Athens Journal of Sciences- Volume 5, Issue 2 – Pages 167-182

A Strategic Model for Forensic Readiness

By Jan Collie[*]

Forensic readiness has been defined as: '...the capability of an organisation to use digital evidence in a forensic investigation'. For businesses, especially medium or small enterprises, gaining this capability can seem time consuming and expensive: it may involve a number of processes, it may require new hardware and software and people with specialised skill sets may need to be hired in order to implement any plan. Yet developing and maintaining a forensic readiness capability is vital in the digital age. Fraud and cybercrime cost almost £11bn in the UK alone last year. Across the European Union, the national annual cost of cybercrime now accounts for 0.41% of GDP. Recent figures have also shown that up to 62% of digital incidents are caused by insiders, either accidentally or knowingly. An astonishing 91% of cybersecurity attacks begin with a single email. This research proposes a structured, strategic approach to forensic readiness for businesses that is economic to implement and run. It is based on people and processes rather than complex electronic systems. Key to this approach is a firm's best asset - its own staff. It is theorised that the foundation stone of forensic readiness is a strong internal security culture. In order to achieve this aim, a unique, scalable model for efficient and inclusive planning is put forward with a reporting construct which aims to assure company-wide involvement.

Keywords: *Data security, Forensic readiness, Incident response, Information security culture.*

Introduction

Forensic Readiness is a relatively new concept and one that is difficult to define since it can be conceived in more than one way. The term was invented by Tan (2001) but not defined by him. Instead, he identified two objectives for Forensic Readiness:

1. Maximising an environment's ability to collect credible digital evidence; and
2. Minimising the cost of forensics in an incident response.

Rowlingson (2004) put these objectives into a single statement and presented Forensic Readiness as: 'the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation', although he added: 'Forensic readiness is incident anticipation compared with incident response.' Other authorities have also tended to centre attention on preserving and gathering digital evidence (Hoolachan and Glisson, 2010; NHS, 2009; Garcia, 2005) and a number of first responder guides have been produced, in particular by law enforcement and government agencies. These are briefly discussed in

[*]Senior Digital Forensic Investigator, Discovery Forensics Ltd, UK.

https://doi.org/10.30958/ajs.5-2-4 doi=10.30958/ajs.5-2-4

this paper but it is clear that although gathering digital evidence is a vital element of forensic readiness it is, nevertheless, only one element. Furthermore, minimising the cost of incident response is a desired outcome and should flow from effective incident handling since better business continuity can be maintained (Jaatun et al., 2009).

Whilst a significant body of research exists around the concept of forensic readiness, a comprehensive literature review has shown that two quite separate approaches to it have normally been adopted. Broadly, these are that forensic readiness can be achieved either:

a) Via policies and procedures aimed at improving organisational data security.
   or
b) Via technical mechanisms aimed at locking down networked computer systems.

A more integrated approach has been proposed by Pooe and Labuschagne (2012) who considered the main activities involved and produced a conceptual model. Pooe and Labuschagne's research identified four core activities within this model, which they classified as: People, Process, Policy and Technology. Within these categories are sub-categories such as organisational requirements and security awareness. Another model, focusing on the types of expertise needed in implementing forensic readiness, has been put forward by Collie (2011) who observed that since data security, system security, risk assessment and risk management all have a part to play, organisations need to assimilate aspects of each rather than making them the preserve of different departments.

A move towards an aggregated view of forensic readiness is now being supported by a number of authorities worldwide. This is seen to be an imperative, since interconnectivity between people, machines and cyberspace is growing at an unprecedented pace. This makes people vulnerable to exploitation both during their working lives and personal lives. Combatting cybercrime can now be described as a permanent struggle rather than a matter of dealing with a distinct series of events (Cardiff University, 2015). Where organisations used to concentrate on defending their communications boundaries, the mood is shifting towards a holistic approach to cybersecurity, the SANS Institute has noted (2001). A key part of this approach is to recognise and prepare for insider threat since it is now increasingly acknowledged that people are the 'weakest link' when it comes to data security. Whether inadvertently or deliberately staff is calculated to be responsible for up to 62% of digital security incidents. In 91% of cases, cybersecurity attacks have been initiated via a single email (Bunker and Kosciuk, 2017). As Alumubark et al (2015) put it: 'Information security begins and ends with people.' In order to understand the cause of information leaks, they state, the relationship between individuals and organisations needs to be explored.

The study of people and their attitude to information security in the workplace represents a third area of research. Surveys carried out over the past ten years

have shown that employees are frequently careless, ignoring or by-passing secure practices and that they fail to comply with company security policies (Ponemon/Dtex, 2016). A root cause is that organisations often fail to develop a shared system of values, beliefs and behaviours amongst staff. The way forward, a number of authorities claim, is to build and maintain a strong information security culture (ISC) (Da Veiga and Eloff, 2010, Schlienger and Teufel, 2003, Von Solms, 2000). This goal needs to be strongly supported by executives and senior management in order to ensure that funding is available and to make high-level decisions e.g. about outsourcing (Tuck School, 2016). These ideas have gained popularity amongst businesses but researchers have found that there is a gap between talking about good security practices and actually implementing them. This may be because there is a lack of information on how ISC can be embedded into corporate culture, according to Lim et al (2010). The same research team carried out case studies on embedding ISC into two different companies and found that it was: '…not as simple as changing employee behaviours and the technical aspects of security.' Instead, they pointed out, there are a number of other important elements, including the involvement of senior management, maintaining both an awareness program and enforcement process and allocating sufficient budget to the in-house ISC program.

The literature review carried out during the development this paper had found that although a large body of work exists around the subject of forensic readiness, approaches to it are very diverse, ranging from the technical to the psychological. The research shows that there is a need to draw these elements together. There is also a need to encapsulate how businesses can grow an ISC. To this end, the main areas of discussion are expanded in the next section and conceptual models, presented in the "Modelling Forensic Readiness" section, are devised to support the argument that two key components of forensic readiness are an incident management strategy based on company-wide involvement and an iterative, think-tank approach to planning. The value of this research proposition is put forward in the "Research Value Proposition" section, followed by a conclusion and suggestions for future research in the last section.

Discussion

Data Security: The Cybercrime Landscape and Insider Threat

Data security is one of the greatest problems of the information age. With incidents of accidental loss and deliberate misappropriation rising, businesses and individuals struggle to keep their intellectual property protected and their personal details private. For the everyday user, identity theft is an increasing threat. Merely accessing the Internet and receiving email makes them prey to continual phishing scams, virus attacks and spyware intrusions. The UK fraud prevention service Cifas, has reported that criminals are now making a point of targeting youth (Cifas, 2016). It has also been shown that social networking puts computer and mobile phone users at a higher risk. An annual survey

carried out in the USA reported that users of platforms such as Facebook, Instagram and Snapchat are 46% more likely to suffer account takeover fraud than others (Javelin and LifeLock, 2016).

Where businesses are concerned, the threat to corporate information is at a level that has never been seen before. According to the National Crime Agency, the threat is of such magnitude, complexity and fluidity that neither businesses nor law enforcement will be able to meet the challenges being presented alone. Cybercrime activity is also becoming more aggressive and technically proficient (NCA, 2016). Attacks on company defences from the outside are often seen as the greatest hazard but studies have shown that they can be much more vulnerable to strikes from the inside. Attacks from the inside often cause the most damage, as an insider threat survey carried out by the SANS Institute (2015) found. The survey goes on to say that information security professionals rate insider threats as one of their top concerns - of a sample group of 772 taking part in the survey, 34% admitted to having been a victim of a successful insider breach that is estimated to have cost their organisation more than $1 million - yet they tend not to do much about it. The misuse of credentials has been identified as a major factor in these cases. Verizon's current Data Breach Investigations Report (2016) states that 63% of breaches involving privileged access involved weak or stolen passwords and asserts that this is why the rapid growth of phishing and other credential-stealing tactics are growing so quickly. The misuse of insider credentials is also difficult to spot, the report adds, so much so that 70% are not noticed for months.

For companies to carry out their day-to-day transactions smoothly, they must put a lot of trust in their staff. Yet, because of the position they occupy, the staff have legitimate access to the very data a business needs to protect. This makes it easy for them to steal information which has value in the market place (Cole, 2015; Lim et al., 2010; Wells, 2004). Data leakage is also prevalent and a model for preventing this happening via email has been devised by Stamati-Koromina et al. (2012). As well as having direct access to data systems, staff has many cheap and simple ways of transporting information out of the office environment. They often carry a number of devices which supply high capacity storage. These include mobile phones, tablets and USB memory sticks. The data security problems caused by the spread of Bring-Your-Own-Device (BYOD) workplace culture are well documented along with the associated potential for the careless or unwitting loss of information (Garrity and Weir, 2010). In fact, staff negligence rather than malicious intent is the main cause of insider incidents, a study by the Ponemon Institute and Dtex Systems (2016) has indicated and the cost, per incident, of containing a negligent data breach is currently around $207,000. The cost of an incident caused by credential theft is more than twice that amount. Despite this, many enterprises do not see insider threat as a security priority until an incident occurs. Sometimes these incidents trigger major security changes but often the problem is allowed to fade away. To paraphrase

the writers, the reason is that: '…insider threat is item 5 on every CISO's top five priorities for the year and the budget line is drawn after item 3'.

Approaches to Digital Forensic Readiness (DFR)

DFR as A Process

A prime aim of DFR is to preserve and collect digital evidence so that it can inform an investigation into a data breach (Rowlingson, 2004; Sommer, 2009). Best-practice methods for the processes involved have been laid out in numerous guides, the majority produced by law enforcement and government agencies. In the UK, the Association of Chief Police Officers (ACPO) has published a well-known set of guidelines that are primarily aimed at serving officers but are also taken to apply to investigators and practitioners of digital forensics in the private sector. The ACPO guidelines, originally approved in 1999, were updated and republished in 2012 (ACPO, 2012). In common with other published guides in this subject area, for example, First Responder reference guides published by the U.S. Department of Justice (2008) and the U.S. Secret Service (2009), the ACPO guidelines advise on how digital equipment should be handled in order to best preserve evidence. The accent is on not losing or inadvertently spoiling digital evidence during the seizure of equipment, in particular, at the scene of a crime. The majority of the guides written for law enforcement agencies do not cover the subsequent analysis of data although the latest (2012) version of the ACPO guide does contain a brief section on analysis, giving views on who should carry out such analysis and the need for analysis to be properly targeted towards gathering evidence relevant to the case in hand.

The four aims of the digital forensic process, as identified from these guides and in order of importance are to:

1. Identify the evidence
2. Preserve the evidence
3. Recover the evidence
4. Present the evidence

A visual encapsulation of this process is given in Figure 1, below.

Figure 1. *The Digital Forensic Process, A Model*

From a law enforcement perspective, presenting the evidence will usually mean in support of pressing criminal charges and taking a case to court. Corporates may also wish to enter into court proceedings following a data breach, for example where industrial espionage or intellectual property theft is discovered, and the guidelines set out by law enforcement have been extensively adopted and modified for business purposes. Vom Solms et al. (2006) have identified the four key activities of the digital forensic process as:

1. Securing the evidence without contaminating it.
2. Acquiring the evidence without altering or damaging the original.
3. Authenticating that the recovered evidence is the same as the original seized data.
4. Analysing the data without modifying it.

Hoolachan and Glisson (2010) have also focused on how digital evidence should be handled within organisations as part of DFR. A document that goes into further depth is the Directors' and Corporate Advisors' Guide to Digital Investigation and Evidence (Sommer, 2009). The guide details the legal issues involved in the analysis of computer systems, media and mobile phones as well as their collection and preservation. Advice is also given on a 'Corporate plan of action' for digital incidents, although the guide does not go into data analysis procedure.

Incident Response, Technical and Human Elements

The technical nature of locating and gathering potential digital evidence has led to businesses setting up specialist information security teams with appropriate skill sets. The SANS Institute (2001) has recommended that corporates should establish a Computer Emergency Response Team (CERT) to work within the company's incident response procedures. Members of the team should include upper management, the information security team, the IT department, the physical security team, lawyers and the human resources and public relations departments. The National Institute of Standards and Technology (NIST, 2004) has also recommended that organisations in critical infrastructure technologies should establish CERTs as well as a defined set of policies and procedures. Nevertheless, corporate cybercrime mitigation and cyber-risk management remains: '…hampered by many businesses continuing to see the threat as a purely technical issue - rather than as a challenge for the board, the entire organisation and for business strategy.' (NCA, 2016).

The movement towards company-wide involvement in digital security and incident response has gained traction as businesses have become more aware of the threat from cybercrime, particularly the information security problems caused by insiders. Kraemer et al. (2009) found that technical problems and coding errors were only one source of computer system weakness; human and organizational factors could introduce vulnerabilities, too. More recently, researchers have

directly studied the moral behaviour of employees (Da Veiga and Eloff, 2010; Alfawaz et al., 2010) and how this can be influenced by corporate culture. Van Niekerk and Von Solms (2010) have stated that it is essential for organisations to establish a culture of information security and clear information morals because by establishing those standards, the human factors that generate risk to information security are minimised and managed. Gebrasilase and Lessa (2011) have also emphasised the effect that corporate culture has on the information morals of employees, adding that an information security culture is made up of a set of information security characteristics that are valued by an entire organisation.

Alumubark et al. (2015), found that security incidents can be attributed to: '…unaddressed information security vulnerabilities and the disharmony between organisational objectives and social values.' The research team found that the most influential factors in this miss-match were sectarian behaviour and what they termed the 'belonging scale', inferring that employees need to feel part of an organisation if its rules are to matter to them.

The need to persuade employees to make a personal investment in the security of the businesses that they work for has been noted by Collie (2010) who advised that giving staff a role in the security process is a key motivator. A model for small to medium enterprise (SMEs) was also introduced by Collie, the core aspects being the education, consultation and participation of staff, supported by awareness training that is accessible, relevant and up to date. It is crucial that management is committed and fully invested in the process, as Greene D'Arcy (2010) have shown. The Tuck School (2016) has also strongly supported this view. An executive workshop held by the Glassmeyer/McNamee Center for Digital Strategies affirmed: 'To really create a security culture.. Awareness and buy-in have to permeate through all the levels of the organisation.'

The Importance of Planning

While most businesses now recognise that cybersecurity is important, many may not completely understand how their organisation is at risk and what action to take. This is particularly true of small firms. In the UK, for example, only 51% have attempted to identify cybersecurity risks via health checks, risk assessments or audits (Klahr et al., 2016). While many authorities have stressed the importance of having sound incident handling plans, guidelines and procedures in place before an incident occurs, a large number of organisations remain ill-prepared for incident handling and even tend to ignore it, choosing instead to focus on maintaining production (Tan et al., 2003). While there are internal economic reasons for this, as Verizon (2016) has pointed out, firms also have a tendency to be reactive rather than pro-active. Since the majority of businesses now rely on information technology to trade and communicate, data security should be a driving force, not an afterthought. In brief, as Rowlingson (2003) remarked: 'If you wait until you know you have a problem, it's probably too late.'

Modelling Forensic Readiness

A literature review has found that forensic readiness is a broad subject and a number of elements are embodied within the concept. A number of different approaches to forensic readiness have also been identified with inputs from a variety of disciplines. Drawing the threads together presents difficulties not least, this paper suggests, because the terms 'forensic readiness' and 'incident response' are often used interchangeably. In fact, incident response is one component of forensic readiness. Barske et al. (2010) have proposed that it is possible to group the essential elements of digital forensic readiness into thematic categories, summarised as:

A. Strategy
B. Policy & Procedures
C. Compliance & Monitoring
D. Technology
E. Digital Forensic Response

The researchers' accompanying model depicts these elements as separate from each other but contributing to the DFR process. This paper seeks to move the idea forward by showing how key components of DFR fit together. Further, it seeks to show how a whole organisation can be involved in planning and strategy, each department following the same reporting construct and facilitating the free flow of information.

The HAUS Forensic Readiness Strategy Model

This section introduces a model for forensic readiness which has been derived from assimilating and analysing relevant research literature across the core disciplines. The model is an: Homogeneous, Answerable and Unified Strategy (HAUS). The process is driven by management, which needs to have continuous involvement. However, the process is enacted and delivered by staff i.e. all staff, not just technical staff or staff from selected departments. All staff can have roles because technical skills are not needed for a significant proportion of the work involved. Education and awareness is, however, vital.

The HAUS model depends on the following planning construct.

Staff Involvement - A Model for Inclusive Planning

In the same way as an organisation's employees need to know, in advance, what to do in the event of a fire, in the event of a digital incident they need to know what to do, how to do it and who's responsible for what.

They also need to know, at least at a basic level: what needs protecting; where it is; how crucial data might escape and how equipment e.g. workstations, laptops can be secured.

To this end, non-technical staff can be invited to participate in and contribute to the four stages of a proactive, cyclical process which is Aware, Alert and Always-on (AAA). The AAA cycle (Figure 2) involves:

a) Thinking - what needs protecting
b) Planning - how to spot a problem, contain it if possible and who needs to know
c) Gathering - information
d) Reviewing - information

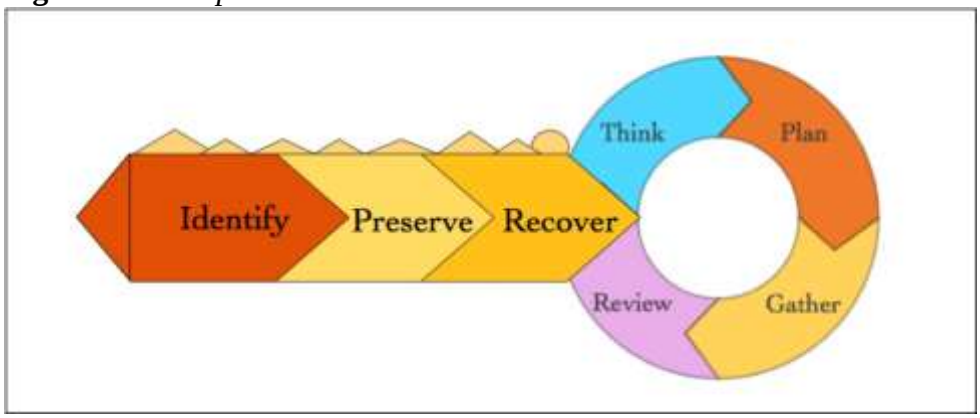
Appropriately trained technical staff or outside professional help will be needed to gather and review potential digital evidence.

Figure 2. *Conceptual Model - AAA Cycle*

The AAA cycle links into the Digital Forensic process model (Figure 1) by aiding the identification, preservation and recovery of potential evidence.

The following model conceptualises the connection. To make it easily memorable, it is rendered as a key - the Data Lockdown Operation Key (DLOK) (Figure 3).

Figure 3. *Conceptual Model – DLOK*



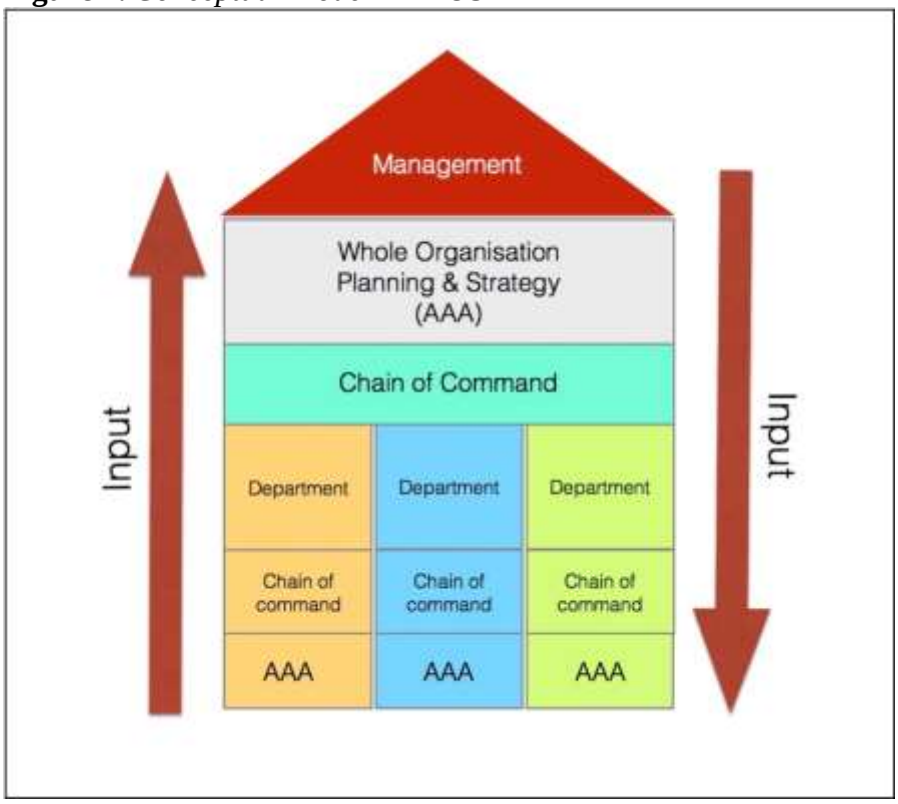
Overall Strategy Model

The HAUS model (Figure 4) can be adapted and utilised by both small and large enterprise. A key feature of the model is that each department of an organisation needs to have its own AAA cycle in place and in process. Information derived from the cycle is passed to the people who need to know and can take action. For this reason, a chain of command needs to be established in each department so that staff knows who to report to. Information and input from all departments should be pooled and proposed actions discussed by representatives who form the next link in the chain of command. Input should flow both ways, from staff to management and from management to staff.

The first steps towards implementing HAUS are for an organisation to identify:

a) Which departments should be involved
b) First responders within each department
c) A clear Chain of Command

Figure 4. *Conceptual Model – HAUS*



Research Value Proposition

As has been discussed, cybercrime is a global problem which increases year on year, at vast cost to nations, organisations and individuals. While organisations

still tended to meet the cybersecurity challenge by concentrating attention on defending their communications boundaries, it is now recognised that one of the biggest threats to corporate data comes from within - from staff. Although companies are aware of this threat, they do little to address it. Drawing on studies into human behaviour and the moral response to organisations, authorities have concluded that if data theft and data leakage are to be prevented, there is a need to build an internal information security culture which is based on shared values. However, previous research has shown that there is a lack of information on how ISC can be embedded into corporate culture. Furthermore, a compressive literature review has not uncovered any model that attempts to do so. This research advances the proposition that all staff can be and should be invited to engage in the processes that guard and maintain data security. It is postulated that this not only aids and enhances an organisation's forensic readiness, it has the potential to help it build a security culture. Planning and strategy are integral to forensic readiness. This paper puts forward models for both, representing a consolidation of knowledge gathered from a number of disciplines that have contributed to the research debate.

The proposed conceptual model AAA provides a proactive and continuous planning method which feeds information into the HAUS forensic readiness strategic model. The AAA process connects with and supplements the Digital Forensic process model by aiding the identification, preservation and recovery of potential evidence. Applied across each department the two processes, conceptualised as the unified model DLOCK, help form the backbone of an organisation's data lock-down operation.

The HAUS model is a collaborative strategic approach which aims to help organisations to consolidate DFR activities and build their capacity to detect, prevent and manage incidents. Allowing all staff to be involved in and contribute to the process allows them to be part of the joint effort, encouraging the sense of community and thus a strong security culture. Since existing staff carry out the majority of the procedures, the model should be economic to implement and run, the financial benefits of enhanced data security and consequent reduction in business losses far outweighing the cost of time expended on DFR projects. This outcome can be anticipated since behaviour analytics and threat intelligence solutions already being deployed have been shown to deliver the highest incremental cost saving to industry (Ponemon and Dtex, 2016).

Conclusions

Interconnectivity between people, machines and cyberspace is growing at an unprecedented pace, exposing individuals to exploitation during their working lives and their personal lives. Although cybercrime attacks from external agents pose a significant threat to organisations and businesses worldwide, research has shown that data compromise, theft and leakage largely happens from the inside due to the inadvertent or deliberate actions of staff. Although organisations need to protect their communication boundaries, equal attention needs to be paid to

the role that insiders play if cybersecurity is to be improved and maintained. The human factor has been widely acknowledged as a problem when it comes to implementing information security practices. Staff are often careless, they ignore or by-pass security measures and fail to comply with company security policies. As a result, organisations are vulnerable to data security breaches. Corporate culture and budget considerations also tend to lead to a reactive rather than proactive response. In practice, surveys have found, forensic readiness is often talked about by businesses but they fail to develop the capability.

Annual statistics on the causes of cybercrime have consistently shown that staff plays a vital role because they represent a weak point in corporate defences. Researchers have studied the phenomenon and found that employees often have no vested interest in maintaining the data security of the companies they work for. A core reason is that organisations fail to develop a shared system of values, beliefs and behaviours amongst staff. The remedy, it is now theorised, is for businesses to build a strong information security culture but, as yet, no clear way of embedding such a culture into organisations has emerged.

A review of literature across a range of disciplines which have contributed to research into forensic readiness has found that it is a broad subject and a number of elements are embodied within the concept. This complexity means that the notion is difficult to grasp. Forensic readiness is also not well understood since the term is often used interchangeably with the term 'information security'. This paper has drawn the threads of discussion together to show that although information security is the central aim of forensic readiness, it is not the same thing. Further, it has shown that while preserving and collecting digital evidence is imperative to the process, it is nevertheless only one activity within it. Forensic readiness is about being prepared for data security incidents. It is essential firstly because, in the information age, it is impossible to avoid them and secondly, as one authority has remarked: 'If you wait until you know you have a problem, it's probably too late.'

This research has aimed to advance the idea that all staff can and should be engaged in the processes that support and sustain data security. It is argued that this will not only aid and enhance an organisation's forensic readiness but also help it to build a security culture. Since planning and strategy are foundational components of forensic readiness, this paper has put forward conceptual models for both. These have been extrapolated from knowledge collated from numerous academic sources. A proactive and continuous planning and reporting method (AAA) which integrates with the digital forensic process has been proposed. This supplies inputs into an overall strategic model (HAUS). The HAUS concept represents a structured, inclusive approach to forensic readiness which can be scaled and customised according to an organisation's needs. It is suggested that the model should be economic to set up and run since the majority of DFR activities can be carried out by existing staff. The cost in terms of time expended on these should be more than matched by a reduction in losses due to data security breaches.

Further research opportunities lie in conducting surveys in different sized organisations in order to assess how the HAUS model and the AAA model that

is integral to it could be applied and in order to gauge corporate reaction to the concepts. The surveys should be designed to gather responses from management and staff at all levels with feedback being used to improve and refine the model. Opportunities to test customised versions of the model, initially on a small scale, could then be sought.

Acknowledgments

The author thanks Dr. Paul Hunton of Hunton Woods Ltd., and Peter Wood, CEO of First Base Technologies Ltd., for providing useful discussion and insights during the writing of this paper.

References

Alfawaz, S., Nelson, K. and Mohannak, K. 2010. Information security culture: a behavior compliance conceptual framework. In *Proceedings of the Eighth Australasian Conference on Information Security*, .Volume 105 (pp. 47-55).

Alumubark, A., Hatanaka, N, Uchida, O., Ikeda, Y. 2015. Enlighten Information Morals through Corporate Culture. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015).*

Association of Chief Police Officers (ACPO) 2012. ACPO Good Practice Guide for Digital Evidence. 2012. DOI= http://bit.ly/2Fh2LqD.

Barske, D., Stander, A., Jordaan, J., 2010. A Digital Forensic Readiness Framework for South African SME's, Information Security for South Africa (ISSA), 2010, IEEE. DOI= http://ieeexplore.ieee.org/document/5588281/.

Bunker, G, and Kosciuk, S. 2017. Cybersecurity Predictions for 2017. DOI=http://clear swift-security.co.uk/blog/

Cardiff University, 2015. The Implications of Economic Cybercrime for Policing, City of London Corporation. DOI= http://bit.ly/2CV4kfq.

Cifas, 'Criminals Target UK Youth As Identity Fraud Rises' (2016). DOI= http://bit.ly/ 29gt4wt. [Accessed: April 26, 2017].

Cole, E., Insider Threats and the Need for Fast and Directed Response (2015) SANS Institute. DOI= http://bit.ly/2CY8UKQ.

Collie, J. 2010. The Enemy Within. Intrusion Prevention from the Inside, Out. BrightTalk. DOI= https://www.brighttalk.com/webcast/288/21735.

Collie, J. 2011. 'Forensic Readiness - Strategy and Methodology'. Course materials (Unpublished).

Da Veiga, A. and Eloff, J. H. 2010. A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.

Garcia J. 2005. Proactive & Reactive Forensics. DOI= http://bit.ly/2maF36H.

Garrity S, Weir G. 2010. Balancing the threat of personal technology in the workplace. International Journal of Electronic Security and Digital Forensics 2010; 3(1): 73-81.

Gebrasilase, T., and Lessa, L. F. 2011. Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. The African Journal of Information Systems, 3(3), 1.

Get Safe Online and National Fraud Intelligence Bureau (2016). Fraud & cybercrime cost UK nearly £11bn in past year. DOI= https://www.getsafeonline.org/news/fraud-

cybercrime-cost-uk-nearly-11bn-in-past-year/.

Greene, G. and D'Arcy, J. 2010. Assessing the Impact of Security Culture and the Employee-Organization Relationship in IS Security Compliance. In *Proceedings of the 5th Annual Symposium on Information Assurance*, 2010. pp. 42-49.

Hoolachan, S. and Glisson, W. 2010. Organizational Handling of Digital Evidence. In *Association of Digital Forensics Security and Law Conference on Digital Forensics, Security and Law 2010*. St. Paul, Minnesota, May 19-21.

Jaatun, M., Albrechtsen, E., Line, M., Tondel, I. and Longva, O. 2009. A framework for incident response management in the petroleum industry. International Journal of Critical Infrastructure Protection 2 (2009) 26-37.

Javelin and LifeLock 2016. ID Fraud Hits Record High. DOI= http://bit.ly/2knzvaE.

Klahr, R., Button, M., Amili, S., Shah, J. and Wang, V. 2016. Cyber Security Breaches Survey 2016. UK Government, Ipsos MORI and University of Portsmouth. DOI= http://bit.ly/1T4MveX.

Kraemer, S., Carayon, P., and Clem, J. 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities, Computers & Security, 28, 509-520.

Lim, J. S., Ahmad, A., Chang, S. and Maynard, S. 2010. Embedding information security culture emerging concerns and challenges. In *Proceedings of Pacific Asia Conference on Information Security* (PACIS 2010) Paper 43.

McAfee. 2014. Net Losses: Estimating the Global Cost of Cybercrime. DOI= http://bit.ly/2qKroc2.

National Crime Agency. 2016. NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016. DOI= http://bit.ly/29wgHzO.

NHS Information Risk Management (2009), Digital Information Policy, NHS Connecting for Health. DOI= http://bit.ly/2CIR76e.

Ponemon Institute and Dtex Systems. 2016. The Hidden Cost of Insider Threat. DOI= https://dtexsystems.com/cost-of-insider-threat/.

Pooe, A and Labuschagne, L. 2012. A conceptual model for digital forensic readiness. 978-1-4673-2159-4/12/$31.00 ©2012 IEEE.

Rowlingson R. 2003. Forensic Readiness – Enabling a Corporate Approach to Digital Evidence v. 1.2. QinetiQ.

Rowlingson R. 2004. A Ten Step Process for Forensic Readiness, International Journal of Digital Evidence, Vol. 2, Issue, 3. DOI= http://bit.ly/2AI1g14.

SANS Institute. 2001. Computer Incident Response Team. DOI= http://bit.ly/2maig YA.

Schlienger, T. and Teufel, S. 2003. *Information Security Culture - from Analysis to Change*. South African Computer Journal, Volume 2003, Issue 31, Dec 2003, p 46-52.

Sommer, P. 2009. *Directors' and corporate advisors' guide to digital investigations and evidence.* DOI= http://bit.ly/2Fhjp9x.

Stamati-Koromina, V., Ilioudis, C., Overill, R., Georgiadis, C., Stamatis, D. 2012. Insider Threats in Corporate Environments: A case study for Data Leakage Prevention. Proceedings of the Fifth Balkan Conference in Informatics, P. 271-274. DOI= http://bit.ly/2CXaETA.

Tan, J. 2001. Forensic Readiness. http://bit.ly/2D9rnAR.

Tan, T., Ruighaver, T. and Ahmad, A. 2003. Where the need for planning is often not recognised. In *Proceedings of the 1st Australian Computer, Network & Information Forensics Conference*, (Perth ,Western Australia. 25 November 2003).

Tuck School of Business at Dartmouth, Glassmeyer/McNamee Center for Digital Strategies. 2016. Embedding Information Security Risk Management into the Extended Enterprise. DOI= http://www.ists.dartmouth.edu/library/198.pdf.

U.S. Department of Homeland Security, United States Secret Service. 2009. Best Practices for Seizing Electronic Evidence v3. DOI= http://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf.

U.S. Department of Justice, USA. 2008. Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders. DOI= http://bit.ly/1nQP00T.

Van Niekerk, J. F. and Von Solms, R. 2010. Information security culture: A management perspective. Computers & Security, 29(4), 476-486.

Verizon. 2016. 2016 Data Breach Investigation Report. DOI= http://vz.to/1Svr72f.

Von Solms, B. 2000. Information Security -- the Third Wave? Computers & Security, 19(7), 615- 620.

Von Solms, S., Louwrens, C., Reekie, C., and Grobler, T., 2006. A Control Framework for Digital Forensics. In Advances in Digital Forensics II, IFIP Advances in Information and Communication, vol 222. Springer, Boston, MA. DOI=http://link.springer.com/chapter/10.1007/0-387-36891-4_27.

Wells, J. T. 2004. Corporate Fraud Handbook. Prevention and Detection. New Jersey USA: John Wiley & Sons.