Annual ADFSL Conference on Digital Forensics, Security and Law

2010
Proceedings

May 19th, 10:30 AM

Organizational Handling of Digital Evidence

Sheona A. Hoolachan
HATII, George Service House, 11 University Gardens, Glasgow, Scotland, UK, pse57812@gmail.com

William B. Glisson
George Service House, 11 University Gardens, Glasgow, Scotland, UK, b.glisson@hatii.arts.gla.ac.uk

Organizational Handling of Digital Evidence

Sheona Anne Hoolachan
HATII
George Service House
11 University Gardens
Glasgow, Scotland, UK
G12 8QH
pse57812@gmail.com

William Bradley Glisson
Room 402B HATII
George Service House
11 University Gardens
Glasgow, Scotland, UK
G12 8QH
B.Glisson@hatii.arts.gla.ac.uk

ABSTRACT

There are a number of factors that impact a digital forensics investigation. These factors include: the digital media in question, implemented processes and methodologies, the legal aspects, and the individuals involved in the investigation. This paper presents the initial idea that Digital Forensic Practice (DFP) recommendations can potentially improve how organizations handle digital evidence. The recommendations are derived from an in-depth survey conducted with practitioners in both commercial organizations and law enforcement along with supporting literature. The recommendations presented in this paper can be used to assess an organization's existing digital forensics practices and a guide to Digital Forensics Improvement Initiatives.

Keywords: first responder; forensic readiness; organizations; procedures; digital evidence; Digital Forensic Practice.

1. INTRODUCTION

The digital revolution has profoundly affected how both private and law enforcement organizations handle digital evidence. With the increase of globalization and the advancing nature of technology, criminals are targeting digital media as well as using them as a tool to conduct crimes [2]. Organizations underestimate how often they will be subject to one of these attacks and how often they will have to produce reliable evidence to present in court [14]. Therefore, it is becoming increasingly important to identify potential weaknesses and rectify them [14]. Hence, digital forensic practices and the handling of digital evidence is an issue which is pertinent to many organizations throughout the world. Within the course of a year, the average organization will encounter events such as unauthorized access to the computer system, computer based attacks (e.g. phishing or denial of service), or online defamation [5]. In a study conducted by the Home Office in 2004 [8], organizations identified 101 different types of criminal threats administered by 137 different technological methods. The participants in the Home Office research study included Information Technology Security, Law Enforcement, Academic and Governmental organizations with a range of experience over a variety of security oriented topics [8].

With the exponential growth in technological advances and their utilization for criminal end, one might expect these figures to be higher in 2009. The criminal threat categories delineated in the Home Office study demonstrates the array of knowledge necessary to investigate potential violations. An act

such as fraud would be considered an offence under the Fraud Act 2006 (England) and could, if successfully prosecuted, lead to 10 years imprisonment [4]. Should an offence like this occur during the course of business and the discoverer (herein after referred to as the 'first responder') is untrained in the handling of digital materials, vital evidence could be lost or compromised, and a prosecution may not be secured. Incidences of money laundering and child pornography can be the most problematic for the organizations, as untrained first responders can inadvertently taint the evidence. These two particular crimes are the only ones which organizations are obligated, in the United Kingdom (UK), to report to the police [2].

Ueli Maurer discusses, in relation to Digital Rights Management (DRM), the importance of technical, legal, social and business aspects when managing information and information technology systems [7]. Highlighting these four criteria is useful for the examination of digital evidence. During the aforementioned discovery scenario, the relationship between the technology and the first responder is inseparable and, therefore, interdependent. The problematic technological discovery and subsequent evidence recovery is solely reliant on the first responder's action and the complexity of the technological discovery will affect who has the skills to correctly handle the situation. Implementation of protocols must take into account the culture of the organization, policies and laws applicable to the type of information handled, as well as the size and nature of the organization.

This paper summarizes the results of an initial UK Organizational survey that examines how institutions handle digital evidence when it is discovered by untrained first responders. The results of the survey established the initial justification for Digital Forensic Practice (DFP) recommendations. These recommendations are based on the small sample of individuals interviewed for this research and cannot encompass every type of organisation. The purpose of this study is to initiate discussion surrounding issues that arise within organisations where there is currently no standardised set of protocols in place to protect the integrity of digital evidence.

2. EXISTING RELEVANT WORK

There are three major areas that should be addressed when considering the significance of digital evidence becoming tainted by an untrained first responder: legal aspects including admissibility; the forensic readiness of the organization; and the first responder themselves. This paper will not concentrate on the legal aspects as these are jurisdictional and will vary both nationally and internationally. The latter problems, however, will be briefly discussed in order to contextualise the research and its value.

2.1 Forensic Readiness

Forensic readiness is a concept outlined by Robert Rowlingson from QinetiQ Ltd, an internationally recognised defence technology and security consultancy [15]. From the perspective of law enforcement agencies the forensic process begins when the crime has been committed or it has been discovered and reported. The concept of forensic readiness, according to Rowlingson, is that an organization can pre-empt the occurrence of a crime by gathering evidence in advance and in doing this, organizations will benefit not only in instances where prosecution becomes an issue but also in limiting their own business risks [13]. Although this definition of the forensic readiness strategy acts as the primary thesis of Rowlingson's paper, he addresses other matters of benefit and contention. These are identified below and in Section 2.2.

One of the main strengths of the forensic readiness model is the recognition of the range of personnel within an organization who can become involved in a legal inquiry and this is something that will be critiqued in Section 2.1.3. Rowlingson identifies no less than eleven different departments and their associated personnel that must be considered in an investigation.

Although the variety of staff involved will vary depending upon the magnitude of the investigation, this observation identifies the crux of this paper's argument – there are a multitude of people who need to understand the correct protocol within a digital investigation.

2.2 First Responder: Policies

Forensic readiness may be implemented as an organization, but when evidence is discovered the strength or weakness of that evidence is reliant on the first responder and their actions [6]. The United States Department of Justice (USDoJ), in their first responder's guide, defines a first responder, in a digital evidence context, as:

- Anyone encountering a crime scene that might contain electronic evidence;
- Anyone processing a crime scene that involves electronic evidence;
- Anyone supervising someone who processes such a crime scene;
- Anyone managing an organization that processes such a crime scene [9].

This means that there is a desire to be forensically ready within the organization and in relation to evidence gathering, but also there is a need for forensic readiness amongst all members of staff.

Many organizations implement incident readiness through company policies. However, given the complexity of digital forensics, the expectation of staff members to understand both technical and legal principles is unreasonable based on other areas of expertise that the employee may possess. Reliance on policies is the downfall of Rowlingson's forensic readiness implementation as a high level of expectation of technical knowledge is forced upon the average user. Relying on this knowledge for the purposes of digital security, particularly in the context of evidence collection, is completely unacceptable. A notable example of unreasonable expectation within current digital security literature is David Harley's article focusing on the problem of phishing attacks. Harley makes a number of strong remarks regarding what comprises phishing, the pitfalls of the average user and methods by which phishing scams can be educated against and defeated. From the perspective of this paper, however, the major downfall of his proposed solutions comes from the relationship between technological indicators and the untrained end user, or first responder in the context of this research. He expects the average user to identify security cues such as accessing the HTML source code to verify the legitimacy of the senders email address; Domain Name Service (DNS) misdirection; and identification of deceptive embedded Universal Resource Locators (URL's) – activities many users would be unable to undertake regardless of their desire to act more securely [3]. Harley's paper, by no means, disregards less-technically capable individuals, as he proposes quizzes to simplify the issues. His paper does, however, act as a useful baseline by which "simple" technological cues can be measured and, when contextualised to an untrained first responder, it becomes apparent why this dichotomy can become problematic for the field of digital forensics.

Regardless of the technical knowledge requirements outlined, policies are problematic at a very basic level. The complexity of jargon and the expectation to read and understand complicated ideas, concepts and rules leads to the insecure behavior demonstrated when policies are presented to many employees – they sign the documents without reading them [16]. Julie Nosworthy identifies some of the key downfalls of a policy culture including the tension between technological solutions and the human factor [10]. She identifies the failings previously indicated with regards to a lack of understanding of external departmental issues, specifically in relation to Human Resources (HR) and Information Security (IS) [10].

2.3 First Responders: Automated Tools

In order to fully explore the various tools currently utilised within the realm of first response, it is important to address automated solutions as well as more human-driven techniques previously discussed, such as policies. These will not play a particular role within the Digital Forensic Practices recommended in Section 4.0, but are beneficial for background understanding of the problems and solutions. FRED is a tool used by the American Air Force Office of Special Investigations and its objective is to handle digital evidence without the intervention of any users [6]. The goal of the actual

FRED tool is to determine whether or not an intrusion had occurred by means of analysis of network connections, active processes, dynamic link libraries (DLL) and open ports with MD5 hash values recorded for critical files on the system [6]. Furthermore, the entire tool fits onto a CDROM and the disk would play host to a batch file created by the tool to create an audit trail [6].

Ideally, an automated tool would remove responsibility from the first responder and allow unified evidence collection regardless of their specific knowledge. It could be argued that on these grounds the aforementioned criticism of policies and their unreasonable expectations placed upon the user are circumvented. However, an automated tool does not remove the human factors from the acquisition process and therefore there is still scope for data to become compromised. An individual will be required to insert the disk and execute the tool. How can it be determined what they did to the computer before the auditing tool began its work? Depending on the size of the system the tool may take some time to complete its functions. What happens if the first responder leaves the room while the tools is executing? There is scope for a suspect or bystander to compromise the tool while it is in operation and issues surrounding the field of live forensics which are outwith the scope of this paper. Some of these issues are addressed in the conclusion on Kornblum's article where it is indicated that:

> "There have been some procedural questions regarding when FRED should be run and by whom, but these are issues of policy, not technology" [6].

This harks back to Nosworthy's analysis of the problematic areas of policy making where a 'them and us' culture exists [10]. The technological implementations in this scenario cannot exist without the human factor and it is, therefore, unacceptable to blame any shortcomings on the individuals who are required to make the whole system operate correctly.

3. SURVEY COMPILATION

The study attempts to investigate whether or not the individuals in charge of implementing policies and dealing with the implications of digital evidence handling have a sufficient understanding of the issues and the practices within the field. The following sub-sections present the experimental approach and demographic information.

3.1 Methodology

The style for this case study was a combination of both structured and semi-structured interviews. Structured interviews have a specific set of questions which are presented to each interviewee and, upon answering the questions, the interviewer moves to the next question or set of questions. Semi-structured interviews begin with a broad set of themes to be discussed and the responses from the interviewee will lead the direction of the interview and generate new lines of questioning [12]. The case study questions were pre-defined and were split into two main thematic groups: policies and general issues, together with technical issues for the organizational questions; organizational evidence and technical issues for the law enforcement questions. The same sets of questions were asked of each individual interviewee. Where their responses afforded the opportunity, further questioning along these lines was followed to gain as much information as possible.

The organizational survey questions were initially validated by an individual who not only possesses corporate environment work experience but has also undertaken research projects at the University level. An ex-senior police officer was approached to validate the law enforcement questions in a similar manner. Both of these validations led to minor adjustments being made to the questions to clarify semantic ambiguities. For example, prior to the validation process, one question read: "How is this communicated to all staff?" This was changed to "How is this communicated to all staff within the organization?" in an attempt to mitigate ambiguity for the interviewee.

Prior to distributing the questions and in addition to the initial validation procedure, individuals who were not due to participate, but yet had relevant background knowledge, were asked to validate the questions to ensure they were easily understood by the target audience. This was done at the

recruitment stage for the organization questions. After ascertaining that an individual was not appropriate for the research project due to their lack of daily contact with the subject matter, they were asked to explain their understanding of each question to ensure that their understanding matched the interview intention.

3.1.1 Interview Demographics

A total of ten interviewees were recruited based initially on two broad areas concerned with digital evidence, i.e., organizations and law enforcement. Within these categories a balance was sought between public/government organizations, corporate organizations and educational institutions. A balance was also sought between the organizational sides and the police, lawyer and 'other' (such as private investigator) for the law enforcement side. Table 1 provides a detailed insight into the survey participant's organizations, years of experience and job title.

TABLE 1

Interviewee Key	Type of Organization	Years Experience.	Occupation
A1	Academic	Undisclosed	Information Security Coordinator
HB1	Health Board	24	Head of Information Governance
HB2	Health Board	11	Information Governance Technical Advisor
F1	Financial	5	Security and Technical Consultant
F2	Financial	8	Internal Audit Manager
F3	Financial	18	Divisional Records Officer
F4	Financial	4	Information Security Manager
CS1	Civil Servant	10	Procurator Fiscal
DE1	Digital Examiner	4	Digital Analyst for a Private Company

The intention behind seeking the balance among the various categories was to gain an objective understanding of issues addressed by organizations and those which are distinctive to law enforcement agencies in order to identify areas of correlation and anomalies. Due to the separation between organizations and law enforcement interviewees, two different sets of interview questions were posed to participants depending on their respective associations. The individual questions are available upon request.

3.2 Results

The survey findings identified the following four areas as areas that need to be discussed:

- Problems identified by the organizations surrounding digital security
- Current first responder practices
- Issues surrounding communication and training
- Variables identified by the organizations that act as unique difficulties or points of note.

3.2.1 Problems identified by the organizations surrounding digital security

When interviewees were asked to identify the type of attacks, crimes or general issues which are problematic within their organization, the following were acknowledged:

- Theft of physical objects including hardware
- Loss or the need for encryption of USB keys
- Implementing security measures that only addressed external attacks rather than

considering the internal threats

- First response errors
- Warning colleagues of digital device seizure or search
- Unauthorized access to data
- Emails including spam and viruses
- Phishing attacks on customers and staff
- Making copies of child pornography for the purpose of examinations
- Malicious malware
- Personal use of the organization's system (e.g. via photographs and music)
- Identity theft
- Human error
- Password complacency.

Although there were overlaps in the problems identified by the interviewees, this list demonstrates that, within a relatively small interviewee group, a vast range of different problems encountered has been identified. This supports the aforementioned critique of automated first response tools - how can an automated tool be expected to handle such a range of subjective issues and cope with human error? Some of these problems can be automatically handled, such as malicious malware or email problems, but many of the issues facing digital security exist in a non-digital medium. For example, HB2 identified unauthorized access of digital patient records to be a problem within their health board. He commented that people access data that they are not supposed to access because "people are nosey". Although access control software could help prevent this problem, determining what is an act of curiosity and what is a genuine access of confidential records is a subjective issue which cannot be determined by automation. HB1 reinforced this point, saying that:

> "You can put as many procedures and policies in place and you can put as many technical measures in place but there is this big grey area in the middle with people in it and they'll always let you down."

In terms of policies, interviewees often agreed with the critique outlined in Section 2.2 First Responder: Policies regarding the unreasonable expectation of individuals to understand technical problems. It was, however, noted by F3 and F1 that often leaving the level of education at a basic awareness level is safer for the company's interest. F3 commented that:

> "Personally, I feel that staff don't need to know the details of digital security, they need to know it at a high level and the importance of it but we would tend to leave that to subject matter experts who are dealing with it on a daily basis…There is a risk that if too many people know too much detail there is potential for something to happen."

F1 concurred saying "the less they know the better for us". There is a conflict existing here because much of the literature suggests that the only way for individuals to take digital security seriously is to fully understand why they are taking certain actions rather than a different set of actions [10]. F1 and F3 acknowledge that it is often safer to restrict the amount of knowledge staff have regarding digital security, but there is a limit to the amount of information that can be discretionary and a point in which it will restrict the awareness of issues.

This is a notable conflict of interests between those implementing the security and the end-users and

there were other such incompatibilities identified through the interviews which will be discussed in Section 3.2.3 Issues surrounding communication and training.

3.2.2 Current first responder practices

One of the most conspicuous blanket practices amongst all of the organizations was how to deal with a first responder discovery of evidence on the organization's system. Every individual in the organization category of interviewees details a policy involving a phone call to another department should an end-user discover something that could potentially be used as evidence. The interesting aspect arises from the fact that each organization suggested contacting a different person. Even individuals within the same organization, in different roles, identified different departments that should be contacted. These included:

- Local I.T. support
- Legal
- Help-lines
- Financial Crime
- Line Manager.

F3 and F2 are employed by the same financial institution within different areas of the team. F3 identified the legal department as the point of contact whereas F2 suggested the financial crime department. This anomaly could have arisen through their differing roles and within their specific role or the type of information they frequently handle, then these departments may be the most suitable. The most striking aspect about the response to this question, across the board, is that there is no definitive standard regarding what end-users should do upon discovery of potential evidence. However, all the organizations provided their staff access to policies regarding general digital security via their intranet or equivalent. The potential problem with this system is addressed in Section 4.1 Do not use the intranet for policies regarding the handling of digital evidence.

The impact of not using the intranet for policy dissemination, from the law enforcement perspective, varied between DE1 and CS1. DE1 identified instances where he had been called to an organization and upon arrival the requesting member of staff was still on the computer and eager to show him information they had found. He explained to the individual that:

> "her activity on the computer was going to result inevitably in the loss of recoverable information that could have been useful…from there onwards you're not looking at the computer that the suspect used…all I was looking at was how her boss was using the computer"

He did, however, explain that this was a small company and perhaps this could account for the method in which it was reported and handled. CS1 explained that the difference in resources and capabilities between large and small organizations often results in different methods of handling and reporting. This, and similar incidents are often reported to a private investigator, perhaps not exclusively but in part, because of the size of the company as smaller organizations are more likely to circumvent any of their own departments and hand the information directly to the police or investigators. Larger companies, CS1 continues, would just sack the individual to avoid reputational damage. On the whole, however, CS1 did not feel the reliability of the evidence would be problematic for admissibility because if the first responder did alter any information forensic analysis would be able to identify and account for any of these changes.

3.2.3 Issues surrounding communication and training

Training was widely identified as a problem area within this study. Two of the most candid interviewees were F4 and HB1 and their perspectives on the subject of training were very interesting.

F4 identified many weaknesses in the field of digital security within his organization and, as he is relatively new to the organization, he has been tasked with rectifying these issues. The difficulty, from his perspective, is that the organization has fallen far behind in its process of reviewing company policies and this is the first review conducted since the policies were written seven years ago; creating an immensely difficult task. The only communication, at present, of policies and digital security training is a Computer Based Training (CBT) scheme which forms part of employees' initial induction – there is no follow up training.

Furthermore, although policies and procedures can be accessed electronically after this initial induction, most of the staff, according to F4, do not know this capability exists and subsequently do not seek access to them. He explains that there are hard-copies of the policies distributed to each manager, but "I suspect most of them end up in a cupboard".

HB1 identified an ongoing battle with staff regarding information security training. She highlighted that although the organization as a whole has agreed to annual information governance training, individual staff have not taken this up and, as mentioned in 4.1, the staff must understand the issues in order to heighten their awareness. This breakdown in communication will be discussed further later in the paper. HB1 explained that their health board also has a CBT scheme in place for training which has become outdated to the point of redundancy. She explained that the boost in their training numbers can be credited to the Personal Development Programs (PDPs) in their health board whereby staff must meet certain personal targets for training amongst other aspects of their role in order to progress up their pay-band. This is the theory of behavioral economics where an individual's internal desire to achieve something is driven by monetary rewards [1]. Although this theory is criticized for driving individuals by non-altruistic goals, HB1 concedes that she is "quite happy to use this system if it means training improves".

Beyond the scope of training, another recurrent theme about communication was salesmanship. HB1, A1 and F4 all discussed the notion that, as a department, you have to sell your ideals to other departments in order for them to recognize your cause. HB1 and A1 both described instances where they would give lunchtime seminars or take part in other departmental meetings in order to highlight the importance of digital security. F4 discussed it in a much more business sense:

> "At the moment, I don't think we are selling the benefits well enough and, therefore, it gets ignored. But it's down to us to sell the benefits because we can't just expect to say 'you should do it. It's a good idea' and not say well hang on, this is what you're going to get for your money. Everything comes down to money and we have to justify our existence."

This pragmatic attitude was somewhat refreshing regarding the literature around this subject, such as the example of Harley's phishing article, outlined in section 2.2, which seemed to expect something from users simply because he tells them to expect something [3]. As identified, Harley's approach does not take into account different skill levels of users whereas F4 wants to make people understand why digital security is a pertinent issue rather than simply imposing his views upon them. It could be argued that although the literature is often too idealized in its suggestions of best practices, the implementation can sometimes be more pragmatic.

3.2.4 Variables identified by the organizations that act as unique difficulties or points of note

At the end of the formal interview questions, interviewees were asked to raise any issues that they felt were unique to their organization or that were prevalent in the current climate that had not yet been raised. Although the issues raised during this section were not directly related to first response discovery or the underlying training issues, very diverse problems were identified.

Because F3, F2 and F1 were all from financial institutions, their responses were similar acknowledging that problems are fairly uniform throughout the financial world. These included the lack of mandatory training and education as well as risk assessing the organization from a variety of levels and vantage points. Interestingly, F1 identified the organized crime aspect to be a large problem

facing all types of organizations.

HB1 and HB2 both identified patient care as the unique aspect of their health board over other types of organizations. HB1 highlighted that:

> "Everything we do will potentially affect the patients and if someone isn't doing what they're meant to electronically, they could kill somebody."

HB2 elaborated upon this point by highlighting the reputational aspect of their health board versus organizations. He indicates that one of the worst outcomes for a corporate organization is reputational damage, whereas within a health care situation there are lives at stake. Furthermore, their health board's reputation is arguably more valuable than an organization because for many people there is no alternative. He notes that if a company's reputation is damaged, the customers have the option of moving elsewhere. Other than private medical care, there is no alternative to their health board. HB1 concurs, explaining that within her specific health board "we have to be whiter than white".

F4 states that the problematic area for his particular organization is their relative infancy within the financial sector. He explains that the organization is only beginning to push branding of the company and his concerns lie in the raised profile of the company outweighing the security measures to prevent attacks:

> "If we raise our profile as a brand someone will start looking at us and saying well what's going on here and what can we get from these people?"

This was not raised specifically as an issue, but perhaps his concerns are more relevant given the current financial climate and the desperation of people to have enough money to survive. He goes on to say that it would have been nice if both brand profile and brand protection had developed in parallel rather than one being required to catch up.

A1's unique aspect of the academic organization stemmed from the diverse nature of the staff, students and their requirements. Web filtering, for example, is a limited security measure within the University as there is no way to predict what topical areas students and staff will be researching at any particular time. He comments on the financial ties relating to this situation. Often, research grants will be awarded only if the researcher can provide proof that the institution is equipped to allow the research to be conducted. This may involve reducing security measures for particular parts of the University or taking specific computers off the network. He also comments that mandating anything within the University, such as training and education is extremely difficult as academia takes priority over all else.

This lack of standardization and mandating is prevalent within the law enforcement side also, according to DE1. He comments that varied approaches to the handling of digital evidence by different police forces and organizations can make it difficult to work as an independent outsourcing company as different clientele will require information to be presented in a variety of formats. This is definitely a recurring theme within the field of digital security regardless of whether one is implementing it or handling the aftermath.

Although not a unique aspect of his position, CS1 explains that he has recently been told about a police force in Holland that is training all their Criminal Investigation Department (CID) police to handle digital evidence in a forensically sound manner. According to CS1, the problems surrounding digital devices has become so prevalent and widespread that they are ensuring that all their detectives have a basic understanding of how to handle the devices and will pass on particularly difficult cases to experts. He described it as 'triaging' the computers and this was also a phrase used by HB1 in a discussion of outsourcing versus handling information internally.

4. DIGITAL FORENSIC PRACTICE (DFP) RECOMMENDATIONS

An analysis of the results generated from the interview process, as well as studying current literature,

provided three recommendations that organizations should consider when dealing with digital evidence. Beyond these three recommendations there are too many variations within organizational structure and the unique problems faced by different types of organizations as demonstrated in section 3.2.4 for formal restrictions to be productive. These recommendations provide a solid basis for evidence to be handled at the discovery stage in order to assist the preservation of evidence integrity. The three recommendations are as follows:

1. Do not use the intranet for policies regarding the handling of digital evidence.
2. Have a centralized co-ordination point so staff members are clear on who should be contacted.
3. Use an external company to perform forensic analysis but have internal 'triaging' capabilities.

4.1 Do not use the intranet for policies regarding the handling of digital evidence

Many of the organizations used the intranet as a communication point for staff should they need to refer back to policies at a post-training stage, as mentioned in Section 3.2.2 Current first responder practices. Although this approach, for the most part, is a sensible measure to ensure the ability staff to be able to access policies at all times. For the purpose of handling digital evidence, it is unacceptable. After the point of evidence discovery, the staff member should be able to access the information required without asking anyone or touching the suspect computer. In terms of asking anyone, this is not recommended as it may not be clear who has perpetrated the crime and giving warning to individuals within the office may compromise the evidence. F3 highlighted an incident that had occurred involving a laptop whereby the individual owning the laptop had been warned ahead of time that it would be investigated. This allowed the individual to delete information from it and although this was subsequently recovered the potential for affecting the admissibility existed. Although interaction with other individuals could be counterproductive within an investigation, the primary concern would be those in the immediate vicinity of discovery and, therefore, providing staff with a centralized "help" facility would allow explanation of protocol, within minimised risk, to the digital evidence. This is discussed in Section 4.2. A hard copy of policies should also be accessible to all staff members as supplementary, supporting and verification materials, as initial training can be easily forgotten after the fact. These facilities should be available to every employee regardless of whether an incident is likely to occur within their job as anyone can be a first responder to an incident.

4.2 Have a centralized co-ordination point so staff members are clear on who should be contacted

Although this may incur cost to the company, Section 3.2.2 Current first responder practices demonstrated the range of responses by interviewees when asked who a first responder should contact in instances of evidence discovery. Having a centralized point acting as a call centre for coordination will assist in the implementation of the first recommendation.

All that would be required is a card or sticker attached to every terminal or laptop in the company and first responders would have access to the appropriate information rather than having to consult the intranet.

4.3 Use an external company to perform forensic analysis but have internal 'triaging' capabilities

F3 and HB1 noted that it is sensible to handle forensic analysis externally to avoid any potential corruption or to prevent people from not reporting issues to protect friends or colleagues. This is a very sensible idea but, in line with CS1's information about the Dutch police, internal 'triaging' capabilities are essential to an organization. Although those interviewees who noted outsourcing as a company policy said they used local companies to ensure they were on the scene quickly, there will still be a time lapse between discovery and the arrival of an outsourcing team. Having staff members on site who can secure and handle the device at this interim point would prove invaluable to an organization when issues of admissibility are raised. Larger organizations may have dedicated

departments that deal with digital investigations; however, a contingency of outsourcing would be beneficial should an incident arise where the investigative department itself requires examination. Arguably, this recommendation could be split into two issues. The first addresses the use of external forensic companies and the second has the responsibility of internal 'triaging'. However, given that there will be a natural time-lapse between discovery, reporting the incident and the external company arriving on the scene. Having the plan for handling the evidence between these time-lapses is fundamental in ensuring the continuity of evidence. Based on the outcome of this research, 'triaging' capabilities would be recommended for every organization. Although interviewees indicated that their external contractors would endeavor to be on-scene at the earlier point, there are limitations as to how quickly this would occur and the data has the potential to change within this time.

5. CONCLUSION

The continued integration of the digital data into business environments highlights the need for organizations and law enforcement to be able to handle digital evidence from a first responder perspective. A lack of digital forensics practices and procedures cultivates an environment that is conducive to compromising evidence in organizations. This research attempts to identify areas within organizations where the provisions for first responder evidence handling are not at an acceptable level to guarantee the admissibility of items of evidentiary value.

The conclusions derived from the survey resulted in the creation of DFP recommendations. The implementation of these recommendations should assist in the mitigation of inadmissible evidence. The DFP recommendations are as follows:

1. Do not use the intranet for policies regarding the handling of digital evidence.
2. Have a centralized co-ordination point so staff members are clear on who should be contacted.
3. Use (or plan for) external companies to perform forensic analysis but have internal 'triaging' capabilities.

Future research should investigate higher level staff members who are responsible for dictating the culture of the organization and setting the budgets which ultimately shape the implemented digital forensic strategies.

Furthermore, it would be interesting to broaden the research scope to include private companies. This is due to the limited financial scope of the current research which perhaps masks a fuller understanding of the bigger picture. It would also make a noteworthy addition to future research to consider businesses that are purely internet based to determine if they face the same problems. In addition, it would be beneficial to investigate companies that operate within a technological field rather than those simply using technology within the course of their business

Additional research would also benefit from an examination of the front-end or lower-level staff's perspective to verify whether the assessment made, by higher level interviewees, of their ability to cope with discovering evidence was accurate. The scope of the research could also be expanded to incorporate the business issues involved in implementing security matters such as cost risk analysis and management issues.

6. REFERENCES

1. Gonzalez JJ, Sawicka A. (2003) 'The role of learning and risk perception in compliance'. 21st International Conference of the System Dynamics Society. July 21st. New York, USA.

2. Haggerty J, Taylor M. (2006), "Managing corporate computer forensics," Computer Fraud & Security, Vol 6: 14-16.

3. Harley D, Lee A. (2007) 'Phish Phodder: is User Education Helping or Hindering?'. Virus Bulletin Conference Proceedings. Sept 19th-21st. Ottawa, Canada.

4. Home Office (2009), 'Fraud Law Reform | Home Office', http://www.homeoffice.gov.uk/documents/cons-fraud-law-reform/, Accessed Jun 4th 2009.

5. IAAC (2009), 'Directors and Corporate Advisors' Guide to Digital Investigations and Evidence', http://www.iaac.org.uk/Portals/0/DigitalInvestigationsGuide.pdf, Accessed Jan 15th 2009.

6. Kornblum J (2009), 'Preservation of Fragile Digital Evidence by First Responders', http://www.dfrws.org/2002/papers/Papers/Jesse_Kornblum.pdf, Accessed Jan 16th 2009.

7. Maurer U. (2004), "New approaches to digital evidence." IEEE. Vol 92(6): 933-947.

8. Morris S (2009), 'The future of netcrime now', http://www.crimereduction.homeoffice.gov.uk/internet01.htm, Accessed Jun 4th 2009.

9. NIJ Guide (2009), 'Electronic Crime Scene Investigation: A Guide for First Responders', http://www.ojp.usdoj.gov/nij/pubs-sum/219941.htm, Accessed May 25th 2009.

10. Nosworthy JD. (2000), "Implementing Information Security In The 21st Century—Do You Have the Balancing Factors?" Computers & security. Vol 19(4): 337-347.

11. Nuth MS. (2008) "Taking advantage of new technologies: For and against crime", Computer Law & Security Report, Vol 24(5):437-446.

12. Oates DBJ. (2005), Researching Information Systems and Computing, Sage Publications Ltd, London.

13. Rowlingson R, Ltd QQ. (2004), "A ten step process for forensic readiness", International Journal of Digital Evidence, Vol 2(3): 1-28.

14. Taylor M, Haggerty J, Gresty D. (2007) "The legal aspects of corporate computer forensic investigations", Computer Law & Security Report, Vol 23(6): 562-566.

15. Unknown (2009) 'QinetiQ - Inspired solutions for a changing world', http://www.qinetiq.co.uk/, Accessed Jun 20th 2009.

16. Wright D, Gutwirth S, Friedewald M, De Hert P, Langheinrich M, Moscibroda (2009) "A. Privacy, trust and policy-making: Challenges and responses", Computer Law & Security Report, Vol 25(1): 69-83.