenas et al. (2011)
		Smartphone	Landman (2010); Theoharidou et al. (2012)
	Incident prioritisation	Model	Frühwirth and Männistö (2009); Herrmann et al. (2011); Anuar et al. (2011)
Response (containment, eradication and recovery)	Response selection technique	Static mapping	Ping et al. (2010)
		Dynamic mapping	Anuar et al. (2013); Luo et al. (2014); Mu and Li (2010); Zan et al. (2010); Kundu and Ghosh (2014); Zonouz et al. (2014)
		Cost-sensitive mapping	Strasburg et al. (2009a,b); Kheir et al. (2009); (Kheir and Cuppens-Boulahia (2010); Zhou and Yao (2012); Shameli-Sendi and Dagenais (2013); (Fessi et al. (2014)
	Backup and recovery	Performance	Tan et al. (2011); Junqueira et al. (2011); Xia et al. (2013)
		Technologies	Hsu et al. (2014); Sindoori et al. (2012); Wood et al. (2010)
		Techniques and implementation	Zhang and Wang (2011); Zhang et al. (2011); Ongaro et al. (2011); Zhang et al. (2012); Bang et al. (2013)
Post incident	Adaptive incident learning	Model, information content and template	Ardi and Shahmehri (2009); He et al. (2014); Kulikova et al. (2012)
		Organisational learning theory	Shedden et al. (2010); Ahmad et al. (2012); Shedden et al. (2011a,b); Kearney and Kruger (2013)
		Web-based technology	He et al. (2013); Ping et al. (2010); Valiente et al. (2012)

Table 5 – Research areas and themes in digital forensics ($n = 59$).

Digital forensic		
Research area	Theme/application domain	References
Digital forensic model	Generic	Agarwal et al. (2011); Cohen (2009); Valjarevic and Venter (2013); Kohn et al. (2013); Ismail et al. (2011)
	Cloud computing	Martini and Choo (2012); Quick and Choo (2013a); Quick et al. (2014)
	Network/wireless network	Pilli et al. (2010)
	Critical infrastructure	Wu et al. (2013); Slay and Sitnikova (2009)
Forensic readiness	Generic	Valjarevic and Venter (2013); Trček et al. (2010); Grobler et al. (2010); Barske et al. (2010); Antonio and Labuschangne (2012); Elyas et al. (2014)
	Information privacy	Reddy and Venter (2009);
	Wireless network	Ngobeni et al. (2010); Pilli et al. (2010); Ngobeni et al. (2012); Cusack and Kyaw (2012)
	Cloud computing	Trenwith and Venter (2013)
	Encryption	Valjarevic and Venter (2011)
Forensic analysis (examination/investigation)	Generic	Moser and Cohen (2013)
	Cloud computing	Taylor et al. (2011); Chung et al. (2012); Lee and Hong (2011); Farina et al. (2014); Quick and Choo (2013a,b,c); Quick and Choo (2014a,b,c); Quick et al. (2014); Martini and Choo (2013); Dykstra and Sherman (2012); Yu et al. (2009); Thethi and Keane (2014)
	Mobile computing and smartphone	Mylonas et al. (2012); Morrissey (2010); Al Mutawa et al. (2012); Jung et al. (2011); Ntantogian et al. (2014); Grover (2013); Vidas et al. (2011); Sylve et al. (2012); Omeleze and Venter (2013); D'Orazio et al. (2014)
	Critical infrastructure	Afzaal et al. (2012)
	Email/web technologies	Hadjidj et al. (2009); Pereira (2009); Husain and Sridhar (2010)
	Technique improvement	Shields et al. (2011); Moser and Cohen (2013); Shosha et al. (2013); Inglot and Liu (2014); Owen and Thomas (2011); Garfinkel et al. (2012); Alazab et al. (2009); Irwin and Slay (2011); Ariffin et al. (2013a,b,c)

Fig. 5 – Generated keywords from publications.

has been demonstrated by Monfared and Jaatun (2012) where they adapted NIST Computer Security guidelines in an IaaS environment and pointed out the specific requirements for IaaS incident handling during each phase. As explained by Martini and Choo (2012, p. 78) that '[t]here will most certainly be variation in the way criminal investigation is carried out in each type of cloud platform and deployment model' and, therefore, there is 'a need to undertake further research to develop a library of digital forensic methodologies that would best suit the various cloud platforms and deployment models'.

Cloud security has attracted the attention of security researchers in recent year. Takabi et al. (2010) described the security challenges associated with outsourcing of data and applications, extensibility and shared responsibility, service level agreement, virtualisation and hypervisors, heterogeneity, compliance and regulations. In a separate work, Zissis and Lekkas (2012) described the challenges due to multi-tenancy, account control, malicious insider, data control, and management console. Cloud security challenges presented by Rong et al. (2013) include resource location, multi-tenancy, authentication and trust of acquired information, system monitoring and logs, and cloud standards. We broadly categorise the challenges discussed in the literature into three categories, namely: multi-tenancy, multi-location, and scope of user control – see Fig. 6.

Multi-tenancy utilises virtualisation technology that allows the cloud infrastructure to be shared among various users (i.e. resource pooling), which could significantly reduce resources costs. However, due to the large volume of data logs, this may result in different log formats (Ruan et al., 2011) and, therefore, complicates the analysis of log data. It may also be challenging for the CSP to segregate the log data of the affected CSU from other users for investigating, as well as identifying compromised or malicious virtual machines (VMs). In an unpublished research by participants from the joint BAE Systems Stratsec and University of South Australia 2012 winter school, for example, it was found that 'the attacker only needs to know the cloud provider's API and requisite sysadmin knowledge … [to set up] a group of cloud instances controlled by malicious entities to initiate cyber-security attacks', and 'none of the [five popular] cloud providers generated warning emails, phone calls or alerts, and that only one blocked by default inbound and outbound traffic on FTP, SMTP and SSH – but it was only a temporary fix, as running the tests again on a non-default port bypassed the block' (BAE Systems Detica, 2012).

As noted by a number of researchers, data fragmentation and distribution across two or more datacentres, particularly those in countries with different legal systems, can present technical and jurisdictional challenges in the identification and acquiring of fragile and elusive evidential data in both

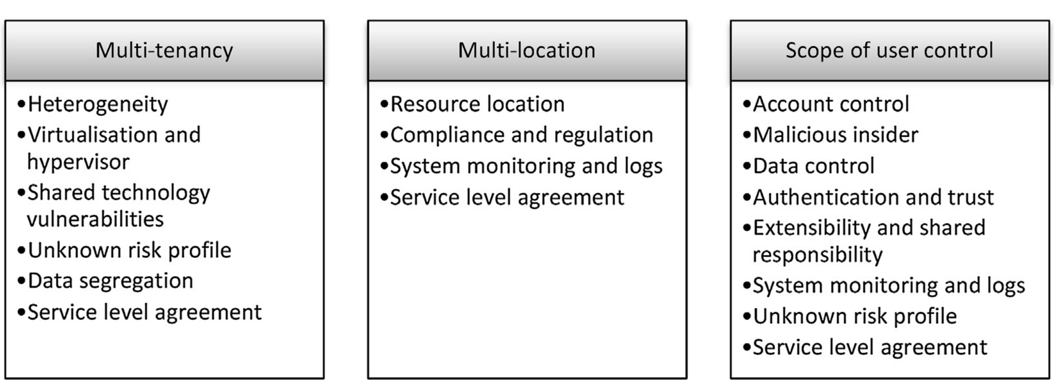

Fig. 6 – Categorisation of cloud security challenges. Compiled from: Khorshed et al., 2012; Modi et al., 2013; Rong et al., 2013; Subashini and Kavitha, 2011; Takabi et al., 2010; Zissis and Lekkas, 2012.

criminal investigations civil litigations (Choo, 2014c; Hooper et al., 2013; Martini & Choo, 2012; Quick and Choo, 2013c; Quick et al., 2014; Yang and Chen, 2010).

There had concerns raised about the potential for CSPs to be compelled to hand over user data that reside in the cloud to government agencies without the user's knowledge or consent due to territorial jurisdiction by a foreign government (Abadi et al., 2014; Clarke et al., 2013). Datacentres located in the US, for example, are subject to intelligence-gathering instruments like the USA PATRIOT Act, the Homeland Security Act and the National Security Letter (Bashir et al., 2011; US District Court for the District of Columbia, 2013).

> [F]oreign intelligence services and industrial spies may not disrupt the normal functioning of an information system as they are mainly interested in obtaining information relevant to vital national or corporate interests. They do so through clandestine entry into computer systems and networks as part of their information-gathering activities. Cloud service providers may be compelled to scan or search data of interest to 'national security' and to report on, or monitor, particular types of transactional data as these data may be subject to the laws of the jurisdiction in which the physical machine is located … overseas cloud service providers may not be legally obliged to notify the clients (owners of the data) about such requests (Choo, 2010, p. 4).

The importance of timestamps, time synchronisation and clock skew (i.e. the amount of time that a clock on a digital device deviates from the 'real' time) has been highlighted in a number of forensic studies (Ariffin et al., 2013a,b,c; Ding et al., 2011; Inglot and Liu, 2014; Kaart and Laraghy, 2014; Quick and Choo, 2014b), although these remain as forensic challenges particularly in the cloud computing environment where datacentres are located in different countries and time zones. As the evidential data are typically provided by the CSPs, the organisations or law enforcement agencies receiving the evidential data may not have an accurate or easy way of determining the time zone of the systems where the data was collected from.

One of the most notable differences in incident handling for organisational CSUs as compared to the traditional IT system model (where the infrastructure is in-house) is the lack of user control. A CSP generally has full control in a Software as a Service (SaaS) deployment whereas a CSU has more control (i.e. in application layer, platform architecture layer and virtualisation layer) in Infrastructure as a Service (IaaS) deployment (Jansen and Grance, 2011; Takabi et al., 2010). SaaS and PaaS rely heavily on the CSP to provide logging and log details for use in incident detection and analysis. In this situation, further incident analysis and investigation should be conducted by CSP if they refuse to share such information with CSU but it would be added cost for the CSPs. Meanwhile, CSU (especially in a SaaS deployment) may have limited knowledge about their deployed architecture which means that it is unlikely to conduct an in-depth incident investigation using in-house CSU personnel. Hence, CSU might require an interface to access relevant data, or deploy a middleware monitoring tool. The middleware can collect assessment information (e.g. vulnerability assessment) received from the existing security scanner solutions; and visualise them via a web interface developed for administrators (Kozlovszky et al., 2013). Another approach is to allow organisational CSU to conduct penetration tests and vulnerability scans, as implemented by Amazon (Amazon Web Services, 2014a).

The involvement of several actors in the cloud ecosystem may lead to poorly coordinated activity correlation. It can also cause misdirection in incident reporting, especially those involving a third party or multiple CSPs. A clear incident reporting strategy such as Amazon Vulnerability Reporting (Amazon Web Services, 2014b) and ENISA Cloud Security Incident Reporting Framework (Dekker et al., 2013) must be provided. To reduce the risk exposure of organisational CSUs, it is suggested that the roles and responsibilities of the CSP be detailed in legally binding documents, such as a Service Level Agreement (SLA).

SLA is a legally and formally negotiated contract between a CSP and a CSU (and/or other cloud actors) that specifies the level of service, describes the performance criteria (e.g. response times), and the minimum standard a CSP must deliver to CSU (Marinescu, 2013; Srinivasan and Rodrigues, 2012). In the case of an incident occurrence, SLA is one key document to identify the scope and responsibilities of both CSU and CSP. Example requirements that must be addressed include clear specification of roles and responsibilities, incident reporting procedures, services and techniques supported, incident investigation process, CSU's access level, logging and monitoring capability, and CSU confidentiality and privacy policies (Cloud Security Alliance, 2011; Grobauer and Schreck, 2010; Ruan et al., 2011). The German Federal Office for Information Security further recommended that.

> Cloud services should be extensively monitored round the clock (24/7), and staff should be held in reserve to respond promptly to attacks and security incidents. If so regulated in the SLA (e.g. where there is a high availability requirement for the cloud services), the customers should also be able to contact the CSP's security incident handling and troubleshooting team round the clock (Federal Office for Information Security, 2011, p. 40).

Table 6 summarises the cloud security challenges discussed, and potential mitigation strategies.

3.3. *A conceptual cloud incident handling model*

It is clear from the discussions in the preceding sections that incident handling and digital forensics are complementary. In this section, we presented our recently proposed conceptual cloud incident handling model by integrating digital forensics principles, Capability Maturity Model for Services (CMMI-SVC), and the cost involved (at each phase) to better support incident handling in the cloud environment. We now describe the basic concepts of CMMI-SVC, and the conceptual cloud incident handling model.

The Capability Maturity Model Integration for Services (CMMI-SVC) is a maturity model that focuses on improving processes for providing better services — developed by the CMMI Product Team from the Software Engineering Institute

Table 6 – Summary of incident handling issues in cloud and potential mitigation strategies.

Cloud	Challenges	Service(s) affected	Potential mitigation strategies	References
Multi-tenancy (virtualised environment)	Confidentiality and privacy issue of data belonging to or about CSUs residing on the same physical machine but are not part of the law enforcement investigation or court orders	SaaS, PaaS, IaaS (slightly)	VM snapshots can serve as the acquisition image; traditional forensic acquisition may need to be adapted; digital forensics readiness; standard event information format; Information disclosure policy Potential research topic: remote cloud forensics	(Grobauer and Schreck, 2010; Monfared and Jaatun, 2012; Ruan et al., 2011; Zimmerman and Glavach, 2011)
	CSP may have difficulties in specifically referring to the malicious or compromised VM, due to resource pooling	IaaS		
	Different log formats due to different hardware used, and challenges in segregating log files of CSUs not under investigation	SaaS, PaaS, IaaS		
Multi-location (i.e. data location)	Complications due to time synchronisation as data is likely to reside on multiple physical machines in multiple geographical regions with different time zones	SaaS, PaaS, IaaS	Harmonised regulation and compliance; improving log generation technique to allow successful analysis and correlation of information from varying sources; improving live analysis techniques; international protocol to achieve time synchronisation (e.g. RFC 5095); digital forensics readiness	(Ruan et al., 2011; Grobauer and Schreck, 2010; Trenwith and Venter, 2013; Zimmerman and Glavach, 2011; Martini and Choo, 2012)
	Data mirroring over multiple machines in different jurisdictions, lack of transparency, and non-uniform privacy and related laws	SaaS, PaaS, IaaS		
	CSP may not be able to provide a precise physical location of the data location	SaaS, PaaS, IaaS		
Scope of user control (and cloud actors participation)	Logging and log details are heavily dependent on CSP: CSU has no or limited access to event sources and vulnerability information generated by infrastructure components under the control of CSP	SaaS, PaaS	• Granular configuration of functionality and access rights; and must be clarified in SLA • Client-side incident response and forensic investigation can be conducted for IaaS and PaaS • CSP should provide a set of security APIs (e.g. event monitoring, forensic services, IDS/IPS, policy-based autonomic management system) as add-on services, or implementing middleware tool • CSP can implement software agent on CSU's site to facilitate a cross-layer security solution; therefore neither CSU nor CSP need to know each other's architecture. • Incident detection and reporting obligations (e.g. Amazon Vulnerability Report, ENISA Cloud Incident Reporting Framework), and must be set out in SLA • More attention to mutual auditability • Dedicated monitoring tool and policy of cloud insider incident.	(Grobauer and Schreck, 2010; Monfared and Jaatun, 2012; Kozlovszky et al., 2013; Sarkar et al., 2011; Ruan et al., 2011; Li et al., 2012; Dekker et al., 2013)
	Inability to add security-specific event sources (e.g. web application firewall)	SaaS, PaaS		
	No or limited knowledge about architecture	SaaS (mostly), PaaS		
	Unclear incident handling responsibilities among cloud stakeholders	SaaS, PaaS, IaaS		
	Data ownership — deleted data, terminated contract, CSP shuts down business.	SaaS, PaaS, IaaS		
	Participation of a few number of CSPs, e.g. a CSP that provides an email application (SaaS) may depend on a third-party provider to host log files (PaaS)	SaaS (mostly), PaaS, IaaS		
	Requires a specific strategy for incident handling	SaaS (mostly), PaaS, IaaS (slightly)		
	CSP's employee (insider) may compromise security and privacy of CSU	SaaS (mostly), PaaS, IaaS (slightly)		
	Lack of coordination or interruption of activities correlation (dependency chain) across cloud stakeholders	SaaS (mostly), PaaS, IaaS		
	Misdirection of incident reporting (to whom should reports be directed?)	SaaS, PaaS, IaaS		

(SEI) (CMMI Product Team, 2010). It covers the activities required to establish, deliver and manage services, and in the context of this paper, VM instances delivering cloud services to CSUs. We, therefore, believe that CMMI-SVC best practice should be incorporated into an incident handling strategy to improve business delivery.

Capability and maturity levels are applied to an organisation to achieve process improvement. There are two representation paths that can be followed, namely: (1) Continuous — an improvement in an individual process or group of processes that are chosen by the organisation; and (2) Staged — an improvement of a set of related processes already defined by the model. Continuous representation allows the capability levels for the chosen process to be achieved, while the Staged representation allows the organisation to achieve evolutionary maturity levels. The capability level consists of levels 0, 1, 2 and 3 whereas the maturity level is between level 0 and level 5. Each maturity level has its own various process areas (see CMMI Product Team, 2010).

An organisation may apply the continuous representation strategy to change a capability level profile to the associated maturity level rating using equivalent staging rule, as described below:

- To achieve maturity level 2, all process areas assigned to maturity level 2 must achieve capability level 2 or 3.
- To achieve maturity level 3, all process areas assigned to maturity levels 2 and 3 must achieve at minimum capability level 3.
- To achieve maturity level 4, all process areas assigned to maturity levels 2, 3, and 4 must achieve at minimum capability level 3.
- To achieve maturity level 5, all process areas must achieve at minimum capability level 3.

In the context of this study, Incident Resolution and Prevention (IRP) is the process area that needs to be addressed at maturity level 3. According to the equivalent staging rules, the following proposed cloud incident handling model must be executed if capability level 3 is to be achieved:

- Incomplete (level 0) – A process that is either not performed or partially performed.
- Performed (level 1) – After the process has accomplished the necessary work required to create work products (i.e. lists of sample outputs from a specific practice).
- Managed (level 2) – A performed process that is planned and executed in accordance with policy; employs skilled people having adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled, and reviewed; and is evaluated for adherence to its process description.
- Defined (level 3) – A managed process that is tailored from the organisation's set of standard processes according to its tailoring guidelines; has a maintained process description; and contributes process-related assets to the organisational process assets.

Table 7 and Fig. 7 outline our conceptual cloud incident handling model. Description for each phase mainly focuses on forensic activities, the cost involved and potential work products for CMMI evaluation (see Section 2.3 for an overview of incident handling activities).

3.3.1. *Preparation + forensic readiness*

Activities for forensic readiness involve the identification of potential sources of evidential data (e.g. log files, network traffic records, CSU devices, off-site datacentres, continually tracking authentication) in a cloud environment (e.g. CSPs, internet service providers and third parties). Forensic readiness measure such as having dedicated digital forensic workstations and software will improve chances of evidence collection and minimise the cost of a forensic investigation. Potential work products in this phase include incident handling strategy manual/handbook, security and risk management policy, and awareness and training programmes report.

Investment cost (*IC*) refers to the cost of implementing Information Security (IS) infrastructure in an organisation. It comprises three main categories, namely: people, process, and technologies. People cost includes the cost of setting up a dedicated department and employing IS personnel, process cost includes the cost of establishing IS objectives, and technology cost includes procurement cost for IS protection technology. The Return on Investment (ROI) is typically used to evaluate investment strategies by comparing investment alternatives. In a security context, Return On Security Investment (*ROSI*) has been studied by various researchers such as Cavusoglu et al. (2004), Kheir and Cuppens-Boulahia (2010), Chai et al. (2011), Tsalis et al. (2013), and Bojanc et al. (2012) to understand the value of IS investment. An example *ROSI* formula is defined in Eq. (1) (Sonnenreich et al., 2006).

$$ROSI = ((Risk\ Exposure{*}\%\ Risk\ mitigated) - IC))/IC \tag{1}$$

Higher values of ROSI indicate a more efficient security investment (Böhme, 2010).

3.3.2. *Detection and analysis + forensic collection and analysis*

During incident detection, forensic examiners will undertake the evidence collection process from the potential sources identified in the previous phase based on existing cloud forensic models such as Martini and Choo (2012). The same process will determine the incident's severity level and assign the appropriate escalation strategy. Potential evidential data sources include CSU's devices and off-site CSP datacentres. Once the evidence has been preserved and collected, the forensic analysis process will then begin. Potential work products in this phase include incident report form, verification of initial assessment, digital evidence analysis report and incident management action report.

Response cost (*RC*) is spread over the second and third phases. In this phase, *RC* mainly involves the cost of detection and analysis activities. Similar to *IC*, *RC* can be broken down into people, process and technology costs. People cost includes the costs of the workforce (e.g. helpdesk personnel logging reports from clients, and digital forensic specialist responsible for digital forensic investigation). Process cost includes the cost of digital forensic analysis (e.g. digital

Table 7 – Conceptual cloud incident handling model.

Phases	Preparation	Detection and analysis	Incident response	Post incident
Digital forensic activities	Forensic readiness	Forensic collection and analysis		N/A

Cost	Investment cost
	• People
	  • Information security personnel (including CSIRT establishment)
	• Process
	  • Information security trainings
	  • Information security policy development
	• Technologies
	  • Hardware – Router, Backup server
	  • Software – Firewall, SIEM, Intrusion Detection/Prevention System (IDPS), anti-virus suite
		Response cost
		• People
		  – Digital forensic specialist
		  – Overtime work rate
		  – Others (e.g. helpdesk)
		• Process
		  – Operational (e.g. digital forensic analysis, availability loss or gain)
		  – System performance or ability
		  – Fix and maintenance
		• Technologies
		  – Digital forensic (hardware and software)
		  – Backup and recovery (hardware and software)
				Damage cost due to:
				• Reputational (e.g. loss of business and clients)
				• Legal (e.g. civil litigations)
				• Data confidentiality, integrity and availability compromises
				• Operational (e.g. service downtime, productivity loss)

CMMI capability level			3	

evidence acquisition), and technology cost includes the expenditure on digital forensic hardware and software.

3.3.3. *Incident response*

In this phase, containment, eradication and recovery will be undertaken. Input from the forensic analysis in the previous phase would inform the response strategies in this phase. Potential work products this phase include response strategy report and monitoring activity report.

In the Incident Response phase, *RC* is the cost associated with incident response. For example, people cost includes the associated employment expenses such as overtime payroll rates, process cost includes the operation costs due to system downtime, and technology cost includes the cost of backing up and recovery of data. An example *RC* formula is that of Strasburg et al. (2009a), which consists of the operational cost *OC*, response goodness *RG*, and the response impact on the system *RSI* – see Eq. (2), where *OC* is associated with various operational aspects of response, *RG* is the ability of a response to mitigate damage caused by the security incident, and *RSI* is the impact of a response on the system quantifies the damage caused to system resources (Strasburg et al., 2009a).

$$RC = OC + RSI - RG \tag{2}$$

Another potentially useful formula for cloud service providers and organisations cloud service users is the Return on Response Investment (*RORI*), proposed by Kheir and Cuppens-Boulahia (2010) – see Eq. (3).

$$RORI = \frac{RG - (RSI + OC)}{RSI + OC} \tag{3}$$

3.3.4. *Post-incident*

Key findings from forensic analysis in phase two will be included as one of the required reports in this phase. The expected content will comprise the documentation compiled during the incident, the analysis methods and techniques, and other relevant findings. The report can also be presented to a judicial body or for further legal actions. Potential work products in this phase include post-mortem meeting report, forensic investigation report and incident learning report.

Damage cost (*DC*) refers to the losses due to the security incident, which can be either direct (e.g. immediate loss due to system downtime) or indirect losses (e.g. reputational and legal) (Böhme, 2010; Bojanc et al., 2012; Tsalis et al., 2013). Indirect loss, however, may have a far greater impact than direct loss, as explained by Bojanc et al. (2012) and Bojanc and Jerman-Blažič (2008). For example, a major security incident that results in the system being offline for a day or two will have a major financial impact on securities organisations (e.g. online stock market). An example formula to measure damage cost proposed by Lee et al. (2002) is described in Eq. (4), where *progress* refers to the successful level of an attack achieving its goal, *criticality* refers to the value of the attack's target, and $base_D$ refers to the cost (predefined) for each of the incident category.

$$DC = progress*criticality*base_D \tag{4}$$

In summary, the cost parameters for *IC*, *RC*, and *DC* vary between organisations due to their business nature, cloud

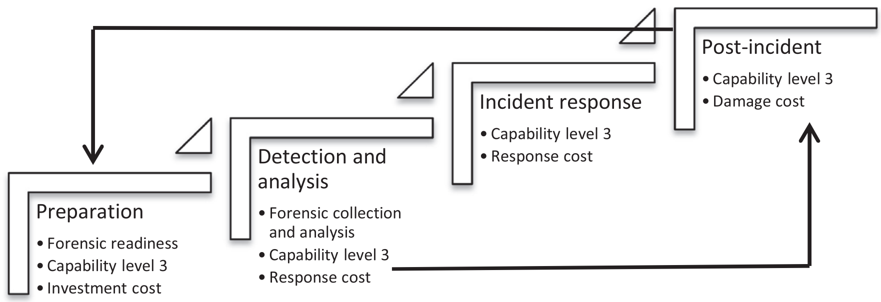

Fig. 7 – Conceptual cloud incident handling model.

deployment, and cloud services model. Shameli-Sendi et al. (2014) describe several example cost parameters, which can either be direct cost or indirect cost. Direct cost includes the total cost of the acquisition, deployment and maintenance of information security technology while indirect costs refer to the non-negligible cost (Böhme, 2010). The measurement unit can be quantitative, qualitative and semi-quantitatively. Interested reader is referred to the NIST Special Publication for Conducting Risk Assessments (Blank and Gallagher, 2012) for a detailed explanation of the measurement units.

While costs can be calculated separately and using different models (depending on the respective organisation needs), it is necessary for cloud service providers and organisational cloud service users to conduct a cost benefit analysis. Taking a common-sense approach, we suggest that an effective incident handling model (and one that is likely to have senior management buy-in) needs to have *IC* larger than or equal to the total of *RC* and *DC* – see Eq. (5).

$$IC \geq RC + DC \tag{5}$$

Finally, all the key processes during each phase must be executed in order to achieve capability level 3. It is expected that the relevant work products will be properly documented. The work products will be an indicator to rank appropriate level. In order for the whole model to be qualified as CMMI-SVC Maturity Level 3, each phase must achieve a minimum of capability level 3.

4. Conclusion and future work

In our increasingly connected society, it is inevitable that organisations including CSPs, regardless of their size, will fall victim to one or more security breaches at some point in time. To ensure organisational competitiveness and resilience, it is crucial for CSP and organisational CSU to have in place an effective incident handling model to act against cyber threats before it is too late, and to recover from a wide range of malicious cyber activities when such threats succeed (Choo, 2014a).

Incident handling is a relatively mature and understood topic, but incident handling processes are complicated by the distributed nature of the cloud (e.g. data is unlikely to reside on the CSU site and each CSP is likely to have data from multiple CSU residing on the same hardware). As noted by a number of researchers, despite the significant increases in evidential data (see Quick and Choo, 2014a,c), the role of digital forensics is often secondary in managing and handling security incidents. This observation is also echoed in our survey of 139 publications on incident handling and digital forensics published in the last five years (i.e. January 2009 to May 2014). Only a small number of studies have highlighted the potential for digital forensic practices to be part of an incident handling strategy.

One of the research areas identified by Nikkel (2014) is the need to integrate digital forensics with incident handling. In this paper, we proposed a conceptual cloud incident handling model by integrating digital forensics principles, Capability Maturity Model for Services (CMMI-SVC), and the cost involved (at each phase) to better support incident handling in the cloud environment. Further research is being conducted to validate the proposed model, which is as described below.

- Next phase of research (Phase 2): We will be conducting technical experiments using both real world data and simulated data in a private cloud computing environment to determine the utility of the conceptual model.
- Phase 3: We will be conducting face-to-face interviews and online questionnaire surveys with CSP and CSU stakeholders to review the conceptual model and make suggestions for refining the model to deal with operational challenges and issues.

Both phases 2 and 3 will be undertaken in parallel, and findings from both phases will be used to refine the model.

Other future works could include:

— A collaborative and international cloud incident management platform with the aims of sharing information between geographically dispersed multiple stakeholders and facilitating real-time incident handling and responses to malicious cyber activities in real-time. Collaborative information sharing among CSIRT members is an area worth further investigation, particularly in a cloud environment context. As explained by Connell et al. (2013) and Khurana et al. (2009), such collaborative model can be implemented across multiple organisations and legal entities so that actively collaboration is encouraged in the handling of incidents. In the context of the cloud, the collaboration could be centrally managed by a trusted entity (e.g. Centre for Cloud Incident Management).

— *A consistent definition for cyber security incident*. Cyber security incidents can be broadly categorised into cybercrime, cyber war, cyber terrorism and cyber espionage, but there is no international consensus on these definitions – (see Bendiek, 2012; European Network and Information Security Agency (ENISA), 2012; Parliament of the Commonwealth of Australia (PoA), 2010). Having a consistent definition for cyber security incidents would allow organisations and governments to have a uniform unit of measurement and categories in their data collecting. As Choo (2011) posited, such statistics would allow organisations and government to have a better understanding of the current and emerging cyber threats and are able to develop responses to neutralise such threat/criminal opportunities before they arise.

Acknowledgements

The first author is currently a PhD student in University of South Australia, from Information Assurance Research Group; supported by Ministry of Education, Malaysia (MOE) and University of Tun Hussein Onn Malaysia (UTHM). The views and opinions expressed in this article are those of the authors alone and not the organisations with whom the authors are or have been associated and supported. The authors would also like to thank the anonymous reviewers for providing constructive and generous feedback. Despite their invaluable assistance, any errors remaining in this paper are solely attributed to the authors.

REFERENCES

Abadi M, Abelson H, Acquisti A, Barak B, Bellare M, Bellovin S, et al. Open letter from US researchers in cryptography and information security. <http://masssurveillance.info>; 2014 [viewed 18.06.14].

Afzaal M, Di Sarno C, Coppolino L, DAntonio S, Romano L. A resilient architecture for forensic storage of events in critical infrastructures. In: 2012 IEEE 14th international symposium on high-assurance systems engineering; 2012. p. 48–55.

Agarwal A, Gupta M, Gupta S, Gupta SC. Systematic digital forensic investigation model. Int J Comput Sci Secur IJCSS 2011;5(1):118–67.

Ahmad A, Hadgkiss J, Ruighaver AB. Incident response teams – challenges in supporting the organisational security function. Comput Secur 2012;31(5):643–52.

Al Mutawa N, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. Digit Investig 2012;9(2012):24–33.

Alazab M, Venkatraman S, Watters P. Effective digital forensic analysis of the NTFS disk image. Ubiquitous Comput Commun J 2009;4(3):551–8.

Albakri SH, Shanmugam B, Samy GN, Idris NB, Ahmed A. Security risk assessment framework for cloud computing environments. Secur Commun Netw 2014;7(11):2114–24.

Alberts C, Dorofee A, Killcrece G, Ruefle R, Zajicek M. Defining incident management processes for CSIRTs: a work in progress. 2004. Pittsburgh.

Aleem A, Sprott CR. Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. J Financ Crime 2013;20(1):6–24.

Amazon Web Services. Penetration testing. <https://aws.amazon.com/security/penetration-testing/>; 2014a [viewed 03.05.14].

Amazon Web Services. Vulnerability reporting. <https://aws.amazon.com/security/vulnerability-reporting/>; 2014b [viewed 03.05.14].

Antonio P, Labuschangne L. A conceptual model for digital forensic readiness. In: 2012 Information security for South Africa (ISSA); 2012. p. 1–8.

Anuar NB, Furnell S, Papadaki M, Clarke N. A risk index model for security incident prioritisation. In: Australian information security management conference; 2011. p. 24–39.

Anuar NB, Papadaki M, Furnell S, Clarke N. A response selection model for intrusion response systems: response strategy model (RSM). Secur Commun Netw November 2014;7(11):1831–48.

Ardi S, Shahmehri N. A post-mortem incident modeling method. In: 2009 International conference on availability, reliability and security; 2009. p. 1018–23.

Ariffin A, Choo KR, Slay J. Digital camcorder forensics. In: Proceedings of the eleventh Australasian information security conference; 2013. p. 39–47.

Ariffin A, Dorazio C, Choo K-KR, Slay J. iOS forensics: how can we recover deleted image files with timestamp in a forensically sound manner?. In: 2013 International conference on availability, reliability and security; 2013. p. 375–82.

Ariffin A, Slay J, Choo K. Data recovery from proprietary-formatted CCTV hard disks. Advances in digital forensics IX. Springer Berlin Heidelberg; 2013c. p. 213–23.

BAE Systems Detica. botCloud – an emerging platform for cyber-attacks. <http://baesystemsdetica.blogspot.com.au/>; 2012 [viewed 18.06.14].

Bang J, Lee C, Lee S, Lee K. Damaged backup data recovery method for Windows mobile. J Supercomput 2013;66(2):875–87.

Barske D, Stander A, Jordaan J. A digital forensic readiness framework for South African SMEs. In: 2010 Information security for South Africa; 2010. p. 1–6.

Bashir MN, Kesan JP, Hayes CM, Zielinski R. Privacy in the cloud: going beyond the contractarian paradigm. In: Proceedings of the 2011 workshop on governance of technology, information, and policies; 2011. p. 21–7.

Baskerville R, Spagnoletti P, Kim J. Incident-centered information security: managing a strategic balance between prevention and response. Inf Manag 2014;51(1):138–51.

Bendiek A. European cyber security policy. SWP research paper 13. Berlin: German Institute for International and Security Affairs; 2012.

Bhilare DS, Ramani AK, Tanwani S. An architecture for a distributed collaborative inter university incident handling mechanism. Int J Comput Internet Secur 2010;2(1):29–39.

Bojanc R. A quantitative model for information-security risk management. Eng Manag J 2013;25(2):25–37.

British Standards Institution. BIP 0107:2008 foundations of IT service management based on Itil V3, UK. 2007.

Butler A, Choo K. IT standards and guides do not adequately prepare IT practitioners to appear as expert witnesses: an Australian perspective. Secur J 2013:1–20.

Cárdenas AA, Amin S, Lin Z. Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM symposium on information, computer and communications security; 2011. p. 355–66.

Caskurlu B, Gehani A, Bilgin CC, Subramani K. Analytical models for risk-based intrusion response. Comput Netw 2013;57(10):2181–92.

Chivers H, Clark JA, Cheng P-C. Risk profiles and distributed risk assessment. Comput Secur 2009;28(7):521–35.

Choo K-KR. The cyber threat landscape: challenges and future research directions. Comput Secur 2011;30(8):719–31.

Choo K-KR. A cloud security risk-management strategy. IEEE Cloud Comput 2014a;1(2):52–6.

Choo K-KR. A conceptual interdisciplinary plug-and-play cyber security framework. In: Kaur H, Tao X, editors. ICTs and the millennium development goals – a United Nations perspective. New York, USA: Springer; 2014b. p. 81–99.

Choo K-KR. Legal issues in the cloud. IEEE Cloud Comput Mag 2014:94–6.

Chung H, Park J, Lee S, Kang C. Digital forensic investigation of cloud storage services. Digit Investig 2012;9(2):81–95.

Cichonski P, Scarfone K. Computer security incident handling guide recommendations of the National Institute of Standards and Technology (NIST). Gaithersburg: NIST; 2012.

Clarke RA, Morell MJ, Stone GR, Sunstein CR, Swire P. Liberty and security in a changing world: report and recommendations of the Presidents Review Group on Intelligence and Communications Technologies. Washington, D.C.: Group on Intelligence and Communication; 2013.

Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing. CSA; 2011. <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf> [viewed 01.08.14].

CMMI Product Team. CMMI® for services. Version 1.3. Pittsburgh: CMU/SEI; 2010.

Cohen F. Toward a science of digital forensic evidence examination. Advances in digital forensics VI. Springer Berlin Heidelberg; 2009. p. 17–35.

Connell A, Waits T. The CERT assessment tool: increasing a security incident responders ability to assess risk. In: 2013 IEEE international conference on technologies for homeland security (HST); 2013. p. 236–40.

Connell A, Palko T, Yasar H. Cerebro: a platform for collaborative incident response and investigation. In: 2013 IEEE international conference on technologies for homeland security (HST); 2013. p. 241–5.

Cusack B, Kyaw AK. Forensic readiness for wireless medical systems. In: Australian digital forensics conference; 2012. p. 21–32.

Cusick JJ, Ma G. Creating an ITIL inspired incident management approach: roots, response, and results. In: 2010 IEEE/IFIP network operations and management symposium workshops; 2010. p. 142–8.

Daley R, Millar T, Osorno M. Operationalizing the coordinated incident handling model. In: Technologies for homeland security (HST), 2011 IEEE international conference on; 2011. p. 287–94.

Dekker M, Liveri D, Lakka M. Cloud security incident reporting framework for reporting about major cloud security incidents. Athens: ENISA; 2013.

Ding X, Road DC, District MH. Time based data forensic and cross-reference analysis. In: Proceedings of the 2011 ACM symposium on applied computing; 2011. p. 185–90.

Dykstra J, Sherman AT. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. Digit Investig 2012;9:90–8.

D'Orazio C, Ariffin A, Choo KR. iOS anti forensics: how can we securely conceal, delete and insert data?. In: 47th Hawaii international conference on system sciences; 2014. p. 4838–47.

Elyas M, Maynard SB, Ahmad A, Lonie A. Towards a systematic framework for digital forensic readiness. J Comput Inf Syst 2014;54(3):97–106.

European Network and Information Security Agency (ENISA). Good practice guide for incident management. Athens: ENISA; 2010.

European Network and Information Security Agency (ENISA). National cyber security strategies. Athens: ENISA; 2012.

Farina J, Scanlon M, Kechadi M-T. BitTorrent Sync: first impressions and digital forensic implications. Digit Investig 2014;11(2014):77–86.

Federal Office for Information Security. Security recommendations for cloud computing providers. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile>; 2011 [viewed 21.10.14].

Fessi BA, Benabdallah S, Boudriga N, Hamdi M. A multi-attribute decision model for intrusion response system. Inf Sci 2014;270(2014):237–54.

Freiling FC, Schwittay B. A common process model for incident response and computer forensics. In: Proceedings of the 2007 IT incident management & IT forensics (IMF 2007), vol. 7; 2007. p. 19–40.

Frühwirth C, Männistö T. Improving CVSS-based vulnerability prioritization and response with context information. In: 3rd International symposium on empirical software engineering and measurement; 2009. p. 535–44.

Garfinkel S, Nelson AJ, Young J. A general strategy for differential forensic analysis. Digit Investig 2012;9(2012):50–9.

Grobauer B, Schreck T. Towards incident handling in the cloud. In: Proceedings of the 2010 ACM workshop on cloud computing security workshop (CCSW 10); 2010. p. 77–85.

Grobler M, Bryk H. Common challenges faced during the establishment of a CSIRT. In: 2010 Information security for South Africa; 2010. p. 1–6.

Grobler CP, Louwrens CP, von Solms SH. A framework to guide the implementation of proactive digital forensics in organisations. In: 2010 International conference on availability, reliability and security; 2010. p. 677–82.

Grover J. Android forensics: automated data collection and reporting from a mobile device. Digit Investig 2013;10(2013):12–20.

Guo W, Wang Y. An incident management model for SaaS application in the IT organization. In: 2009 International conference on research challenges in computer science; 2009. p. 137–40.

Gurkok C. Cyber forensics and incident response. Computer and information security handbook. 2nd ed. Elsevier Inc.; 2013. p. 601–22.

Hadjidj R, Debbabi M, Lounis H, Iqbal F, Szporer A, Benredjem D. Towards an integrated e-mail forensic analysis framework. Digit Investig 2009;5(3–4):124–37.

He W, Yuan X, Yang L, Science C. Supporting case-based learning in information security with web-based technology. J Inf Syst Educ 2013;24(1):31–41.

He Y, Johnson C, Renaud K, Lu Y, Jebrieli S. An empirical study on the use of the generic security template for structuring the lessons from information security incidents. In: 2014 6th International conference on CSIT; 2014. p. 178–88.

Herrmann A, Morali A, Etalle S, Wieringa R. RiskREP: risk-based security requirements elicitation and prioritization. Enschede: Centre for Telematics and Information Technology (University of Twente); 2011. p. 1–8.

Hooper C, Martini B, Choo K-KR. Cloud computing and its implications for cybercrime investigations. Aust Comput Law Secur Rev 2013;29(2):152–63.

Hove C, Marte T. Information security incident management: an empirical study of current practice. Norwegian University of Science and Technology; 2013.

Hove C, Marte T, Line MB, Bernsmed K. Information security incident management: identified practice in large organizations. In: 2014 Eighth international conference on IT security incident management & IT forensics; 2014. p. 27–46.

Hsu CT, Luo GH, Yuan SM. Personalized cloud storage system: a combination of LDAP distributed file system. Genetic and

evolutionary computing. Springer International Publishing; 2014. p. 399–408.
Husain MI, Sridhar R. iForensics: forensic analysis of instant messaging on smart phones. Digital forensics and cyber crime. Springer Berlin Heidelberg; 2010. p. 9–18.
Inglot B, Liu L. Enhanced timeline analysis for digital forensic investigations. Inf Secur J A Glob Perspect 2014:1–13.
International Standard for Organisation. ISO/IEC 27035:2011 information technology – security techniques – information security incident management. 2011. Geneva.
Irwin D, Slay J. Extracting evidence related to VoIP calls. Advances in digital forensics VII. Springer Berlin Heidelberg; 2011. p. 221–8.
Ismail S, Ahmad A, Afizi M, Shukran M. New method of forensic computing in a small organization. Aust J Basic Appl Sci 2011;5(9):2019–25.
Jansen W, Grance T. Guidelines on security and privacy in public cloud computing. Gaithersburg: NIST; 2011.
Johnson LR. The stages of incident response, computer incident response and forensics team management. 2014. p. 21–35.
Jung J, Jeong C, Byun K, Lee S. Sensitive privacy data acquisition in the iPhone for digital forensic analysis. Secure and trust computing, data management and applications. Springer Berlin Heidelberg; 2011. p. 172–86.
Junqueira FP, Reed BC, Serafini M. Zab: high-performance broadcast for primary-backup systems. In: 2011 IEEE/IFIP 41st international conference on dependable systems & networks (DSN); 2011. p. 245–56.
Kaart M, Laraghy S. Android forensics: interpretation of timestamps. Digit Investig 2014:1–15.
Kácha P. Adapting the ticket request system to the needs of CSIRT teams. WSEAS Trans Comput 2009;8(9):1440–50.
Kearney W, Kruger H. Effective corporate governance: combining an ICT security incident and organisational learning. In: The 2nd international conference on cyber security, cyber peacefare and digital forensic (CyberSec 2013); 2013. p. 12–21.
Kheir N, Cuppens-Boulahia N. A service dependency model for cost-sensitive intrusion response. Computer security–ESORICS 2010. Springer Berlin Heidelberg; 2010. p. 626–42.
Kheir N, Debar H, Boulahia CN, Cuppens F, Viinikka J. Cost evaluation for intrusion response using dependency graphs. In: Network and service security, 2009, N2S09. International conference on; 2009. p. 1–6.
Khorshed T, Ali ABMS, Wasimi SA. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener Comput Syst 2012;28(6):833–51.
Khurana H, Basney J, Bakht M, Freemon M, Welch V, Butler R. Palantir: a framework for collaborative incident response and investigation. In: Proceedings of the 8th symposium on identity and trust on the internet; 2009. p. 38–51.
Killcrece G. State of the practice of computer security incident response teams (CSIRTs). Pittsburgh: CMU/SEI; 2003.
Killcrece G, Kossakowski K-P, Ruefle R, Zajicek M. Organizational models for computer security incident response teams (CSIRTs). Pittsburgh: CMU/SEI; 2003.
Kim S-H, Choi S-S, Park H-S, Choi J-W. Advanced bot response mechanism based on DNS sinkhole. Inf Int Interdiscip J 2011;14(7):2499–521.
Klein G, Rogge H, Schneider F, Toelle J, Jahnke M, Karsch S. Response initiation in distributed intrusion response systems for tactical MANETs. In: 2010 European conference on computer network defense; 2010. p. 55–62.
Kohn MD, Eloff MM, Eloff JHP. Integrated digital forensic process model. Comput Secur 2013;38(2013):103–15.
Koivunen E. Why wasn't I notified?: information security incident reporting demystified. Information security technology for application. Springer Berlin Heidelberg; 2012. p. 55–70.
Kostina A, Miloslavskaya N, Tolstoy A. Information security incident management process. In: Proceedings of the 2nd international conference on security of information and networks – SIN; 2009. p. 93.
Kozlovszky M, Kovacs L, Torocsik M, Windisch G, Acs S, Prem D, et al. Cloud security monitoring and vulnerability management. In: IEEE 17th international conference on intelligent engineering systems; 2013. p. 265–9. No. 70.
Kral P. Incident handler handbook. SANS Institute; 2011.
Krichene J, Boudriga N. Incident response probabilistic cognitive maps. In: 2008 IEEE international symposium on parallel and distributed processing with applications; 2008. p. 689–94.
Kulikova O, Heil R, van den Berg J, Pieters W. Cyber crisis management: a decision-support framework for disclosing security incident information. In: 2012 International conference on cyber security; 2012. p. 103–12.
Kundu A, Ghosh SK. Game theoretic attack response framework for enterprise networks. Distributed computing and internet technology. Springer International Publishing; 2014. p. 263–74.
Kurowski S, Frings S. Computational documentation of IT incidents as support for forensic operations. In: 2011 Sixth international conference on IT security incident management and IT forensics; 2011. p. 37–47.
Landman M. Managing smart phone security risks. In: 2010 Information security curriculum development conference on – InfoSecCD; 2010. p. 145.
Lee J, Hong D. Pervasive forensic analysis based on mobile cloud computing. In: 2011 Third international conference on multimedia information networking and security; 2011. p. 572–6.
Lee W, Fan W, Miller M, Stolfo S, Zadok E. Toward cost-sensitive modeling for intrusion detection and response. J Comput Secur 2002;10(2):5–22.
Li H, Tian X, Wei W, Sun C. A deep understanding of cloud computing security issues in cloud computing. Network computing and information security. Springer Berlin Heidelberg; 2012. p. 98–105.
Line MB. A case study: preparing for the smart grids – identifying current practice for information security incident management in the power industry. In: 2013 Seventh international conference on IT security incident management and IT forensics; 2013. p. 26–32.
Luo Y, Szidarovszky F, Al-Nashif Y, Hariri S. A fictitious play-based response strategy for multistage intrusion defense systems. Secur Commun Netw 2014;2014(7):473–91.
Ma WM. Study on architecture-oriented information security risk assessment model. Computational collective intelligence: technologies and applications. Springer Berlin Heidelberg; 2010. p. 218–26.
Marinescu DC. Cloud infrastructure. Cloud computing: theory and practice. 1st ed. Elsevier Inc.; 2013. p. 67–98.
Martini B, Choo K-KR. An integrated conceptual digital forensic framework for cloud computing. Digit Investig 2012;9(2):71–80.
Martini B, Choo K-KR. Cloud storage forensics: ownCloud as a case study. Digit Investig 2013;10(4):1–13.
Martini B, Choo KR. Distributed filesystem forensics: XtreemFS as a case study. Digit Investig 2014;11(4):295–313. http://dx.doi.org/10.1016/j.diin.2014.08.002.
McKemmish R. What is forensic computing? Trends Issue Crime Crim Justice 1999;1999(118):1–6.
Mitropoulos S, Patsos D, Douligeris C. On incident handling and response: a state-of-the-art approach. Comput Secur 2006;25(5):351–70.
Modi C, Patel D, Borisaniya B. A survey on security issues and solutions at different layers of cloud computing. J Supercomput 2013;63(2):561–92.

Monfared A, Jaatun MG. Handling compromised components in an IaaS cloud installation. J Cloud Comput Adv Syst Appl 2012;1(1):1–21.
Morrissey S. iOS forensic analysis for iPhone, iPad, and iPod touch. APress; 2010.
Moser A, Cohen MI. Hunting in the enterprise: forensic triage and incident response. Digit Investig 2013;10(2):89–98.
Mu C, Li Y. An intrusion response decision-making model based on hierarchical task network planning. Expert Syst Appl 2010;37(3):2465–72.
Murray R, Ruefle M. CSIRT requirements for situational awareness. Pittsburgh: CMU/SEI; 2014.
MyCERT. MyCERT incident statistics. <http://www.mycert.org.my/en/services/statistic/mycert/2014/main/detail/949/index.html>; 2013 [viewed 02.04.014].
Mylonas A, Meletiadis V, Tsoumas B, Mitrou L. Smartphone forensics: a proactive investigation scheme for evidence acquisition, in information security and privacy research. Springer Berlin Heidelberg; 2012. p. 249–60.
Ngobeni S, Venter H, Burke I. A forensic readiness model for wireless networks. Advances in digital forensic VII. Springer Berlin Heidelberg; 2010. p. 107–17.
Ngobeni S, Venter H, Burke I. The modelling of a digital forensic readiness approach for wireless local area networks. J Univers Comput Sci 2012;18(12):1721–40.
Nikkel BJ. Fostering incident response and digital forensics research. Digit Investig December 2014;11(4):249–51. http://dx.doi.org/10.1016/j.diin.2014.09.004.
Nowruzi M, Jazi HH, Dehghan M, Shahmoradi M, Hashemi SH, Babaeizadeh M. A comprehensive classification of incident handling information. In: 6th International symposium on telecommunications (IST); 2012. p. 1071–5.
Ntantogian C, Apostolopoulos D, Marinakis G, Xenakis C. Evaluating the privacy of Android mobile applications under forensic analysis. Comput Secur 2014;42(2014):66–76.
Omeleze S, Venter HS. Testing the harmonised digital forensic investigation process model-using an Android mobile phone. In: 2013 Information security for South Africa; 2013. p. 1–8.
Ongaro D, Rumble SM, Stutsman R, Ousterhout J, Rosenblum M, Organization DOS, et al. Fast crash recovery in RAMCloud. In: Proceedings of the 23rd ACM symposium on operating systems principles; 2011. p. 29–41.
Owen P, Thomas P. An analysis of digital forensic examinations: mobile devices versus hard disk drives utilising ACPO & NIST guidelines. Digit Investig 2011;8(2):135–40.
Pangalos G, Ilioudis C, Pagkalos I. The importance of corporate forensic readiness in the information security framework. In: 2010 19th IEEE international workshops on enabling technologies: infrastructures for collaborative enterprises; 2010. p. 12–6.
Patel A, Taghavi M, Bakhtiyari K, Celestino Júnior J. An intrusion detection and prevention system in cloud computing: a systematic review. J Netw Comput Appl 2013;36(1):25–41.
Pereira MT. Forensic analysis of the Firefox 3 internet history and recovery of deleted SQLite records. Digit Investig 2009;5(3–4):93–103.
Pilli ES, Joshi RC, Niyogi R. A generic framework for network forensics. Int J Comput Appl 2010;1(11):1–6.
Ping L, Haifeng Y, Guoqing M. An incident response decision support system based on CBR and ontology. In: 2010 International conference on computer application and system modeling (ICCASM 2010); 2010. V11–337.
Parliament of the Commonwealth of Australia (PoA). Hackers, fraudsters and botnets: tackling the problem of cyber crime. Canberra: PoA; 2010.
Ponemon Institute. 2013 Cost of cyber crime study: United States. 2013.
Poolsappasit N, Dewri R, Ray I. Dynamic security risk management using Bayesian attack graphs. IEEE Trans Dependable Secure Comput 2012;9(1):61–74.
Proctor T. The development of warning, advice and reporting points (WARPs) in UK national infrastructure. In: Critical information infrastructure security. Springer Berlin Heidelberg; 2013. p. 164–74.
Quick D, Choo K-KR. Digital droplets: Microsoft SkyDrive forensic data remnants. Future Gener Comput Syst 2013a;29(6):1378–94.
Quick D, Choo K-KR. Dropbox analysis: data remnants on user machines. Digit Investig 2013b;10(1):3–18.
Quick D, Choo K-KR. Forensic collection of cloud storage data: does the act of collection result in changes to the data or its metadata? Digit Investig 2013c;10(3):266–77.
Quick D, Choo K-KR. Data reduction and data mining framework for digital forensic evidence: storage, intelligence, review and archive. Trends Issues Crime Crim Justice 2014a;480:1–11.
Quick D, Choo K-KR. Google drive: forensic analysis of cloud storage data remnant. J Netw Comput Appl 2014b;40(2014):179–93.
Quick D, Choo K-KR. Impacts of increasing volume of digital forensic data: a survey and future research challenges. Digit Investig December 2014;11(4):273–94. http://dx.doi.org/10.1016/j.diin.2014.09.002.
Quick D, Martini B, Choo K-KR. Cloud storage forensics. Syngress; 2014.
Reddy K, Venter H. A forensic framework for handling information. Advances in digital forensics V. Springer Berlin Heidelberg; 2009. p. 143–55.
Rong C, Nguyen ST, Jaatun MG. Beyond lightning: a survey on security challenges in cloud computing. Comput Electr Eng 2013;39(1):47–54.
Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud forensics. Advances in digital forensic VII. Springer Berlin Heidelberg; 2011. p. 35–46.
Ruefl R, Dorofee A, Mundie D, Householder AD, Murray M, Perl SJ. Computer security incident response team development and evolution. IEEE Secur Priv 2014;12(5):16–26.
Sarkar SR, Mahindru R, Hosn RA, Vogl N, Ramasamy HV. Automated incident management for a platform-as-a-service cloud. In: Proceedings of the 11th USENIX conference on hot topics in management of internet, cloud, and enterprise network and services; 2011. p. 5–11.
Satoh N, Kumamoto H. Analysis of information security problem by probabilistic risk assessment. Int J Comput 2009;3(3):337–47.
Shameli-Sendi A, Dagenais M. ARITO: cyber-attack response system using accurate risk impact tolerance. Int J Inf Secur 2013;(2013):1–24.
Shameli-Sendi A, Ezzati-Jivan N, Jabbarifar M, Dagenais M. Intrusion response systems: survey and taxonomy. Int J Comput Sci Netw Secur 2012;12(1):1–14.
Shameli-Sendi A, Cheriet M, Hamou-Lhadj A. Taxonomy of intrusion risk assessment and response system. Comput Secur 2014;45:1–16.
Shedden P, Ahmad A, Ruighaver AB. Organisational learning and incident response: promoting effective learning through the incident response process. In: Australian information security management conference; 2010. p. 131–42.
Shedden P, Ahmad A, Ruighaver AB. Informal learning in security incident response teams. In: Proceedings of 2011 Australasian conference on information system (ACIS); 2011. p. 1–11.
Shedden P, Scheepers R, Smith W, Ahmad A. Incorporating a knowledge perspective into security risk assessments. VINE J Inf Knowl Manag Syst 2011b;41(2):152–66.

Shields C, Frieder O, Maloof M. A system for the proactive, continuous, and efficient collection of digital forensic evidence. Digit Investig 2011;8(2011):3–13.
Shosha AF, James JI, Hannaway A, Liu C, Gladyshev P, Shosha A. Towards automated malware behavioral analysis and profiling for digital forensic investigation purposes. Digital forensics and cyber crime. Springer Berlin Heidelberg; 2013. p. 66–80.
Simon M, Choo K-KR. Digital forensics: challenges and future research directions. In: Kim I-S, Liu J, editors. Contemporary trends in Asian criminal justice: paving the way for the future. Seoul: Korean Institute of Criminology; 2014. p. 105–46.
Sindoori R, Pallavi PV, Abinaya P. 2012 An overview of disaster recovery in virtualization technology. J Artif Intell 2012;6(2013):60–7.
Slay J, Sitnikova E. The development of a generic framework for the forensic analysis of SCADA and process control systems. Forensics in telecommunications, information and multimedia. Springer Berlin Heidelberg; 2009. p. 77–82.
Srinivasan MK, Rodrigues P. State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud. In: Proceedings of the international conference on advances in computing, communications and informatics; 2012. p. 470–6.
Stakhanova N, Basu S, Wong J. A cost-sensitive model for preemptive intrusion response systems. In: 21st International conference on advanced networking and applications (AINA); 2007. p. 428–35.
Stakhanova N, Basu S, Wong J. A taxonomy of intrusion response systems. Int J Inf Comput Secur 2007b;1(1/2):169–84.
Strasburg C, Stakhanova N, Basu S, Wong JS. A framework for cost sensitive assessment of intrusion response selection. In: 2009 33rd Annual IEEE international computer software and applications conference; 2009. p. 355–60.
Strasburg C, Stakhanova N, Basu S, Wong JS. Intrusion response cost assessment methodology. In: Proceedings of the 4th international symposium on information, computer, and communications security – ASIACCS; 2009. p. 388–91.
Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 2011;34(1):1–11.
Sylve J, Case A, Marziale L, Richard GG. Acquisition and analysis of volatile memory from Android devices. Digit Investig 2012;8(3–4):175–84.
Symantec. 2013 Norton report: total cost of cybercrime in Australia amounts to AU$1.06 billion. 2013 [viewed 02.04.14], <http://www.symantec.com/en/au/about/news/release/article.jsp?prid=20131015_01>.
Takabi H, James BJ, Gail JA. Security and privacy challenges in cloud computing environments. IEEE Secur Priv Mag 2010;8(6):24–31.
Tan Y, Jiang H, Feng D, Tian L, Yan Z. CABdedupe: a causality-based deduplication performance booster for cloud backup services. In: 2011 IEEE international parallel & distributed processing symposium; 2011. p. 1266–77.
Taylor LP. Developing an incident response plan. FISMA compliance handbook. 2nd ed. 2013. p. 95–115.
Taylor M, Haggerty J, Gresty D, Lamb D. Forensic investigation of cloud computing systems. Netw Secur 2011;2011(3):4–10.
Theoharidou M, Kotzanikolaou P, Gritzalis D. Risk assessment methodology for interdependent critical infrastructures. Int J Risk Assess Manag 2011;15(2/3):128–48.
Theoharidou M, Mylonas A, Gritzalis D. A risk assessment method for smartphones. Information security and privacy research. Springer Berlin Heidelberg; 2012. p. 443–56.
Thethi N, Keane A. Digital forensics investigations in the cloud. In: 2014 IEEE international advance computing conference (IACC); 2014. p. 1475–80.
Tøndel IA, Line MB, Jaatun MG. Information security incident management: current practice as reported in the literature. Comput Secur 2014;45(2014):42–57.
Trček D, Abie H, Skomedal A, Starc I. Advanced framework for digital forensic technologies and procedures. J Forensic Sci 2010;55(6):1471–80.
Trenwith PM, Venter HS. Digital forensic readiness in the cloud. 2013 Information security for South Africa. 2013. p. 1–5.
US District Court for the District of Columbia. Morandum opinion: civil action no. 13-0851 (RJL). 2013. <http://s3.documentcloud.org/documents/901810/klaymanvobama215.pdf> [viewed 18.06.14].
U.S. GAO. Information security: agencies need to improve cyber incident response practices. Washington: United States Government Accountability Office; 2014.
Usmani K, Mohapatra AK, Prakash N. An improved framework for incident handling. Inf Secur J Glob Perspect 2013;22(1):1–9.
Valiente M-C, Garcia-Barriocanal E, Sicilia M-A. Applying an ontology approach to IT service management for business–IT integration. Knowl Based Syst 2012;28(2012):76–87.
Valjarevic A, Venter HS. Towards a digital forensic readiness framework for public key infrastructure systems. 2011 Information security for South Africa. 2011. p. 1–10.
Valjarevic A, Venter H. A harmonized process model for digital forensic investigation. In: Peterson G, Shenoi S, editors. Advances in digital forensic IX, IFIP AICT. Springer Berlin Heidelberg; 2013. p. 67–82.
Vidas T, Zhang C, Christin N. Toward a general collection methodology for Android devices. Digit Investig 2011;8(2011):14–24.
Webb J, Ahmad A, Maynard SB, Shanks G. A situation awareness model for information security risk management. Comput Secur 2014;2014:1–15.
West-Brown MJ, Stikvoort D, Kossakowski K-P, Killcrere G, Ruefle R, Zajicek M. Handbook for computer security incident response teams (CSIRTs). 2nd ed. Pittsburgh: Carnegie Mellon/SEI; 2003.
Wiik J, Davidsen PI, Kossakowski KP. Chronic workload problems in CSIRTs. In: 27th International conference of the system dynamics society; 2009. p. 1–19.
Wiik J, Davidsen PI, Kossakowski KP. Persistent instabilities in the high-priority incident workload of CSIRTs. In: 27th International conference of the system dynamics society; 2009. p. 1–15.
Wiik J, Davidsen PI, Kossakowski KP. Preserving a balanced CSIRT constituency. In: 27th International conference of the system dynamics society; 2009. p. 1–11.
Wood T, Cecchet E, Ramakrishnan KK, Shenoy P, Merwe J Van Der, Venkataramani A. Disaster recovery as a cloud service: economic benefits & deployment challenges University of Massachusetts Amherst. In: 2nd USENIX workshop on hot topics in cloud computing; 2010. p. 1–7.
Wu X, Fu Y, Wang J. Information systems security risk assessment on improved fuzzy AHP. In: 2009 ISECS international colloquium on computing, communication, control, and management; 2009. p. 365–9.
Wu T, Ferdinand J, Disso P, Jones K, Campos A, Pagna J. Towards a SCADA forensics architecture. In: 1st International symposium for ICS and SCADA cyber security research; 2013. p. 12–21.
Xia R, Yin X, Alonso J, Machida F, Trivedi KS. Performance and availability modeling of IT systems with data backup and restore. IEEE Trans Dependable Secure Comput 2013:1–14.
Xinlan Z, Zhifang H, Guangfu W, Xin Z. Information security risk assessment methodology research: group decision making and analytic hierarchy process. In: 2010 Second world congress on software engineering; 2010. p. 157–60.

Yang J, Chen Z. Cloud computing research and security issues. In: Computational intelligence and software engineering (CiSE), 2010 international conference on; 2010. p. 10–2.

Yu X, Jiang L, Shu H, Yin Q, Liu T. A process model for forensic analysis of Symbian. Advances in software engineering. Springer Berlin Heidelberg; 2009. p. 86–93.

Yuill J, Wu F, Settle J, Gong F, Forno R, Huang M, et al. Intrusion-detection for incident-response, using a military battlefield-intelligence process. Comput Netw 2000;34(2000):671–97.

Zambon E, Etalle S, Wieringa RJ, Hartel P. Model-based qualitative risk assessment for availability of IT infrastructures. Softw Syst Model 2010;10(4):553–80.

Zan X, Gao F, Han J, Liu X, Zhou J. NAIR: a novel automated intrusion response system based on decision making approach. In: The 2010 IEEE international conference on information and automation; 2010. p. 543–8.

Zhang L, Wang W. Constructions on disaster tolerant backup system of management information system. In: 2011 6th International conference on computer science & education (ICCSE); 2011. p. 425–7.

Zhang X, Wuwong N, Li H, Zhang X. Information security risk management framework for the cloud computing environments. In: 2010 10th IEEE international conference on computer and information technology; 2010. p. 1328–34.

Zhang G, Yang Y, Mao X. Disaster recovery evaluation PROC model framework based on information flow. In: Proceedings of 2011 international conference on computer science and network technology; 2011. p. 1841–5.

Zhang X, Liang K, Zhang X. Research on the recovery strategy of incremental-data-based continuous data protection. In: 2012 International conference on computer science and electronics engineering; 2012. p. 498–502.

Zhao W, White G. Designing a formal model facilitating collaborative information sharing for community cyber security. In: 2014 47th Hawaii international conference on system sciences; 2014. p. 1987–96.

Zhou M, Yao G. Improved cost-sensitive model of intrusion response system based on clustering. In: 2011 International conference in electrics, communication and automatic control proceedings; 2012. p. 931–7.

Zimmerman S, Glavach D. Cyber forensics in the cloud. IAnewsletter 2011;14(1):4–7.

Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst 2012;28(3):583–92.

Zonouz S, Haghani P. Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators responsive behavior. Comput Secur 2013;39(2013):190–200.

Zonouz SA, Khurana H, Sanders WH, Yardley TM. RRE: a game-theoretic intrusion response and recovery engine. IEEE Trans Parallel Distrib Syst 2014;25(2):395–406.

Nurul Hidayah Ab Rahman is a PhD Scholar at the University of South Australia, funded by the Malaysia Ministry of Education. Her research interests include Cloud Security Management, and she has a Master in Computer Science (Information Security) from Universiti Teknologi Malaysia. She is also an academic staff member at Universiti Tun Hussein Onn Malaysia.

Dr Kim-Kwang Raymond Choo is a Fulbright Scholar and Senior Lecturer at the University of South Australia. His publications include a book in Springer's "Advances in Information Security" series and a book published by Elsevier (Forewords written by Australia's Chief Defence Scientist and Chair of the Electronic Evidence Specialist Advisory Group). His awards include the British Computer Society's Wilkes Award for the best paper published in the 2007 volume of Computer Journal. He is the editor of IEEE Cloud Computing Magazine's "Cloud and the Law" column and the Book Series Editor of Syngress/Elsevier's "Advanced Topics in Security, Privacy and Forensics".