

Running Head: INCREASING THE LIKELIHOOD

Increasing the Likelihood of Admissible Electronic Evidence:
Digital Log Handling Excellence and a Forensically Aware Corporate Culture

Lawrence M. Healy

Eastern Michigan University, College of Technology

COT 704, Final Paper

April 12, 2008

Abstract

Collecting and storing potential electronic evidence (commonly in the form of digital logs) that meets the requisite legal rigor, in a rapidly changing technological environment, is a persistent challenge in today's business environment. The corporate culture of most organizations lacks the background to fully comprehend the requisite evidentiary requirements of the legal system. Consequently, potential electronic evidence is inherently difficult to collect and store in an appropriate and admissible manner.

This discourse will present a summary of the primary evidentiary concerns for electronic evidence collected in digital logs for large private-sector corporations. To establish electronic evidence admissibility in legal proceedings, digital logs must be collected pursuant to the Federal Rules of Evidence (as applied to electronic evidence) and the Electronic Communications Privacy Act of 1986. An essential objective for this research paper will be to focus attention on the importance for private-sector awareness as to the value of a forensically ready organizational culture. Hopefully, this awareness will demonstrate how the appropriate collection and storage of its digital logs can influence legal proceedings pursuant to these two statutes.

Introduction

Approximately 85 percent of the 66 million dollars lost by corporations due to computer related crime in 2007 was categorized as computer related financial fraud or company insider abuse of computer networks (Richardson, 2007). A few central factors that inhibit the collection of admissible electronic evidence for financial and legal retribution in a large private-sector organization are (Rowlingson, 2004):

1. Corporate cultures lacking a foundational evidentiary understanding.
2. Employee privacy implications.
3. Corporate cost and productivity.
4. Digital log complexity and volume.

Pursuant to many legal proceedings involving corporate policy violations or network intrusions, digital logs are one of the primary sources of information available to a corporate investigator.

Digital logs are used to record and monitor daily system operations and user activity on a computer network. All digital logs are potential electronic (digital) evidence and must be handled in a legally consistent and appropriate manner. Digital evidence can be defined as: “any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi.” (Casey, 2004, p. 12).

There are many types of electronic evidence; this paper will focus on digital logs collected as potential electronic evidence in the private-sector corporate environment. This discussion will be limited to the legally appropriate requirements for the collection and use of digital logs as evidence pursuant to the Federal Rules of Evidence (FRE) (as applied to electronic evidence) and the Electronic Communications Privacy Act of 1986 (ECPA). There are many other evidentiary concerns that will not be specifically addressed in this paper. These include the

Daubert scientific evidence admissibility guidelines (Daubert v Merrell, 1993; Kenneally, 2001), and a multitude of other privacy laws (Burgunder, 2007). Private-sector corporations may face a myriad of scenarios that entail the appropriate and relevant necessity for digital logs as admissible electronic evidence. These situations may range from corporate espionage to malicious pranks (Stephenson, 2000). The relevant topics of consideration will be limited to: 1) digital evidence of malicious activity resulting from network intrusions and 2) the use of computer records for evidence in employee related case law such as employee termination litigation.

Digital logs as electronic evidence are to a digital forensic investigation what fingerprints are to a conventional crime scene or financial ledgers are to a financial audit (Kenneally, 2004). There are many types of digital logs and the volume of information collected during daily computer operations is significantly large. Potential electronic evidence contained in these digital logs may represent only a small subset of all the digital logs collected during normal computer operations. The evidentiary admissibility requirements of any subset of operational digital logs are not a predictable commodity. This temporal uncertainty makes it imperative that all digital logs, regardless of evidentiary potential be collected in a manner consistent with the evidentiary legal requirements (Casey, 2004; Kenneally, 2004; Rowlingson, 2004; Stephenson, 2000).

Where the digital logs are potential electronic evidence, the handling and storage procedures must be stringent and adhere to the relevant corporate governance best practices. Previous cost-benefit analyses in the literature have shown that business objectives are consistent with mandatory organizational consideration of evidentiary issues (Rowlingson, 2004). Forensic readiness is defined as “the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation” (Rowlingson, 2004, p. 1). This

mandates enhanced system monitoring, secure data collection procedures and an organizational culture that is aware of the legal “sensitivities” required for the collection and storage of admissible electronic evidence. Security policy and procedures that mandate forensically ready organizations can greatly enhance the quality and admissibility of electronic evidence (Stephenson, 2000; Yasinac & Manzano, 2001).

A comprehensive treatise of the nuances of the ECPA and the Federal Rules of Evidence is not appropriate for this discussion. Specific to large private-sector corporations, the primary objective of this discourse is to focus on a few relevant sections in the Electronic Communications Privacy Act of 1986 and the Federal Rules of Evidence and their relevance to the most common electronic evidence admissibility issues. Essentially the objective for this research paper is to encourage private-sector evidentiary awareness. Subsequently, the demonstrated value of a forensically ready organizational culture, along with an understanding of the importance of appropriate digital log handling techniques, may enhance evidence admissibility and quality pursuant to the FRE and the ECPA. First there will be discussion a few relevant sections in the ECPA and the FRE as they pertain to electronic evidence. This will be followed by a consideration of the organizational change required to facilitate the successful application of digital logs as electronic evidence.

Electronic Communications Privacy Act of 1986 (ECPA)

The Wiretap Act of the 1968 Omnibus Crime Control and Safe Streets Act (Wiretap Act) was not designed with consideration to the electronic evidence as seen in today’s court cases. In 1986, congress updated the 1968 Omnibus law through passage of the Electronic Communications Privacy Act of 1986 (ECPA). In order to prosecute a case in the judicial

system, electronic evidence such as intercepted electronic communications and computer records (digital logs) must be collected pursuant to the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2521. While amending the Wiretap Act to include advanced electronic communications considerations, congress added a new section known as the Stored Communications Act (SCA). The Stored Communications Act states that it is unlawful to “intentionally access without authority an electronic communication facility and thereby obtain an electronic communication while it is in electronic storage” (Burgunder, 2007, p. 577). This was primarily protection against a new enemy, the hacker. The Stored Communications Act provides a corporation the foundation for legal remedy relevant to network intrusions.

The ECPA as it pertains to private-sector employee privacy is a foundational consideration of an employer seeking to monitor employee electronic activity on its computer networks. The ECPA protection against unlawful interception or electronic trespass has been the primary judicial foundation for employee privacy rulings in the courts (Burgunder, 2007; Dixon, 1997). One issue of contention has been the application of the ECPA to employee email communications. While the ECPA’s intent with regards to email communications are not directly mentioned in the statute, in general, courts have considered emails as being in the spirit of the ECPA (Burgunder, 2007; Dixon, 1997). The implications of electronic communications in the workplace have not produced comprehensive employee privacy legislation. In the absence of concrete direction, the courts have used the ECPA as the foundational federal legislation for its rulings on electronic communication (including email) and workplace privacy (Burgunder, 2007; Dixon, 1997).

One critical organizational consideration relevant to workplace monitoring of electronic communications and system activity is the proper handling and storage of the resultant digital

logs. Most states have enacted privacy legislation that clarifies the application of the ECPA to employee privacy issues in the workplace (Dixon; United States General Accounting Office, 2002). Therefore, regardless of the jurisdiction, electronic evidence collected pursuant to the ECPA, will greatly enhance its quality and its likelihood of being admissible. The ECPA states that it is unlawful to monitor electronic communications (such as digital logs) in the workplace unless in the monitoring is in the course of ordinary (operational) business to collect information to improve business / system efficiency or to track violations of corporate policy. The employee's prior consent must be obtained through clear communication of corporate policies. The user of the corporate computer system must express either written or implied (through login banner) consent to be monitored as defined in corporate policy.

Private-Sector Prior Consent

While there are other ECPA exceptions applicable to workplace monitoring during the "normal course of business", the most legally prudent course of action for a corporation is to obtain prior consent through its acceptable use policy (Burgunder, 2007). 18 U.S.C § 2511 (2)(d) states that "a person not acting under the color of law" may intercept electronic communications where "such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception". Compliant corporate electronic monitoring pursuant to 18 U.S.C § 2511 (2)(d) requires the corporation obtain employee prior consent. One common method accepted by the courts is through the use of a clearly communicated acceptable use policy (Burgunder, 2007). A corporate acceptable use policy that specifically defines the privacy rights and expectations for employees when they are using corporate systems, serves as official notification that the employee has no expectation of privacy as defined in the policy (Burgunder, 2007).

In general, an acceptable use policy should state that the company reserves certain rights and that by means of employment and the employee's use of corporate computer systems, the employee understands and consents to the corporation's rights to monitor all employee computer activity (United States General Accounting Office, 2002). The acceptable use policy should be easily available to the employee and be communicated on a regular basis. Notwithstanding other ECPA exceptions, electronic eavesdropping without prior consent most likely be deemed inadmissible and may lead to other legal actions against the corporation.

When a corporation presents electronic evidence collected as proof of employee system activity (such as deleting files, sending emails, etc.) the corporation must show that the electronic evidence was collected pursuant to ECPA. The ECPA states in 18 U.S.C § 2511 (2)(c)-(d) that communications can be intercepted if one of the parties consent. To insure that a corporation meets its burden to demonstrate acceptable use policies that indicate that the employee has been informed of privacy expectations, periodic awareness sessions and employee acknowledgement must be demonstrated (Burgunder, 2007). He argues that the acceptable use policies should incorporate the following concepts:

1. That the corporation reserves the right to monitor, audit and review all system activity related to the use of the corporate proprietary assets as defined in the policy.
2. That there is no expectation of privacy when using corporate computer systems.
3. That there will be no tolerance with regards to offensive material as defined in the acceptable use policy (be specific).
4. It is permissible to use the corporate computer systems for limited personal use as defined in this policy and provided examples.

5. The corporation considers certain identified information to be sensitive and proprietary in nature, and this is the defining classification schemes document retention policies, information handling policies.
6. That the employee should be on notice that failure to comply with corporate policy will have consequences at the discretion of the company and that the employee has certain corporate due process options.

In addition, Jacobs (2006) also advocates administration processes that mandate appropriate time during working hours be allocated to provide mandatory training and awareness sessions for all employees. For evidentiary consideration, as validation of the corporate notification process, he advocates that all training material and employee attendance records be maintained as official business records.

Another consideration is that the acceptable use policy should be written fairly, with both employee and corporate expectations clearly defined. If an acceptable computer use policy is slanted towards the corporation without any corporate responsibilities stated in the policy it is likely that the policy will be invalidated as an unfair contract by the courts (Jacobs, 2006). As long as the acceptable use policy is deemed fair, U.S. Gen. Acct. Office (GAO) found that "courts have consistently upheld companies' monitoring practices where the company has a stated policy that employees have no expectation of privacy on company computer systems." (Wen & Gersuny, 2005). Therefore, it would be prudent to have a contract law expert review the policy through the prism of contract law to enhance the probability of meeting the burden for acceptance as prior consent.

Legal Ambiguities

As noted by Strang (2001) and in the United States Department of Justice's guide to searching and seizing electronic evidence (United States Department of Justice, 2002), while "not acting under the color of the law" as defined in 18 U.S.C § 2511(2)(d), Fourth Amendment rights are not applicable to corporations. Upon notification of law enforcement, when acting "under the color of the law" as defined in 18 U.S.C § 2511(2)(c) evidentiary rules change (Strang, 2001). Electronic evidence collection becomes increasingly difficult and the legal restrictions associated with the privacy rights under the Fourth Amendment may become an impediment. With this in mind, once it has been determined that there are issues of jurisprudence; the corporation must decide whether and when it is appropriate to involve law enforcement. Unless specifically engaged with law enforcement, private-sector corporations usually conduct monitoring operations while "not acting under the color of law" pursuant to 18 U.S.C § 2511(2)(d). The distinction between "acting under the color of law" and "not acting under the color of law" may be difficult to centrifuge so to enhance the probability of evidence admissibility, whenever possible, corporate investigators would be wise to work closely with legal counsel so as to fully understand when the line has been crossed.

Federal Rules of Evidence

As well as digital log collection that is compliant with the ECPA, corporations must handle and store electronic evidence pursuant to the Federal Rules of Evidence (FRE). Giordano (2004) illuminates the essential aspects of the FRE. He highlights that for electronic evidence to be admissible it must be authentic, complete, reliable and believable. The Federal Rules of Evidence are relevant in both federal and state courts; most jurisdictions have modeled their rules to be consistent with the federal statute. Therefore, the use of appropriate and widely accepted

best practices for the collection, storage and handling of digital logs will improve the quality and admissibility of potential electronic evidence (Casey, 2004, 2005; Kenneally, 2004). The following is a short discourse on a few sections in the statute that establish the foundation for procuring admissible electronic evidence (as digital logs) pursuant to the Federal Rules of Evidence.

Preliminary Questions – Fed. R. Evid. 104 (Rule 104)

Rule 104 exists to determine whether the electronic evidence presented has a “foundation for authenticity” (Lorraine v. Markel, 2007). The judge has wide latitude in terms of accepting the evidence. He will rule on evidence’s potential for authenticity based its relevancy as determined by “the fulfillment of a condition of fact”. Fed. R. Evid. 401 states that evidence is relevant if it has “any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.” This is not a statement of actual credibility, authenticity or reliability; it merely establishes that a “foundation for authenticity” exists (Lorraine v. Markel, 2007). Therefore, digital logs obtained through well defined and established operating procedures will generally pass this hurdle. If the electronic evidence is deemed admissible pursuant to Rule 104 hearing then the judge must decide on the authenticity of the electronic evidence.

Authenticity – Fed. R. Evid. 901 (Rule 901)

To continue an evidence admissibility inquiry, the evidence must be relevant, that is, “evidence that is not relevant is never admissible” (Lorraine v. Markel, 2007). For evidence to be admissible pursuant to the Rule 901 (FRE 901), the presenter must establish reasonable authenticity. Fed. R. Evid. 901(a) states that for evidence to be deemed authentic, the presenter must show that the evidence is “sufficient to support a finding that the [computer record] in

question is what its proponent claims” (Kerr, 2001). Fed. R. Evid. 901(b)(9) states “evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.” and be deemed authentic by the court. Therefore, properly processed digital logs will most likely be deemed acceptable and authentic under Fed. R. Evid. 901(b)(9) (Giordano, 2004; Kenneally, 2004; Kerr, 2001). The challenges to authenticity are commonly presented as follows (Giordano, 2004; Kerr, 2001):

1. Is there a reasonable expectation that the records have not been altered from their original source?
2. Are the computer programs used to collect and store the information reliable?
3. Who is the reasonable author of the electronic evidence?

Another consideration is the reliability of the tools used to collect the potential electronic evidence. For a detailed consideration of tool reliability issues see Carrier,(2003a, 2003b), Giordano, (2004), Kenneally (2001) and National Institute of Standards and Technology (2001, 2004).

Current State of Authentication under FRE 901

Without specific evidence of tampering, the courts have in general been widely accepting of electronic evidence as being authentic and admissible with a “prima facie aura of reliability” (Giordano, 2004; Givens, 2003; Grossman, 2006; United States v. Gagliardi, 2007). Relevant to electronic evidence, it appears that the courts have been unwilling to set the authenticity bar for admissibility too high (United States v. Gagliardi, 2007; United States v. Meienberg, 2001; United States v. Pluta, 1999). This may be due to the inherently difficult, costly and time consuming task to authenticate digital logs in an evidence admissibility hearing (Rowlingson, 2004; Givens, 2003; Grossman, 2006). Apparently, in general, there is no requirement to "rule

out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be." (United States v. Pluta, 1999 at *16). Subsequently, the courts appear more willing to mitigate the admissibility complexities of authentication by letting the jury decide the weight of the evidence (Givens, 2003; Grossman, 2006; United States v. Catrabran 1988; United States v. Gagliardi, 2007; United States v. Tin Yat Chin, 2004). Givens surmises about the fairness of a low bar relevant to FRE 901 arguing that "although this result may seem unfair, it seems to be the most reasonable method of authentication because forcing the proponent to prove authenticity would be incredibly difficult and time consuming" (at *107).

Important Authenticity Considerations

The literature indicates that there are a significant number of practitioners that are not in favor of a token authentication burden for computer records pursuant to FRE 901. They argue that many juries may lack the expertise to determine electronic evidence authentication and may apply undue weight to inappropriate evidence (Casey, 2004; Chaikin, 2006; Giordano, 2004; Givens, 2003, Kenneally, 2004). As shown in *American Express Travel Related Services Company, Inc. v Vee Vinhnee* (2006), it appears that the courts may be open to consideration of a more stringent test of authenticity under FRE 901. In this bankruptcy proceeding, American Express attempted to increase its share of the bankruptcy claim based on its electronic billing statements. They asserted that its electronic evidence (billing statements) was reliable and accurate solely due to its excellent computer record maintenance processes. Normally, as discussed earlier, their proof of reliable processing would most likely been sufficient to clear the FRE 901 hurdle. They presented no other corroboration pertaining to the reliability and accuracy of their computer records, just the fact that they had processes in place. The US Bankruptcy Appellate Panel of the Ninth Circuit ruled that for American Express to "merely assert that its procedures for

maintaining computer records were designed to ensure accurate records and identify errors in those records” was not sufficient for admissibility. Specifically, the court ruled that proof of digital evidence’s authenticity and accuracy will only be admissible if American Express could prove with corroborated data that “computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging of changes, back up practices, and audit procedures to assure the continuing integrity of the records” were in place at the time of data collection. As will be discussed later in this paper, these are essential components of a forensically ready organization.

In the future, there may be an increased potential for the unexpected, anonymous and concealed manipulation of electronic data as a result of the increasingly complex nature of computer networks and the significant threat of computer vulnerabilities targeted at digital logs (Casey, 2004; Chaikin2006; Richardson, 2007). Consequently, this may potentially lead to a more rigorous authenticity requirement pursuant to FRE 901 for the admissibility of electronic evidence (Giordano, 2004; Givens, 2003; Chaikin, 2006). The objective of this paper is to present strategies to enhance the likelihood of admissibility of electronic evidence. Relevant to evidence authenticity, the following makes it prudent to encourage the corporation to be forensically aware and incorporate digital log handling best practices as defined later in this discourse:

1. The increased potential for a more stringent authentication requirement pursuant to FRE 901 as observed in the American Express v. Vee Vinhnee (2006) ruling.
2. The increased probability of the aforementioned threat of anonymous and concealed malicious alteration of digital logs.

3. The need to provide evidence weight based on the quality and authenticity of the digital logs when they are presented in trial.

The discourse in this section is focused on the admissibility question. Therefore, relevant to the admissibility of electronic evidence, as previously indicated, absent proof of tampering, it appears that currently Rule 901 is not a major hurdle (Givens, 2003; Grossman, 2006; United States v. Catrabran 1988; United States v. Gagliardi, 2007; United States v. Tin Yat Chin, 2004).

Computer Record Storage

Another key consideration to enhance the authenticity of electronic evidence is related to the organization's digital log storage strategy. Whether to encrypt and hash the digital logs as well as determination of the physical storage location are essential considerations. Encryption is used to conceal information, while hashing algorithms are used to guarantee unaltered data. (Bosworth & Kabay, 2002). Digital logs that are stored in an encrypted form and then authenticated through a hashing algorithm are practically impossible to alter maliciously (Forte, Maruti, Vetturi, & Zambelli, 2005; Schneier & Kelsey, 1999). Concealment and protection of computer records through strong data encryption techniques (AES) and hashing algorithm (MD5) techniques is another way to insure computer records remain unaltered and in their original form (Forte, Maruti, Vetturi, & Zambelli, 2005; Schneier & Kelsey, 1999). It may be prudent to selectively encrypt the most sensitive digital logs because encryption of large volumes of digital logs may present significant cost and efficiency issues.

Stephenson (2000) recommends that the logs be spooled on a pseudo real-time basis to another remote highly secure host. This host should not have any trust relationships, have stealthy ports, have limited access and use a tunneled VPN to spool the logs from the operating environment. Data encryption and hashing algorithms are commonly used techniques

implemented by system administrators to protect computer record integrity. The spooled log files should then be backed up to computer tape and physically moved to a secure and isolated location. These tapes should be treated as potential electronic evidence with regards to storage and chain of custody. By depending on the tapes for your evidence (not the actual logs) the organization has significantly addressed the trustworthiness issue for the logs.

Computer Records – Hearsay Exception to Fed. R. Evid. 801 (Rule 801)

Hearsay evidence is a testimonial statement offered that was not directly communicated by its source during legal proceedings. In most cases, the admissibility of human statements is considered for potential hearsay ramifications. Hearsay evidence is not admissible unless it satisfies one of the exception clauses in Fed. R. Evid. 803(6). Since a computer record is presented in court as a testimonial statement of an event, it has been mostly unsuccessfully attempted to consider it hearsay (Kerr, 2001). Computer records collected during the normal course of business are mostly deemed admissible under the business record exception, Fed. R. Evid. 803(6) (Kerr, 2001).

A Few Digital Log Handling Considerations

Corporations utilize log files for tracking of system events such as user activity, system and application access, system process and file usage, network activity, invalid log-on attempts, email communications and resource usage (Bosworth & Kabay, 2002). A few relevant and detailed guides relevant to digital log best practices and published by the National Institute of Standards and Technology include: Computer Security Incident Handling Guide (National Institute of Standards and Technology, 2008), Guide to Computer Security Log Management (National Institute of Standards and Technology, 2006a) and the Information Security

Handbook: A Guide for Managers (National Institute of Standards and Technology, 2006b).

These guides provide an excellent in depth roadmap for implementation of well established digital log best practices that will greatly enhanced probability of legally admissible electronic evidence under the Federal Rules of Evidence.

Stephenson (2002) argues that the Federal Rules of Evidence require a reliable, consistent and corroborated chain of evidence. Digital logs can serve to prove or disprove an investigatory hypothesis. Digital log corroboration involves the synchronization and validation of system events captured in a multitude of varied digital logs stored in different system locations.

Stephenson (2003) stresses “the concept of a fully corroborated, structured end-to-end analysis is important to the successful investigation of complex digital incidents and their presentation in court”. In itself, the content of an individual log file usually does not provide relevant and meaningful evidence in the event reconstruction process. Single log files without corroboration with other system events are not sufficient to satisfy the authenticity requirements of Federal Rules of Evidence (Rule 901). The event reconstruction process requires consideration of evidence from a myriad of electronic sources and digital logs. The large volume of digital logs in varied locations mandates a cohesive, proactive and forensically enabled collection strategy so as to insure a comprehensive, corroborated and admissible evidence analysis process. Solving the investigatory puzzle using the corroborated logs may lead to the most likely scenario of events. (Forte, 2004; Gorge, 2007, Stephenson, 2000).

In the corporate environment, the proper collection and storage of admissible electronic evidence can encounter two primary roadblocks: 1) the high cost associated with appropriate training, data storage, and productivity losses associated with handling large volumes of complex digital logs, and 2) operational data collection processes that don't consider evidentiary and

admissibility implications due to a reactive (not proactive) corporate culture (Barbara, 2005; Rowlingson, 2004; Stephenson, 2000).

Cost and Complexity Issues

In the private-sector, the cost of collecting and analyzing digital logs, maintaining a forensically aware organization and the lack of an appropriate legal and evidentiary organizational knowledgebase are major impediments of obtaining admissible electronic evidence (Barbara, 2005; Rowlingson, 2004).

Cost efficient digital log handling processes that are legally relevant can be achieved through the establishment of a “Corporate Swat Team” (Stephenson, 2000). This team will be trained to investigate situations involving evidentiary concerns, manage evidence collection, interview witnesses, and contain damage during and after a computer security incident (Stephenson, 2000). The “Corporate Swat Team” will facilitate and insure that the requisite “chain of custody” for the electronic evidence is maintained. Casey (2005) argues that “Effective case management and methodological reconstruction of events can help create a more complete picture of the crime and help establish links between computer intruders and their illegal activity”. In addition to the “Corporate Swat Team”, as will be discussed in the next section, a well trained corporate forensics lab can greatly improve digital log processing efficiency and reduce the costs associated with forensic handling.

System log files are a primary information source for the collection of electronic evidence in the workplace. Digital logs (potential electronic evidence) can be ambiguous, complex and contain millions of line entries. Corporate investigations pursuant to legal proceeding can be multifaceted and costly. Large volumes of complex log data will inherently lead to potential evidence admissibility issues. For these digital logs to be admissible, potential

electronic evidence must be converted into a reliable, consistent, accurate, and acceptable format. This can be an overwhelming and time consuming procedure (Carrier, 2003a). Rowlingson (2004) argues that the complexity, volume and cost of high quality admissible electronic evidence can be managed if the proper methodology and incident management procedures are proactively in place.

Rowlingson (2004) thesis is that with appropriate, comprehensive training of system administrators and incident handlers, irrelevant electronic evidence can be more easily distinguished from relevant electronic evidence, thus reducing the overall evidence complexity and its associated costs. One way to reduce the effect of the complexity is to have a unit specially trained in the relevant techniques. A large corporation might setup its own digital forensics lab and have it certified by the same organization that certifies the government labs, that is obtain ASCLD/LAB accreditation (Barbara, 2005). In addition to addressing the cost and complexity issues, there are evidentiary considerations for obtaining ASCLD/LAB accreditation. Two relevant advantages achieved during evidence presentation in legal proceedings are improved authenticity and reliability arguments, as well as the perceived value of evidence collected by an ASCLD/LAB accredited lab. The ASCLD/LAB quality manual provides an organization with the requisite roadmap to establish professional relevance, standards and controls, equipment calibration procedures, practices to continue examiner competence, and audit strategies (Barbara, 2005). These will serve as proof of the organization's ability to collect and store admissible electronic evidence through professionally accepted procedural and electronic evidence validation techniques.

Forensic Readiness and Corporate Culture

Indoctrination of a forensically aware corporate culture will not be a revolutionary process; rather it will be an evolutionary development. The organization will evolve as its employees become forensically aware through consistent use and training that stress well established best practices and their relevance to the organization's well being. Rowlingson (2004) suggests the following will promote a forensically aware corporate culture:

1. Define the business scenarios that require digital evidence.
2. Identify available sources and different types of potential evidence.
3. Determine the evidence collection requirement.
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement.
5. Establish a policy for secure storage and handling of potential evidence.
6. Ensure monitoring is targeted to detect and deter major incidents.
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
9. Document an evidence-based case describing the incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.

When digital logs are collected as potential electronic evidence, the collection protocols must consider the following: evidence admissibility, authenticity, completeness, reliability and believability (Giordano, 2004). A proactively prepared and forensically aware organization that

has established forensic readiness as an operational requirement insures a high probability of procuring admissible electronic evidence (Bosworth & Kabay, 2002; Casey, 2004; Gorge, 2007; Rowlingson, 2004; Stephenson, 2000). It is essential that the organization incorporates a forensic mindset into its daily operational culture (Rowlingson, 2004).

Conclusion

This discourse presented discussion of a few key evidentiary issues pertaining to the Federal Rules of Evidence (FRE) and the Electronic Communications Privacy Act of 1986 (ECPA) as applied to the collection of electronic evidence using digital logs in large private-sector corporations. As was presented in this dialogue, establishment of electronic evidence admissibility in legal proceedings requires digital logs that are authentic, complete, reliable and believable. The primary roadblocks for the collection of admissible electronic evidence in a large corporation are cost, log complexity and organizational culture. The author has presented practical and potential mitigation of these risks through the implementation of the appropriate digital log best practices and acceptable use policies. Creation of an accredited digital forensic lab and a “corporate swat team” was also demonstrated as a possible suitable mitigation strategy. Finally the case was presented for incorporation of these mitigation techniques to facilitate the evolution of a forensically aware corporate culture as a means to achieving a reliable environment for the collection of potential electronic evidence in digital logs.

As stated earlier, approximately 85 percent of the 66 million dollars lost by corporations due to computer related crime in 2007 was categorized as financial fraud or company insider abuse of computer networks (Richardson, 2007). This loss does not include the hidden costs associated with potential adverse affects on a firm’s stock price due to the public perception of

the security breach (Campbell, Gordon, Loeb and Zhou, 2003). This discourse has shown that a forensically aware corporate culture that embraces best-in-class digital log handling practices will most likely provide the requisite rigor for legally admissible and high quality electronic evidence collection. Subsequently, through the recommended actions presented, corporate costs and legal vulnerabilities may be mitigated through the appropriate criminal deterrence and financial retribution.

References

- American Express Travel Related Services Company, Inc. v Vee Vinhnee, BAP No. CC-04-1284-KMoP, 2005 U. S. Bankruptcy Appellate Panel for the Ninth Circuit, LEXIS 2602.
- Barbara, J. J. (2005). Digital evidence accreditation in the corporate and business environment, *Digital Investigation*, 2(2), 137-146.
- Bosworth, S., & Kabay, M. E. (Eds.). (2002). *Computer Security Handbook* (Fourth ed.): Wiley.
- Burgunder, L. (2007). *Legal Aspects of Managing Technology* (Fourth ed.): Thomson, West.
- Campbell, K., Gordon, L., Loeb, P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3). 431-448.
- Carrier, B. (2003a). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of Digital Evidence*, 1(4).
- Carrier, B. (2003b). Open source digital forensics tools; the legal argument. Retrieved October, 2004, from http://www.cerias.purdue.edu/homes/carrier/forensics/docs/opensrc_legal.pdf.
- Casey, E. (2004). *Digital Evidence and Computer Crime* (Second ed.): Elsevier Academic Press.
- Casey, E. (2005). Case study: network intrusion investigation - lessons in forensic preparation. *Digital Investigation*, 2(4), 254-260.
- Chaikin. (2006). Network investigations of cyber attacks: the limits of digital evidence. *Crime, Law and Social Change*, 46(4), 239-256.
- Daubert v. Merrell Dow Pharmaceuticals, Inc., No. 92-102, 1993 U.S., LEXIS 4408.
- Dixon, R. (1997). Windows Nine-to-Five: Smyth v. Pillsbury and the scope of an employee's right of privacy in employer communications [Electronic Version]. *Virginia Journal of*

Law and Technology, 2. Retrieved March, 2008, from
http://www.vjolt.net/vol2/issue/vol2_art4.html.

Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521 (1986).

Forte, D. (2004). The "art" of log correlation: tools and techniques for correlating events and log files. *Computer Fraud and Security*, 2004(8), 15-17.

Forte, D.V., Maruti, C., Vetturi, M.R., & Zambelli, M. (2005). SecSyslog: an approach to secure logging based on covert channels. *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, 248-263.

Giordano, S. (2004). Electronic evidence and the law, *Information Systems Frontiers*, 6(2), 161-174.

Givens, L. (2003). 2003 Cumberland Law Review, 2003 34 Cumb. L. Rev. 95, LEXIS

Gorge, M. (2007). Making sense of log management for security purposes - an approach to best practice log collection, analysis and management. *Computer Fraud & Security*, 2007(5), 5-10.

Grossman, A. (2006). 2006 George Mason Law Review, 2006 13 Geo. Mason L. Rev. 1309, LEXIS

Jacobs, L. (2006). 2006 Journal of Law and Policy Journal of Law and Policy, 2006 14 J.L. & Pol'y 837, LEXIS

Kenneally, E. (2001). Gatekeeping out of the box: Open source software as a mechanism to assess reliability for digital evidence [Electronic Version]. *Virginia Journal of Law and Technology*, 6. Retrieved March, 2008, from <http://www.vjolt.net/vol6/issue3/v6i3-a13-Kenneally.html>.

Kenneally, E. (2004). Digital logs – proof matters. *Digital investigation*, 1, 94-101.

- Kerr, O. S. (2001). U.S. Department of Justice, United States Attorneys' USA Bulletin: Computer records and the federal rules of evidence [Electronic Version], 49(4). Retrieved March, 2007, from http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm.
- Lorraine v. Markel Am. Ins. Co. NO. PWG-06-1893, 2007 U.S. Dist. (Maryland), LEXIS 33020.
- National Institute of Standards and Technology (2001). General test methodology for computer forensic tools. Retrieved October 2, 2004, from <http://www.cftt.nist.gov/documents.htm>
- National Institute of Standards and Technology (2004). Computer forensics tool testing. Retrieved November 11, 2004, from <http://www.cftt.nist.gov/>.
- National Institute of Standards and Technology (2006a). Guide to computer security log management. Retrieved March, 2008, from <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>.
- National Institute of Standards and Technology (2006b). Information security handbook: a guide for managers. Retrieved March, 2008, from <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>.
- National Institute of Standards and Technology (2008). Computer security incident handling guide. Retrieved March 11, 2008, from <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>.
- Richardson, R. (2007). 2007 CSI/FBI computer crime and security survey. Retrieved March, 2008, from <http://www.gocsi.com/>
- Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3).
- Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. *ACM Trans. Inf. Syst. Secur.*, 2(2), 159-176.

- Stephenson, P. (2000). *Investigating Computer-Related Crime* (First ed.): CRC Press.
- Stephenson, P. (2002). Digital end-to-end digital forensics: getting the whole picture. *Computer Fraud and Security*, 2002(9), 17-19.
- Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report*, 8(2), 42-54.
- Strang, R. (2001). U.S. Department of Justice, United States Attorneys' USA Bulletin: Recognizing and Meeting Title III Concerns in Computer Investigations [Electronic Version], 49(2). Retrieved March, 2007, from http://www.usdoj.gov/criminal/cybercrime/usamarch2001_2.htm.
- United States Department of Justice. (2002). *Searching and seizing computers and obtaining electronic evidence in criminal investigations* [Electronic Version]. Retrieved March, 2008, from <http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm>.
- United States General Accounting Office. (2002). Report to the ranking minority member, subcommittee on 21st century competitiveness, committee on education and the workforce, House of Representatives, employee privacy: Computer-use monitoring practices and policies of selected companies. (GAO-02-717).
- United States v. Catabran, No. 86-1134, 1988 U.S. App., LEXIS 66.
- United States v. Gagliardi, No. 06-4541-cr, 2007 U.S. App., LEXIS 24644.
- United States v. Meienberg, No. 00-1390, 1984 U.S. App., LEXIS 16004.
- United States v. Pluta, No. 98-1443, 1999 U.S. App., LEXIS 8189.
- United States v. Sanders, No. 84-1327, 2001 U.S. App., LEXIS 19177.
- United States v. Tin Yat Chin, No. 03-1621, 2004 U.S. App., LEXIS 10707.

- Wen, H.J., & Gersuny, P. (2005). Computer-Based monitoring in the American workplace: surveillance technologies and legal challenges, *Human Systems Management* (24), 165-166.
- Yasinac, A., & Manzano, Y. (2001). *Policies to enhance computer and network forensics*. Paper presented at the Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. United States Military, West Point, NY, June 2001.