4-12-2006

Enterprise Computer Forensics: A defensive and offensive strategy to fight computer crime

Fahmid Imtiaz
Edith Cowan University

DOI: 10.4225/75/57b1311ec7051
4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.

Enterprise Computer Forensics: A defensive and offensive strategy to fight computer crime

Fahmid Imtiaz
School of Computer and Information Science
Edith Cowan University
fahmidimtiaz@gmail.com

Abstract

As days pass and the cyber space grows, so does the number of computer crimes. The need for enterprise computer forensic capability is going to become a vital decision for the CEO's of large or even medium sized corporations for information security and integrity over the next couple of years. Now days, most of the companies don't have in house computer/digital forensic team to handle a specific incident or a corporate misconduct, but having digital forensic capability is very important and forensic auditing is very crucial even for small to medium sized organizations. Most of the corporations and organizations are still not aware of the risks and this can be very harmful in the long run. This paper will particularly focus on examining different aspects of enterprise computer forensics with in-house forensics capability. It will also try to clarify some of the issues that surround enterprise computer forensics.

Keywords

Enterprise computer forensics, computer crime, digital forensics.

INTRODUCTION

In today's fast growing economy, a company's IT infrastructure controls a significant part of business and communication needs. The needs are obvious but often companies misunderstand or sometimes deliberately ignore the need for proper security measures to secure the company's network resources and intellectual property. A single security breach or an attack can cause great financial and reputation loss, which can be devastating for a well-known organization. As security experts are trying their best to defend against the latest forms of attacks, attackers are moving on devising plans and potentials for more sophisticated attacks. This causes growing concerns for security experts around the world. That is why organizations really have to realize the risks before an actual attack or security breach. Therefore, both internal and external threats should be considered and a significant portion of the IT budget of an organization needs to be devoted for hiring security experts and taking proper security measures. Now days, security experts prefer detecting and tracing attacks before an actual attack and they also try to motivate the organizations to think about the post attack scenario. A certain security breach can leave different trails and clues, which helps forensic experts to identify the person/s responsible for the incident. Of course, external forensic teams can be brought in and they can work on a certain case/security breach. Nevertheless, companies have to understand that this is an ongoing problem and it repeats over time. Often the company looses control of the case or hide information from the third party forensics examiners as sensitive internal issues/secrets can be revealed. Having in-house forensic team can save both time and money and it would reduce the chance of information leakage about any internal matters. Therefore, having an in-house forensic team to validate and gather information that can have forensic value will help a company to defend against attacks and prosecute attackers; as a result, save the company from great loss. Companies and organizations that deal with sensitive customer information like credit card numbers; health records, mortgage information and so on are particularly vulnerable to attacks. Other companies no matter what type of business they do are not safe because IT is almost an essential part of every business now days. Every company deals with sensitive business information no matter how small and regardless of what business they do. Attacks and intellectual property theft is more common these days as it was couple of years ago. A company would be

fortunate if they were able to recover the financial loss caused by an attack/ breach but their reputation will be at stake and what if the attack comes from an external source, which sometimes makes prosecuting the attacker even more difficult. This is where enterprise computer forensics can come in with in-house forensic experts and save a company from disaster. Forensic audits can reveal information that would be some intruder's nightmare. To be very specific, in-house forensic teams can save a company from both financial and intellectual property losses in most cases. Forensic audits are vital to analyse and validate information that enables experts to scientifically and forensically analyse and reconstruct the events that took place. This paper examines how enterprise computer forensics can help to trace and deal with attacks and intellectual property thefts when applied in-house. It will also identify some important issues related to enterprise computer forensics.

THE ROLE OF COMPUTER FORENSICS

According to Information Systems Audit and Control Association (ISACA) "Computer forensics is the collection, preservation, analysis and court presentation of computer related evidence. In addition to civil and criminal jury trials, computer evidence often is presented in arbitration, administrative and mediation proceedings, congressional/government hearings and presentations to corporate management. Accordingly, the proper collection and analysis of computer evidence through accepted computer forensic protocols is a critical component to any internal investigation or audit where the results have at least the potential to be presented in legal proceedings". Barish (2002) says, "We have to take every precaution to make sure the data we collect is accurate, trusted, and is not modified from the time of collection onward. By recording each step in the collection and processing of forensic data, and tracking its movement, who accessed it, and what was done to it, we help preserve the 'Chain of Custody'". Computer forensics is used not only for internal investigation, compliance due diligence and law enforcement, it can be also applied as a counter-measure to detect and stop computer crimes. In brief, Computer forensic is a scientific approach that is used to process computer related attacks/security breaches and misconducts. By using proper forensic tools and tests, forensic examiners are capable to prove and validate certain actions (misconducts) in the court. It is important to understand that computer forensic methodologies are applied not only to prove guilt; it can also be used to prove innocence as well. Besides that, forensics methodologies can be applied for operational troubleshooting, log monitoring, data acquisition, data recovery and due diligence.

THE REAL PICTURE

"In 2006 Total average annual losses from electronic attack, computer crime, and computer access misuse or abuse increased by 63% to $241,150 loss per organization compared to 2005" says AusCERT (2006). According to CSI/FBI computer crime and Security Survey 2006 "Virus attacks continue to be the source of the greatest financial losses. Unauthorized access continues to be the second-greatest source of financial loss. Financial losses related to laptops (or mobile hardware) and theft of proprietary information (i.e., intellectual property) is third and fourth. These four categories account for more than 74 percent of financial losses". The information is relevant and not very surprising. However, the 2005 and 2006 CSI/FBI Computer Crime and Security Survey claims that the total dollar amount of financial losses resulting from security breaches had a substantial decrease in year 2004 and 2005 respectively. According to The Internet Crime Compliant Centre (IC3), it is true that the financial loss decreased in 2004 but in 2005, it did not. The CSI/FBI survey conducted in 2004 reported that the number of cyber crime incidents has dropped. The CSI/FBI 2005 survey and IC3 report 2005 contradict each other although they both provide information based on actual complaints. IC3 complaints are reported through their web site and their report shows that cyber crime is on the rise and there is no reason to believe that cyber crime incidents are decreasing. According to Arnone (2006) "Cyber crime increased dramatically in 2005 and 2006 promises even more incidents, a panel of federal cyber security experts said. Driven by profit, cyber criminals in 2006 will use the massive increase in malware variants created in 2005 to initiate even more insidious and hard-to-detect attacks, said Dave Cole, director of Symantec Security Response at Symantec. Botnets – remote-controlled networks of hijacked computers – will grow in size and popularity, said Cole, who moderated the discussion that Symantec sponsored in Washington, D.C". This is not good news and it conflicts and disagrees with the CSI/FBI 2005 findings. Moreover, the IC3 Internet Crime Report 2005 agrees with

Michael and mentioned in their report "From January 1, 2005 – December 31, 2005, The Internet Crime Compliant Centre (IC3) website received 231,493 complaint submissions. This is an 11.6% increase over 2004 when 207,449 complaints were received. These filings were composed of fraudulent and non-fraudulent complaints primarily related to the Internet". The CSI/FBI 2006 report claims that 80% of the organizations perform security audits comparing to that of 2005, which was 87%. If this is true, the number of security breaches and complaints should have decreased in 2005 if not in 2006. This enables us to conclude that the security audits are not enough to stop computer/cyber crime. Moreover, how effective and successful security audits do majority of the organizations perform that is questionable. These finding has reasons to believe that internet and computer crime is on the rise, the computer security audits are not enough to stop computer crimes. Moreover, security precautions are reasonably weak, which allows intruders and frauds to continue with their activities. Therefore, instead of depending on third party security experts and security audits only, it is time that organizations think about enterprise computer forensics strategies and therefore, have in-house forensic experts. This will enable an organization to gather intelligence on its own computer and network systems resources. It will also enable tracking of staff activities. Talking about security audits, forms and methods of forensic auditing has to be included within the security audit. Otherwise, there is no likelihood of decrease in cyber crime.

ENTERPRISE COMPUTER FORENSICS

Enterprise computer forensics is a strategic security measure that not only ensures integrity and availability of the corporate information system but also saves millions of dollars if applied in-house. In general, an organization's security strategy reflects their willingness to secure their systems. In Australia, the picture is frightening because "More than half of the organizations in Australia do not follow any form of IT security standards at all", says AusCERT (2006). According to CSI/FBI Computer Crime and Security Survey 2006 and AusCERT Computer Crime and Security Survey 2006 "In the U.S. 38% of the companies use forensic tools and techniques as a form of security strategy, whereas in Australia it is only 6% and only 5% companies spent 43% of their IT budget for IT security in a whole year in Australia". Enterprise computer forensic team will not only need to deal with all the computing resources used by an organization, it also has to forensically audit whether the employees are following the organization policies or not, while using the companies IT resources. The threat against cyber crime, no matter it is from external or internal forces, can be reduced by taking measures that is capable of dealing with both pre and post attack situations. There is a growing phenomenon among the top managements of enterprises, which is to detect sophisticated attacks through real-time analysis, detection and prevention strategies, which is good. However, often companies would not think about the scenario after the attack. Incident response plan and post analysis and discovery of the intrusions are equally important. Enterprise computer forensics is about getting all these bits and pieces together and this enables an organization to be capable of handling any computer related incidents. Today there are network and host based computer forensic tools that are used for forensics analysis of different events. Encase is one of the network based forensics analysis tool that is being widely used now days. Besides that, there are host based analysis tools as well like Autopsy. Often the scope and the geographical distance involved in external attacks make it impossible to take legal actions against the intruders. Therefore, there is likelihood that attackers cannot be prosecuted due to the local law of the place they originate. In some countries, there is no telecommunication and interception law at all. Nevertheless, in near future these restrictions and situations will change and computer forensics methodologies will enable enterprises to get the intruders/attackers behind the bar regardless from where they are operating.

Incident Response

Incident response facilitates an organization by taking quick pre-planned actions after a certain security breach/ incident. Enterprise computer forensics needs integration of forensic techniques in incident response and this will enable prompt response and action after a certain incident in a forensic manner. As soon as a security breach occurs, the evidence and scene is to stay as it is for forensic analysis and this is a part of the computer forensics methodology. "Understanding the methodology and technology behind computer forensic investigations is of critical importance to those interested in protecting their assets both from internal and external forces", says Patzakis, President and CEO of Guidance Software. The use of proper forensic methodology quickly and

correctly in case of a security breach is crucial to determine the force behind the breach and it should be a part of the organizations incident response plan. All employees must know where to contact when a certain breach or misconduct occurs. Before anyone else gets to the scene the forensic experts needs to search and seize the evidence and use it to backtrack the intruder or to reconstruct the event that took place. A company's incident response strategy needs to detail the structure, alert mechanisms, reporting and personnel involved in incident response. According to the AusCERT Computer Crime and Security Survey 2006, "Only 51% companies used incident management procedures this year". Therefore, there are many companies still out there, which do not have any incident response plans.

Forensic Analysis

Forensics analysis is the heart of enterprise computer forensics. Through analysis forensic experts are able to track the origin and time of an incident. Analysis of the evidence is required to identify the perpetrator, claim damages and defend copyrights. Enterprise computer forensic team needs to analyse and search for clues in deleted information, web activity logs, Internet traffic logs, hard drives and so on. These are very important for enterprise information security. The audit logs and incident reports need careful analysis in order to find clues or trails of attacks or breaches. In a post-incident situation, it is important to make sure that the evidence has not been altered. Patzakis (2003) says, " Electronic evidence is fragile by nature and can be altered and erased without proper handling". The most critical and important part of electronic evidence is the need to follow a sound forensic methodology of seizure and handling that guarantees the reliability, and therefore the admissibility, of the data collected. Seizing and acquiring evidence is very critical because there might be backdoors that are still open if the system connected to a network. While copying/imaging the storage media, it is important for the forensics examiners to make sure that every media image is validated and the evidence is recoverable. Patzakis (2003) says "An important feature computer forensic software is the verification process that establishes that the investigator did not tamper or corrupt with the subject evidence at any time in the course of the investigation". Careful observation is required for anything unexpected or suspicious in the compromised system's image. "Digital evidence has both physical and logical aspects. The physical side of it involves hardware components, peripherals, and media, which may contain data or the means to access it, while the logical side deals with the raw data extracted from a relevant information source" says Jansen (2004) .It is vital for forensic examiners to understand that evidence and data may not always be in digital format. In some cases, the clues and the evidence may be in different format other than digital. For, example interviews and involved system surroundings can sometimes help in a certain investigation. Forensic analysis today is so advance that even after information has been deleted, traces and clues about the deleted information are recoverable. Patzakis (2003) says "In addition to the active data normally seen by the computer user, compute forensics software allows the examiner to recover all the deleted files that have not been completely over-written, as well as other forms of unallocated or temporary data. Moreover, successful computer forensic investigation often depends on advanced techniques such as recovering temporary files from unallocated clusters or recovering and decoding deleted Windows recycle bin files, deleted registry entries and so on". Therefore, if the proper forensic model were followed, such as the abstract digital forensic model stated by Reith (2002), it would enhance the chance to recover from disaster and data loss. By analysing the forensic audit logs, attacks can be traced early and precautions can be taken well before the attack. One of the facts about forensics analysis is that it costs a lot when it comes to time and money. At the beginning of this paper it was mentioned that a significant portion of the IT budget needs to be devoted in computer forensics activities in order to get the full advantage of computer forensic techniques and methodologies. Therefore, companies need to consider the budget at very first before taking any enterprise computer forensics initiatives.

Forensic Discovery

Discovery on computer evidence forensically retrieved should have compelling information about the intrusions and attacks. After careful analysis, the forensic discovery findings should be able to back trace and justify what actually happened. This will make sure the enterprise is capable of presenting admissible evidence in court if required. Moreover, in certain cases proper forensic discovery will enable a company to get rid of its cheating

employees. During the forensic discovery process, every step has to be documented precisely, so that any evidential information can be reported and verified; in certain cases, a witness can sign the forms/documents. The forensic discovery process is primarily dependent on the skill and knowledge of the forensic expert who is conducting a certain analysis or discovery. For example, a forensic expert who is specialized in magnetic data storage and magnetic disks is likely do a better forensic discovery and analysis on hard disks and storage medias. These things need to be considered carefully at enterprise level. An enterprise forensic team will need to have people with different forensic expertise to solve the different corporate computing misconducts. There is an interesting old phenomenon about computer-based discovery, which may be still bouncing inside the head of the some top management, is cost. Discovery of computer-based information seems to cost more, take more time and create more headaches than conventional paper based discovery. However, the thing that needs to be considered now is that almost 90% of information is written and stored in digital format and this helps to reduce the huge amount of paperwork.

Challenges

The way to enterprise forensics is full of challenges and complications, but still it is a subject of interest to security professionals and forensics experts. As new computing, communication and storage devices come out and take over the market forensics examiners have to find new tools and techniques for forensic analysis and discovery. In future, PDA's and mobile devices will replace desktop computers and therefore, digital forensic will have to cope and evolve with what the future has to offer. It will not be an easy task for forensic examiners and experts. Researchers and practitioners who deal with these devices know that there are many complications in acquiring the images of these devices. The main problems are that these devices have very small storage space and they run on battery. Jansen (2004) says, "Where PDAs are concerned, the collection process normally involves dynamic and volatile information that may be lost unless precautions are taken at the scene of the incident or crime". As their memory is volatile and it runs on battery a successful data acquisition is always a challenge. Some smart phones have power saving mode but limited power supply remains an issue. There are different tools and software available in the market to acquire the information stored in cell phones but none of them are complete because none is capable of acquiring the information from a single vendor product, let alone all products. Different versions of a product have different ROM and firmware and the interoperability problem of the forensic tool used becomes an issue while forensic acquisition. The firmware and ROM can be different even in the same model of a specific product. These issues make things challenging and complicated. However, an enterprise should decide carefully and analyze these issues before giving corporate phones to their employees. Phone and PDA's now days have extended storage capacity and Bluetooth. The storage space, although very small, a lot of information can be stored and transferred via Bluetooth. Again, these issues need careful consideration and a company should only hand over such phones to their employees, which the company is capable of analyzing forensically.

EMPLOYEES WITH CRIMINAL INTENT

Anyone who works with Computer forensics and network security will agree that not only external attackers can compromise corporate networks and computer systems, staffs that work or use to work for the company can cause significant damage as well. According to AusCERT Computer Crime and Security Survey 2006 "In the year 2005 from the total number of attacks, 81% attacks were external and 37% internal". Because employees work within the internal network of the company, it is easier for them to access the computer systems inside. Since they already have the knowledge, and approved authentication and privilege needed, internal staffs can easily compromise systems that are sometimes impossible for external attackers to get into. Often organizations will take steps to safe guard their computer system from external sources but they forget that the so-called virus can be within the boundary of the enterprise. There are numerous examples where current or former employees have tired to cause damage to the protected computer systems. The website of Computer Crime & Intellectual Property Section United States Department of Justice contains numerous incidents related to computer crime, one of the latest one is "Florida man sentenced for causing damage and transmitting threat to former employer's computer system". Organizations have to take measures to stop identity theft, trade secrets/intellectual property theft, financial theft, sabotage and so on. and to do that they have to devote substantial amount of the IT budget to computer forensics, forensic audits and network security. "Now is not the time to be winding back on

protective security countermeasures or reducing IT security budgets. Greater effort needs to be made at the organizational level and through computer security initiatives that benefit the broader Internet using community in general", says AusCERT (2006). The way to overcome the problem is to enforce proper policies and having an incident response plan integrated with forensic techniques. According to AusCERT (2006), "In 2006 only 54% companies applied business continuity management (BCM) policies and procedures". To secure the enterprise computer system small to medium sized organizations need in-house forensic experts and forensic audits are essential to gather intelligence about intruders and attackers both external and internal. This will consolidate the enterprise security system by enabling the organization to trace criminal intents and prosecute criminals.

CORPORATE ENPIONAGE VS ENTERPRISE COMPUTER FORENSICS

Corporate espionage can mislead or even destroy information that has forensic value. It is a very informal approach, to some it might sound ridiculous, but it does not solve the problem instead, it intensifies it. Often people in the higher order of the chain in an organization just ignore this fact and espionage is more acceptable to them instead of having policies that lawfully enables the organization to perform legitimate forensics analysis and audits. The fact is the analysis and acquisition of information that can have forensic value, should only be validated and tested by experts not the department heads or any other person. There are numerous examples where the human resource head or the IT manager responded to a corporate misconduct knowing or not knowing that a breach has occurred and destroyed the integrity of the actual forensics evidence. This makes the actual job harder for the computer forensics experts because what they could have proved and solved in days would take them weeks because of the so-called corporate espionage. Knowing that, just by putting effective policies in place a company legally has the right to forensically analyse and audit its computing and information resources, would just amaze some people, but it is true.

COMMITMENT TO POLICIES

According to Grimes (2006), "This years IDG Security Research Report mentioned that 44% employees underestimate importance of following security policy and this is the one of the top challenges for enterprise security". To enforce enterprise forensic methodology, top to bottom level staffs in organizations need to be committed to follow and abide by the company policy. Warning about policy breaches are to be mentioned clearly within the policy statement. Policies clarify responsibility, expectations and acceptable use of company resources. Many companies have policies in place but some top-level management just ignores the policy and policy changes are a boring topic for them in general or board meetings. Now days, companies should develop policies that can take advantage of forensics capabilities and methodologies. Ignoring these will leave a big hole in the security system of the company. If the proper policy is in place then an organization can legally make and store an image of the hard drive of an ex-employee for example. This will enable the company to prove or resolve any acquisitions that the company or the staff might have later after the dismissal. The use of policy not only prevents fraudulent activities, it also saves the company from potential liability. Therefore, to successfully deploy computer forensics methodologies at enterprise level, top to bottom level commitment towards policies and procedures are essential.

FORENSIC AUDITS

This study already has revealed that security audits are not enough to secure the enterprise computing resources and computer evidence if often ignored in security audits. According to Information Systems Audit and Control Association (ISACA), "University studies reveal that more than 90 percent of all information is now created in digital form. Therefore, when company auditors ignore computer evidence, they essentially limit themselves to 10 percent of the available information." Top-level managements need to understand that audit is the process where records are maintained of a particular series of events in order to provide evidence in the case of misconduct/incident. It ensures compliance with certain rules and regulations and checks on the effectiveness of control systems such as policies and procedures. Most of all, audit logs provide evidence in the case of criminal activity. By deploying various security tools and techniques but ignoring, the computer evidences such as audit

logs (Firewall, IDS logs); will not help an organization to completely secure their information system. “Employing preventive measures, such as the use of firewalls and intrusion detection devices to prevent data breaches and thwart external attacks, many organizations around the world have been using computer forensics to identify instances of computer misuse and illegal intrusion. The use of computer forensic techniques also has flourished in the internal audit profession. However, many internal auditors are unaware of the advantages that computer forensics can bring to audit investigations”, says Purita (2006). The development of forensic audits will contribute to effective and efficient incident handling. Due to attitudes within Information Technology (IT) divisions not all organizations have comprehensive audit systems in place. All the above information indicates that forensic audit is very important for an organization regardless of whether the company has forensics capability or not. Firewalls, intrusion detection systems, supported protocols within the internal and external network, antivirus updates, applications/services and patches, software management system, backup processes and procedures, intranet and Internet activity and security all these needs to be audited on regular basis. Forensic audit therefore will enable the enterprise to verify whether the security standards conform to the IT policy and procedures that is in place.

USE OF OPEN SOURCE TOOLS

The use of open source tools is very common among forensics examiners and security experts. There is no reason to believe that open source tools cannot be used for enterprise forensics. People debate about the reliability and accuracy of using open source tools for computer forensics analysis and discovery. Enterprise forensic examiners will eventually come across someone either in the organization or in the court or some outsider, who will challenge the use of open source tools for forensics analysis and discovery. However, because an examiner used open source platform and tools to analyse and discover evidence, does not mean that the result is not reliable and accurate. At the end, it comes down to the methodology and procedure used to carry out the forensics process. Open source tools are just as reliable as other tools and sometimes they offer even more flexibility than other platform tools. They enable forensic examiners to analyse and work on individual layers of a network, which the non-open source tools cannot provide. People forget and do not seem to understand that one of the most important purposes of using computer forensics is to prove that someone is innocent or guilty beyond reasonable doubt and that is the challenge. The debate about using open source tools is just a myth or an area which people comment on without understanding it properly. “Arguably the most important area to cover when presenting evidence to a court is that of continuity. It is absolutely critical to be able to account for what happened to an exhibit such as a computer from the moment it was seized to the moment it was examined by a forensic examiner”, says Kennedy (2006). There should be no doubt that open source tools can be widely used for enterprise computer forensic purposes. In fact, by using open source tools an organization can cut down a significant portion of the enterprise computer forensics and security budget

CONCLUSION

The paper has tried to reveal that having enterprise computer forensics with in-house forensics capability helps in prosecuting and stopping computer crimes. It also helps to protect the integrity and availability of enterprise information system by tracing attacks using forensic auditing. Organizations in the U.S have already realized that they need in-house forensic capability at enterprise level as a form of security measure. However, in Australia, it is still a new concept and it is good to know that some of the companies have already started using enterprise computer forensics as a form of defensive and offensive strategy. The new regime of computer and communication technology has a lot to offer to us in future but the greatest challenge will always be to keep the systems secured. New techniques might be used and currently used forensic techniques and methodologies will evolve in future. But understanding the need for security in the corporate environment will remain the most challenging issue for individual business. Therefore, part of the security strategy needs to be devoted towards enterprise computer forensics. This is a security measure that is fairly sophisticated and there can be issues if the proper tool, techniques and methodologies are not used.

REFERENCES

Arnone, M. (2006) Panel: Cyber crime will grow in 2006, URL http://www.fcw.com/article92085-01-25-06- Web, Accessed 14 Oct 2006

Australian Computer Crime and Security Survey 2006, URL http://www.auscert.org.au/images/ACCSS2006.pdf, Accessed 14 Oct 2006

Barish, S (2002) Windows Forensics: A Case Study (Part 1), URL http://www.securityfocus.com/infocus/1653, Assessed 14 Oct 2006

Barbin C.D and Patzakis J. (2002) Computer forensics emerges as an integral component of an enterprise information assurance program, URL http://www.isaca.org/Content/ContentGroups/Member_Content/Journal1/20023/Computer_Forensics_Emerges_as_an_Integral_Component_of_an_Enterprise_Information_Assurance_Program.htm#f1, Accessed 4 Oct 2006

Dickerman, D. (2005) Enterprise Forensics: Changing the Paradigm, URL http://www.techsec.com/TF-2005-PDF/DanDickerman.pdf, Accessed 14 Oct 2006

Gordon L.A., Loeb M.P., Lucyshyn W. and Richardson R. (2006) CSI/FBI Computer Crime and Security Survey 2006, URL http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf, Accessed 3 Oct 2006

Grimes, R. (2006) Are attackers winning the Security Arms Race, *Information Age*, Dec 2005/Jan 2006.

IC3 2005 Computer Crime Report, *National White Collar Crime Centre and Federal Bureau of Investigation,* URL http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf, Accessed 4 Oct 2006

Jansen W. and Ayers R. (2004) Guidelines on PDA Forensics, URL http://www.securitytechnet.com/resource/crypto/standard/fips/sp800-72.pdf, Assessed 17 Nov 2006

Kennedy, I (2006) Presenting Digital Evidence to Court, URL http://www.bcs.org/server.php?show=ConWebDoc.7372, Accessed 4 Oct 2006

L. Greenemeier, Put up a strong defence, URL http://www.informationweek.com/security/showArticle.jhtml?articleID=177102288, Accessed 14 Oct 2006

Panko, R. R (2004) Corporate computer and network security, *Prentice Hall*, URL http://pankosecurity.com/1SC01_Early10.24.pdf, Accessed 14 Oct 2006

Patzakis, J. (2003) Computer Forensics an Integral component of the Information Security Enterprise, retrieved URL http://www.encase.com/corporate/downloads/whitepapers/computerforensics.pdf, Accessed 15 Sep 2006

Pollitt, M. M. (2001) Report on Digital Evidence, URL http://www.interpol.int/Public/Forensic/IFSS/meeting13/Reviews/Digital.pdf Accessed 15 Sep 2006

Purita, R. (2006) Computer Forensics: A Valuable Audit Tool, *The Institute of Internal Auditors*, URL http://www.theiia.org/itaudit/index.cfm?iid=490&catid=21&aid=2345, Accessed 15 Sep 2006

Reith M., Carr C. and Gunsch G. (2002) An Examination of Digital Forensic Models, URL http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf, Accessed 17 Nov 2006

COPYRIGHT