A Framework for Examining the Human Side of Anti-Forensic Measures

Research-in-Progress

Jason Nikolai
Dakota State University
janikolai@pluto.dsu.edu

Yong Wang
Dakota State University
yong.wang@dsu.edu

Raj Kumar Nepali
Dakota State University
rknepali@pluto.dsu.edu

Abstract

The need for forensic computing and the legitimacy of anti-forensic computing have been examined in literature. However, the majority of existing research in forensic and anti-forensic computer is primarily based around the technology and processes for or against gathering as well as presenting evidence. In this work, we examine the topic through a different lens by exploring the dilemma of why users employ anti-forensic technology in the first place. Our work provides an early conceptual framework based on the theory of reasoned action and the theory of planned behavior to assist researchers and practitioners to understand why computing users employ anti-forensic tools and techniques. If organizations can determine the reasons forensic counter measures are applied, then improved policies and procedures can be put in place to address the computing users' concerns while retaining the ability to enact forensic measures when a violation of policy or illegal activity occurs.

Keywords

Forensic computing, Forensic Countermeasures, Theory of Reasoned Action, Theory of Planned Behavior

Introduction

Computer crime, especially relating to financial institutions, is costly and dangerous (Gottschalk and Solli-Saether 2010). Manipulation of financial markets can significantly impact the operation of societies in negative ways. Furthermore, computer crimes including industrial espionage and cyber terrorism jeopardize citizens, corporations and governments (Grabosky 2007). Computer criminals pose a grave threat to corporate and national security interests. The rapid expansion of computing and the growth of computer crime along with the need for investigation and prosecution has resulted in a relatively new discipline termed computer forensics (Busing et al. 2005).

The need for forensic computing and the legitimacy of anti-forensic computing have been examined in literature. However, the majority of existing research in forensic and anti-forensic computer is primarily based around the technology and processes for or against gathering as well as presenting evidence. In this paper, we examine the topic through a different lens by exploring the dilemma of why users employ anti-forensic technology in the first place. Our work provides a conceptual framework based on the theory of reasoned action and the theory of planned behavior to assist researchers and practitioners to understand why computing users choose to deploy anti-forensic tools and techniques. If organizations can determine the reasons forensic counter measures are applied, then improved policies and procedures can be put in place to address the computing users concerns while retaining the ability to enact forensic measures when a violation of policy or illegal activity occurs.

Our paper is organized as follows. First, an overview of forensic and counter forensics is presented. Second, the theoretical foundation for our conceptual model is examined. Third, the methodology for our

work is provided. Fourth, our anti-forensic conceptual framework is posited. Last, our paper concludes with a discussion of our research in progress and limitations of our work.

Overview of Forensic and Counter Forensic Computing

Computer Forensics

The field of computer forensics originated from the discipline of forensic medicine. Similar to forensic medicine, computer forensics utilizes postmortem techniques to establish evidence of a crime or breach of policy (Berghel 2003). Some have called computer forensics a "modern crime fighting tool (Busing et al. 2005)." Computer forensics provides formal techniques for collecting, analyzing, as well as presenting evidence gathered from computer systems in a court of law. This field is concerned with the rules of evidence, legal processes, and expert testimony (Behr 2008). Furthermore, it involves the preservation, identification, extraction, documentation, and interpretation of data from computing systems (Busing et al. 2005; Crowley 1997). The aim of computer forensic investigators is to find "the truth" and not establish a bias around guilt or innocence of an individual under investigation (Wolfe 2003).

Unfortunately, a lack of computer forensic skills exists in law enforcement (Bhaskar 2006; Lane 2011). Some police organizations have employed technical savvy computer experts to assist with forensic investigation and computer crime (Harrison et al. 2004). However, this model does not scale well. There are many law enforcement agencies in most communities, but it is not likely that there will be computer security and forensic experts in the same locales. Therefore, in order to prevent and catch computer criminals will require new methods, training, and tools for conducting computer forensic investigations (Casey 2006; Collier and Spaul 1990).

An important subject for computer forensic investigation is incident response management. Incident response management and proper training can help once a security or policy breach has occurred. Best practices and techniques have been proposed (Mitropoulos et al. 2006). In addition, the suggestion of going beyond simply using technology to conduct forensic investigation and using criminal profiling techniques has been posited. This technique requires investigators to use both inductive and deductive profiling. Inductive profiling examines personality traits of potential offenders in a general population. Deductive profiling looks at the case and the evidence to construct a behavioral profile for that particular case (Rogers and Seigfried 2004).

Forensic computing can be divided into a taxonomy of five categories: computer science, law, information systems, social sciences and other. Computer science aims to research computer security, operating systems and application software, as well as systems programming and computer languages. Law approaches the topic from the various legal and law enforcement perspectives including criminal, civil, and soft law. Information systems involve system management, organizational policies, and user education. Social sciences are interested in socio-political issues especially those related to privacy and encryption, surveillance, activism and hacktivism as well as issues around cyber terrorism. Finally, other issues in forensic computing include topics such as documentation skills, forensic skills of investigators, and authenticating evidence (Broucek and Turner 2002). The goals of computer forensics include: identifying, preserving, and presenting legally acceptable evidence; recovering evidence free from alteration; and the reconstruction of events of an unauthorized or criminal activity (Broucek and Turner 2006).

Anti-Forensic Computing

The opposite of forensic computing is anti-forensic computing. Harris (2006) defines anti-forensic computing as "any attempt to compromise the availability or usefulness of evidence to the forensics process." More generally, anti-forensic computing is a term to describe tools and techniques intended to change data in order to contaminate the reliability of digital forensic data making it essentially inadmissible in a court of law.

Anti-forensics can be segmented into four parts: evidence destruction, evidence hiding, evidence source avoidance, and evidence counterfeiting. First, evidence destruction involves the deletion of files and evidence. While this may appear trivial on the surface, it is a rather complex problem as traces of data remain on systems when common deletion techniques are used. Second, evidence hiding is a technique to

retain data but restrict others from viewing it. Third, evidence source avoidance consists of techniques to hide the fact that anti-forensic techniques were employed to hide or remove evidence. Fourth, evidence counterfeiting occurs when data is created to make false representation such as modifying a time stamp (Behr 2008). Anti-forensic computing is more than simply tools. Rather, it is a combination of approaches and tactics to obstruct computer forensic investigation (Dahbur and Mohammad 2011).

Anti-Forensic Tools and Techniques

Anti-forensic tools are becoming widely available to general computer users (Behr 2008; Dahbur and Mohammad 2011; Martin and Jones 2011). Generally, anti-forensic tools aim to avoid detection of a specific event, disrupt the collection of information, increase the time required by investigators to examine data, and cast doubt on forensic data in a court of law. Furthermore, anti-forensic tools may attempt to discover forensic tools, attack forensic investigators, or remove all evidence of the existence of the anti-forensic tool itself (Garfinkel 2007). A multitude of tools exist for completely wiping data from systems that can make forensic analysis practically, if not completely, impossible (Berghel and Hoelzer 2006). Furthermore, data hiding techniques have been commonly used since the 1970s, or even earlier (Berghel 2007).

Approaches to counter anti-forensic measures have been proposed and implemented. For example, computer forensics using live methods has been proposed (Adelstein 2006). However, even these techniques can be impeded by anti-forensic tools and measures introduced by computer users. Forensic investigators commonly depend on the use of tools to gather evidence and conduct the investigation. The use of a combination of tools can help overcome attacks against specific tools. Unfortunately, even the use of multiple tools may come under attack and forensic toolkits can be expensive (Harris 2006). In addition, technical techniques for countering anti-forensic tools as well as storing forensic data have been proposed (Garfinkel 2007; Garfinkel 2006; Hosmer 2006; Johansson 2002; Peron and Legary 2005). Calls for more advanced technologies and techniques have been made by researchers (Caloyannides 2009; Golden and Roussev 2006). However, the war between computer forensic tools and techniques and counter techniques continues to rage on. Digital technology is constantly changing and forensic techniques will need to adapt in order to keep up (Mercuri 2005). As processors get faster, more individuals gain access to networks, and storage devices continue to rapidly increase in size, forensic tools will need to quickly adapt.

Forensic Countermeasure Dilemma

On the surface, one may assume that the forensic investigators are the "good guys" and the computer users deploying anti-forensic tools and measures are "bad guys" or "black hats." Some have suggested that the use of anti-forensic tools, such as encryption, raises suspicion of the computer users applying that technology. However, this type of thought raises a much larger question about human rights and privacy (Broucek and Turner 2006). Many developers of anti-forensic tools and techniques claim that they are not trying to thwart forensic investigations. Rather, they are working to improve the justice system by revealing weaknesses in computer forensics (Behr 2008). In addition, the expectation of privacy is a legitimate reason for applying anti-forensic tools and measures on computer systems (Afanasyev et al. 2011). Some argue that computer users within corporations should be concerned about the right to privacy. This may be reinforced through comments made by executive officers that suggest employees have no right to privacy (Caloyannides 2009). This suggestion is concerning to many computer users. The right to privacy and workplace surveillance plague the computer forensics discipline. Legislation in many countries has been proposed but has not been thoroughly tested in courts around the world (Brungs and Jamieson 2005). Legislation such as the USA Patriot Act has given authorities power to conduct computer forensic investigations. In some cases, these new powers do not require a warrant from a court of law (Busing et al. 2005).

With all the investigative powers of corporations and governments, some argue that computer users should be concerned about privacy. Judges and juries typically lack a technical understanding of evidence and many lawyers have not studied computer forensics while in law school. They may not be able to provide an adequate defense against poor forensic evidence or improper evidence collection. Simply because a computer user has not committed a crime or used a computer illegitimately does not protect them from prosecution or legal action. In some cases, a computer user may be working on a computer

which is performing activities that the user is unaware of. Criminals can take control of computers remotely and cause then to perform unauthorized activities.

Computer forensics has at least two significant limitations. First, it cannot determine who put the evidence on the machine in the first place. And, second, computer forensics is unable to find evidence that does not exist. A plethora of techniques exist that allow computer users to use a computing device and never leave evidence behind, such as using portable storage (Caloyannides 2009).

Computing users may want to prevent data theft and protect legitimate secrets that do not violate laws or policies. A number of counter forensic measures can be applied to protect a computer user's privacy including data hiding, disk wiping, steganography, and degaussing (Caloyannides 2009; Garfinkel 2007). Techniques such as disk wiping and encryption have valuable purposes in legitimate computing. In a study, 55 hard disks that were discarded were analyzed and held approximately 300,000 files which contained identifiable information (Medlin and Cazier 2011). If proper anti-forensic techniques were applied, this data would not have remained on the storage which could be used for unlawful activities.

Theoretical Foundation

Our proposed framework is based on the theory of reasoned action and the theory of planned behavior. The theory of reasoned action suggests that the behavior of individuals is driven by intentions where the intentions are a function of attitude toward the behavior and subjective norms that surround the performance of the behavior. The attitude toward the behavior is explained by the positive or negative feeling that an individual has about performing a particular behavior. Subjective norm can be explained as how people around the individual that are considered important to the individual are perceived to view the behavior (Eagly and Chaiken 1993).

The theory of reasoned action does not account for the individual's capability to perform an action. In many cases, individuals are constrained by ability, time, environment or organizational limits which impede the execution of the behavior. To address the limitations, the theory of planned behavior extends the theory of reasoned action by incorporating the construct of perceived behavioral control (Ajzen 1991). The theory of reasoned action was developed to predict and explain human social behavior. The conceptual model of the theory of planned behavior is shown in Figure 1.

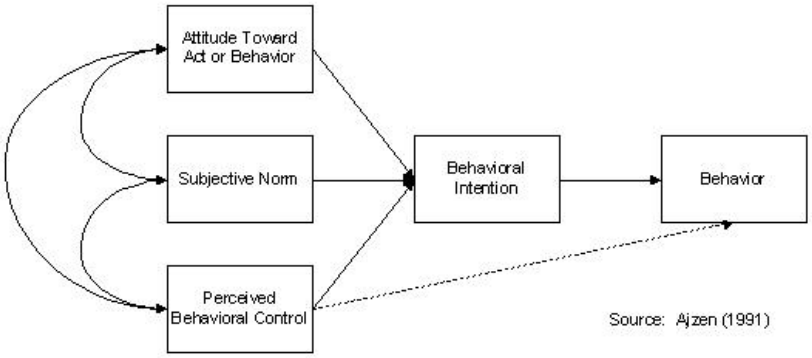

Figure 1. Theory of Planned Behavior

The theory of planned behavior consists of five constructs: attitude toward act or behavior, subjective norm, perceived behavior control, behavioral intention, and behavior (Ajzen 2006). Behavioral belief, which is the biased probability that a particular behavior will result in a given outcome, influences the attitude toward an act or behavior. Similar to the theory of reasoned action, the attitude toward an act or behavior is the degree where enactment of a behavior is positively or negatively valued. To calculate the attitude toward the act or behavior, a strength value for each belief is multiplied by an evaluation weight and summed.

Subjective norm is influenced by normative beliefs. Here, normative beliefs can be defined as the perceived behavioral expectations of individuals or groups that are important to the individual. The

subjective norm is determined by the apparent social pressure to engage or not engage in a particular behavior. The subjective norm is calculated by a summation of the product of the strength of each normative belief and a weighted factor for the motivation to comply with the referent in question.

The perceived behavior control is influenced by control beliefs, and is similar to self-efficacy. Control beliefs can be described as the observed presence of elements that either facilitate or impede the performance of a particular behavior. Perceived behavior control is the individual's perception of ability to perform a particular behavior. The combination of perceived behavior control and behavior intention can be used to predict actual behavior. Furthermore, actual behavior control, which is the capability of the individual to perform a particular behavior, plays a role in predicting actual behavior. To calculate the perceived behavior control, the products of the strength of each control belief and perceived power are aggregated.

Behavioral intention is an indicator for the individual's willingness to carry out a particular behavior. This is considered to be an immediate precursor to conducting a behavior. The behavior intention is influenced by the attitude toward the act or behavior, subjective norm, and the perceived behavioral control as well as the actual behavior control. Behavior is the apparent response in a particular situation with reverence toward a given target.

Methodology

Our work aims to establish a conceptual framework to understand why computer users who adhere to policies, procedures, and laws introduce forensic countermeasures into their environment. To derive our framework, we performed a literature review using ABI Inform, ACM Digital Library, Google Scholar, and the Google Search engine. We felt this would give us both the researcher and practitioner prospective. The search terms used were "computer forensics" and "computer anti-forensics." Several hundred results were returned. Initially, the abstracts were reviewed for relevance. Papers that discussed issues around forensic computer and anti-forensic computing where reviewed. A total of 43 references were reviewed in detail from a wide variety of sources. At the point when no new discovery of information was made, the literature review was concluded. A summary of the literature review is presented in table 1, below.

Reference Type	Forensic Computing Only	Anti-Forensic Computing Only	Forensic and Anti-Forensic Computing	Totals
Law Enforcement and Legal focus	10	1	0	11 (~25.6%)
Management and IS focus	8	0	0	8 (~18.6%)
Technical focus	9	12	3	24 (~55.8%)
	27	13	3	43

Table 1. Summary of Literature Review

From Table one, one can observe that the reviewed references are broken into three categories: legal focus, management and IS focus, and technical focus. Legal focus consists of the references that mainly discussed legal issues relating to forensic and anti-forensic computing. These references examine the legality of forensic data collection, forensic countermeasures, and various law enforcement topics. Management and IS focus can be described as the focus around policies and procedures as well as management issues. And, technical focus includes references that examine the technical nature of forensic and anti-forensic computing. References in this category examine tools, techniques, and designs relating to forensic and anti-forensic computing. In addition, three primary topics for the references are summarized. The primary topics consist of forensic computing, anti-forensic computing, and forensic and

anti-forensic computing. While many references had some overlap, a subjective categorization was made to put each reference in one of the categories based on the primary focus of the reference.

Table one provides data indicating that over half of the references discovered in this literature review had a technical focus, a quarter had a legal focus, and a little over 18 percent had a management and information system focus. This suggests a gap in research and not surprisingly, there appears to be a stronger focus on technology and tools and not a large amount of research in the human factors around forensic and anti-forensic computing.

Anti-Forensic Conceptual Framework

Much research has been conducted around the technologies used in forensic and anti-forensic computing. However, it is unlikely that forensic investigators will ever be able to completely counter the anti-forensic measures deployed by computer users. Understanding why computer users deploy anti-forensic measures may help organizations and law enforcement officials shape policies and procedures that reduce the increased usage of such tools by legitimate users. The intent of our paper is not to suggest that the use of anti-forensic measures is always "bad" or "wrong." Certainly, there are legal and legitimate uses for such measures. Our work aims to provide a conceptual framework to understand why legitimate computer users within organizations deploy anti-forensic measures.

The conceptual framework is adapted from the theory of planned behavior (Ajzen 1991) with the purpose to explain why computer users deploy anti-forensic measures on computing devices within an organization. The model is deduced from literature and attempts to explain three constructs that determine whether or not a user will deploy anti-forensic tools. First, it is deduced from literature that some computer users are concerned about the privacy of data (Afanasyev et al. 2011; Brungs and Jamieson 2005; Busing et al. 2005; Caloyannides 2009). Certainly in recent years, legislation has changed and the general public has become more aware of new legislation, such as the USA Patriot Act, which provides government officials with the ability to obtain evidence without a warrant. Second, this paper suggests that organizations without clear policies and procedures around which tools can be deployed on user workstations do not discourage the use of these tools. And, third, anti-forensic tools have become more common place and available to end users. Many are easy to use and can be downloaded at no charge (Caloyannides 2009; Garfinkel 2007; Johansson 2002; Peron and Legary 2005). Our proposed conceptual model is presented in Figure 2.

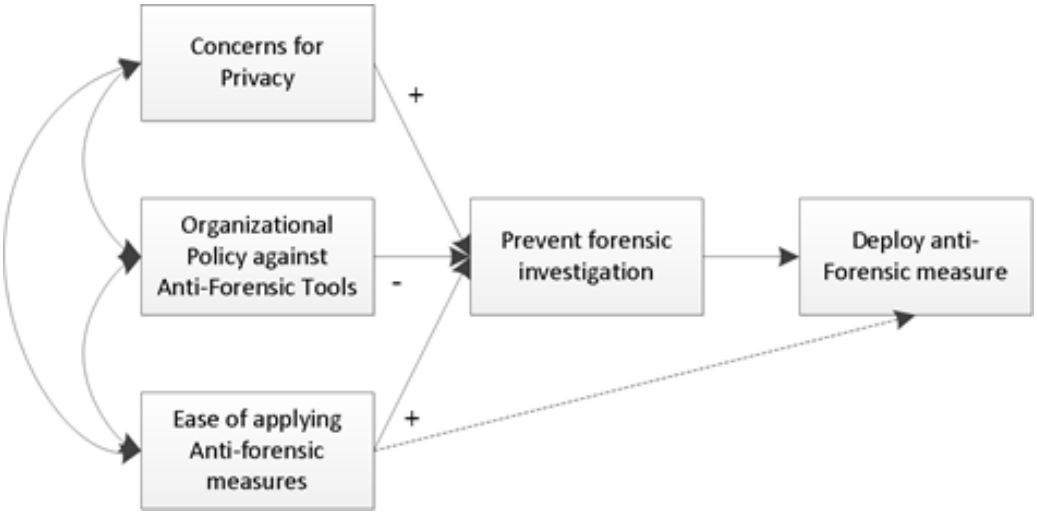

Figure 2. Anti-forensic Measures Conceptual Model

From Figure Two, one can observe five constructs that map to the theory of planned behavior. First, concerns for privacy maps to attitude toward act or behavior. The reasoning is that a computer user's personal attitude toward privacy will play a role in whether a forensic counter measure will be deployed. Second, organizational policy against anti-forensic tools maps to subjective norm. Here, the thought is that if the organization does not have clear policies and procedures around anti-forensic tools and techniques on user workstations, social pressure to not deploy these tools or techniques is not present. Third, the ease of applying anti-forensic measures aligns with perceived behavioral control, and actual behavior control. If anti-forensic tools and techniques are easy to implement and deploy, it is reasonable to suggest that more users will have the capability to enact such mechanisms. Prevent forensic investigation maps to behavioral intention in the theory of planned behavior. This is the precursor to deploying the anti-forensic tools and techniques. And, finally, deploy anti-forensic measures maps to the user performing the actual behavior.

This paper posits three propositions around the constructs: concern for privacy, organizational policy against anti-forensic tools, and ease of applying anti-forensic measure.

Concern for Privacy

Based on the literature review, it is clear that some computer users within corporations are concerned about the right to privacy. As previously mentioned, some executive officers has suggested that employees do not have a right to privacy (Caloyannides 2009). In addition, legislation around the right to privacy in the workplace have been proposed in many countries but has not been vetted in courts around the world (Brungs and Jamieson 2005). Furthermore, legislation such as the USA Patriot Act has given authorities power to conduct computer forensic investigations. In some cases, these new powers do not require a warrant from a court of law (Busing et al. 2005). It is reasonable to theorize that privacy is a concern for some individuals in organizations. Therefore, it is proposed that:

Proposition1 (P1): *The computing users concern for privacy is positively associated with the deployment of anti-forensic methods and tools.*

Organizational Policy against Anti-Forensic Tools

The theory of planned behavior states that subject norm is influenced by normative beliefs. And, normative beliefs can be defined as the perceived behavioral expectations of individuals or groups that are important to the individual. The subjective norm is determined by the apparent social pressure to engage or not engage in a particular behavior (Ajzen 1991; Ajzen 2006). Applying the theory of planned behavior to an organization where anti-forensic mechanisms may be deployed, this work suggests that when an organization does not have clear policies and procedures in place to influence the user communities normative beliefs, essentially a subjective norm that discourages anti-forensic tool deployment does not exist. Here, if an organization had policies and procedures around whether anti-forensic tools can be installed on workstations, social pressure from the organization, which is presumed to be a group that is important to the individual, would shape the subjective norm against applying such mechanisms. Therefore, it is proposed that:

Proposition2 (P2): *A clearly communicated policy within an organization stating that anti-forensic tools are not permitted is negatively associated with the deployment of anti-forensic tools on computing users' machines.*

Ease of applying anti-forensic measures

Perceived behavioral control in the theory of planned behavior helps to predict whether an individual will perform an action based upon whether that individual perceives to have the capability to perform that action. In addition, actual behavior control plays a part in whether the action is performed (Ajzen 2006). In the proposed conceptual framework, it is theorized that the ease of applying anti-forensic measures enables perceived behavior control. In recent years, a number of anti-forensic tools have become available and can be downloaded and installed at no charge. These tools allow users to easily wipe data from systems so that forensic investigators cannot recover information and hide or encrypt data which makes it difficult or impossible to recover (Caloyannides 2009; Garfinkel 2007; Johansson 2002; Peron

and Legary 2005). Given that these tools have become widely available and many are much easier to use than the tools and techniques of anti-forensics in years past, it is proposed that:

Proposition3 (P3): *The easier anti-forensic methods and tools are to deploy is positively associated with the deployment of anti-forensic methods and tools.*

Discussion and Conclusion

Our paper has described the problem of computer crime and the importance of investigating illegal and illegitimate activities conducted on computing systems. Furthermore, two concepts in computer crime investigation where discussed: forensics and counter forensics. Computer forensics provides formal techniques for collecting, analyzing, as well as presenting evidence gathered from computer systems in a court of law. This field is concerned with the rules of evidence, legal processes, and expert testimony (Behr 2008). On the other hand, anti-forensics is a term used to describe tools and techniques intended to change data in order to contaminate the reliability of digital forensic data making it essentially inadmissible in a court of law. Not all anti-forensic application involves illicit or illegal activities. The expectation of privacy is a legitimate reason for applying anti-forensic tools and measures on computer systems (Afanasyev et al. 2011).

Our work set out to examine why legitimate users incorporate the use of anti-forensic techniques and tools in their computing environment by proposing a theoretical model based on the Theory of Planned Behavior. If practitioners can understand why these approaches are deployed, they can potentially create as well as adjust policies and procedures to meet the concerns of the user community while maintaining the forensic capabilities needed to investigate legitimate policy violations and crimes. The model put forth in our paper has implications to both practitioners and scholars. The constant struggle between forensic computing and anti-forensic computing currently has no pragmatic solution. As new forensic techniques are developed, counter forensic methods are deployed. Furthermore, technology is constantly evolving making forensic computing a never ending progressive discipline. In order for forensic investigators to win this ongoing battle, the human factors of anti-forensic computing must be understood.

Certainly, getting legitimate users to stop thwarting forensic investigation will not solve the greater problem of computer crime and forensic countermeasures. However, if organizations can instantiate, communicate, and obtain buy-in for proper policies that result in which only a user community which has something to hide applying anti-forensic tools and methods, it will be easier to profile criminals and those who are breaching corporate policies using computers. With that said, this approach should be used with caution as it is unlikely every user will buy in to such a policy.

Limitations

In this paper, we have put forth three propositions have been derived from the Theory of Planned Behavior. First, a computing users concern for privacy is positively associated with the deployment of anti-forensic methods and tools. Second, a clearly communicated policy within an organization stating that anti-forensic tools are not permitted is negatively associated with the deployment of anti-forensic tools on computing users' machines. And, third, the easier anti-forensic methods and tools are to deploy is positively associated with the deployment of anti-forensic methods and tools.

The model is limited because it only explores a single attitude, privacy, and a single norm, organizational policy. As we expand our model, we will examine other relevant human elements discussed in the literature such as personality, neural correlates and non-technical deterrence. In addition, the model, after completed, will need validation using techniques presented by Ajzen.

REFERENCES

Adelstein, F. 2006. "Live Forensics," *Association for Computing Machinery. Communications of the ACM* (49:2), pp. 63-63.

Afanasyev, M., Kohno, T., Ma, J., Murphy, N., Savage, S., Snoeren, A.C., and Voelker, G.M. 2011. "Privacy-Preserving Network Forensics," *Association for Computing Machinery. Communications of the ACM* (54:5), p. 78.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational behavior and human decision processes* (50:2), pp. 179-211.

Ajzen, I. 2006. "Tpb Diagram." Retrieved April 14, 2012, from http://people.umass.edu/aizen/tpb.diag.html#null-link

Behr, D.J. 2008. "Anti-Forensics: What It Is, What It Does and Why You Need to Know," *New Jersey Lawyer Magazine* (December 2008:255), p. 4.

Berghel, H. 2003. "The Discipline of Internet Forensics," *Association for Computing Machinery. Communications of the ACM* (46:8), pp. 15-20.

Berghel, H. 2007. "Hiding Data, Forensics, and Anti-Forensics," *Association for Computing Machinery. Communications of the ACM* (50:4), pp. 15-20.

Berghel, H., and Hoelzer, D. 2006. "Disk Wiping by Any Other Name," *Association for Computing Machinery. Communications of the ACM* (49:8), pp. 17-21.

Bhaskar, R. 2006. "State and Local Law Enforcement Is Not Ready for a Cyber Katrina," *Association for Computing Machinery. Communications of the ACM* (49:2), pp. 81-81.

Broucek, V., and Turner, P. 2002. "Bridging the Divide: Rising Awareness of Forensic Issues Amongst Systems Administrators."

Broucek, V., and Turner, P. 2006. "Winning the Battles, Losing the War? Rethinking Methodology for Forensic Computing Research," *Journal in Computer Virology* (2:1), pp. 3-12.

Brungs, A., and Jamieson, R. 2005. "Identification of Legal Issues for Computer Forensics," *Information Systems Management* (22:2), pp. 57-66.

Busing, M.E., Null, J.D., and Forcht, K.A. 2005. "Computer Forensics: The Modern Crime Fighting Tool," *The Journal of Computer Information Systems* (46:2), pp. 115-119.

Caloyannides, M.A. 2009. "Forensics Is So Yesterday," *Security & Privacy, IEEE* (7:2), pp. 18-25.

Casey, E. 2006. "Investigating Sophisticated Security Breaches," *Association for Computing Machinery. Communications of the ACM* (49:2), pp. 48-48.

Collier, P.A., and Spaul, B.J. 1990. "Information Systems Forensics," *Journal of Information Technology* (5:3), pp. 134-140.

Crowley, W.T. 1997. ""Forensic" Computer Information for Those Engaged in the Preservation of Data and Recovery of Assets," *Journal of Security Administration* (20:2), pp. 47-59.

Dahbur, K., and Mohammad, B. 2011. "The Anti-Forensics Challenge," ACM, p. 14.

Eagly, A.H., and Chaiken, S. 1993. *The Psychology of Attitudes*. Harcourt Brace Jovanovich College Publishers.

Garfinkel, S. 2007. "Anti-Forensics: Techniques, Detection and Countermeasures," p. 77.

Garfinkel, S.L. 2006. "Aff: A New Format for Storing Hard Drive Images," *Association for Computing Machinery. Communications of the ACM* (49:2), pp. 85-85.

Golden, G.R., III, and Roussev, V. 2006. "Next-Generation Digital Forensics," *Association for Computing Machinery. Communications of the ACM* (49:2), pp. 76-76.

Gottschalk, P., and Solli-Saether, H. 2010. "Computer Information Systems in Financial Crime Investigations," *The Journal of Computer Information Systems* (50:3), pp. 41-49.

Grabosky, P. 2007. "Requirements of Prosecution Services to Deal with Cyber Crime," *Crime, Law and Social Change* (47:4-5), pp. 201-223.

Harris, R. 2006. "Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the Anti-Forensics Problem," *Digital Investigation* (3), pp. 44-49.

Harrison, W., Heuston, G., Mocas, S., Morrissey, M., and Richardson, J. 2004. "High-Tech Forensics," *Association for Computing Machinery. Communications of the ACM* (47:7), pp. 49-52.

Hosmer, C. 2006. "Digital Evidence Bag," *Association for Computing Machinery. Communications of the ACM* (49:2), pp. 69-69.

Johansson, C. 2002. "Forensic and Anti-Forensic Computing."

Lane, S.W. 2011. "Are Local Authority Fraud Teams Fit for Purpose?," *Journal of Financial Crime* (18:2), pp. 195-213.

Martin, T., and Jones, A. 2011. "An Evaulation of Data Erasing Tools," *The proceeding of the 9th Australian Digital Forensics Conference*, p. 84.

Medlin, B.D., and Cazier, J.A. 2011. "A Study of Hard Drive Forensics on Consumers' Pcs: Data Recovery and Exploitation," *Journal of Management Policy and Practice* (12:1), pp. 27-35.

Mercuri, R. 2005. "Challenges in Forensic Computing," *Association for Computing Machinery. Communications of the ACM* (48:12), pp. 17-21.

Mitropoulos, S., Patsos, D., and Douligeris, C. 2006. "On Incident Handling and Response: A State-of-the-Art Approach," *Computers & Security* (25:5), pp. 351-351.

Peron, C.S.J., and Legary, M. 2005. "Digital Anti-Forensics: Emerging Trends in Data Transformation Techniques," *Proceedings of 2005 E-Crime and Computer Evidence*

Rogers, M.K., and Seigfried, K. 2004. "The Future of Computer Forensics: A Needs Analysis Survey," *Computers & Security* (23:1), pp. 12-16.

Wolfe, D.H.B. 2003. "Computer Forensics," *Computers & Security* (22:1), pp. 26-28.