Journal of International Technology and Information Management

Volume 16 | Issue 2 Article 1

2007

Improving the Judicial System to Handle Computer Crime

Gerald V. Post
University of the Pacific

Albert Kagan
Arizona State University

Improving the Judicial System to Handle Computer Crime

Gerald V. Post
University of the Pacific

Albert Kagan
Arizona State University

ABSTRACT

This paper asked professionals in the legal system to evaluate the current state and effectiveness of laws to identify and deter computer crime. Responses were evaluated with a formal structural equation model. The results generally show that legal professionals believe potential jurors have minimal knowledge of computer crime issues. More importantly, they also believe that judges have little knowledge or experience. A similar lack of knowledge by defense attorneys indicates that it could be difficult for a person accused of computer related infractions to find adequate representation. On the other hand, more experienced participants do not believe computer laws present an effective deterrent to computer crime. The bottom line is that all levels of the legal profession will need more education and training in aspects of computer security laws.

INTRODUCTION

Computer security topics within the literature have traditionally focused on technical issues, see Bidgoli (2003) and Opara and Marchewka (2006). These issues are important and relatively complex. However, computer usage and security exist within a society, where the framework is defined by laws and the judicial system. Ultimately, computer security requires both technical and legal solutions. The oft-criticized Digital Millennium Copyright Act (DMCA) presents a classic case. Prior to its enactment, copyright law made it illegal to steal satellite shows and other content. Broadcasters used encryption and other technical methods to protect the content from casual theft. However, it was legal for people to sell technology that could decrypt the signals. Possession and sale of this technology could not be stopped, and it was difficult and expensive to detect and enforce copyright laws on a person-by-person basis. Implementation of the DMCA makes it easier to curtail the distribution of the tools used to steal the satellite signals. Whether DMCA goes too far or has undesirable consequences is not the point here. The case highlights the importance of the judicial system in providing a remedy with respect to technology issues.

The judicial system encompasses three main aspects: (1) Creation of laws, (2) Investigation of potential crimes, and (3) a trial phase which involves prosecutors, defense attorneys, judges, and sometimes jurors. A broader definition would also include punishment issues, involving prison sentences and fines, but these issues remain constant regardless of the type of law or crime, and these concerns have been covered extensively in other literature. Civil complaints and trials can also become important tools in dealing with computer security topics, but many of the circumstances will be similar to criminal cases, although the various roles will be handled by different organizations. A primary question posed here is whether the current U.S. judicial system needs to be improved to be able to handle computer security cases. In particular, the federal government has passed several new laws in the past few years that relate to computer and technology issues. However, are the supporting parts of the judicial system able to handle these new laws? What changes or support might need to be added? To begin to address these questions, a survey of legal professionals was undertaken to evaluate current conditions and highlight aspects of the judicial process that need to be improved. The simple answer to the main question is that most participants do not feel the system is prepared to handle complex technical cases. The most pressing need is for education and training of the various levels of judicial participants. The degree of shortfall and the details are explored in this paper.

RELEVANT LITERATURE

The literature on computer security and crime is increasingly diverse, and there is not sufficient space to summarize all of it here. As E-commerce applications continues to expand the online business model, firms are attempting to determine fair information usage practices and the legal dynamics as part of an overall policy, as explained by Ryker, Khurrum and Bhutta (2006). Prior research has attempted to characterize the diverse nature of computer crime and judicial involvement.

Dowland et al (1999) found that the public in the UK was aware that computer crime and security are concerns in the general case but they lack knowledge as to how the two most prominent laws available at that time were effective in deterring computer crime. In fact many respondents were unfamiliar with the concept of computer crime and effective legislation.

Carr and Willams (2000) compare the implementation of computer crime laws in the UK, Malaysia and Singapore to gauge the effectiveness as deterrents. The conclusion is that these laws have not led to any large amount of prosecutions due to a series of factors. The factors localize themselves into a lack of firm level participation in the investigation and reporting process, an absence of sufficient training by members of the legal establishment and that the basis of the legislation centers upon economic positioning (punishment) as opposed to security deterrence.

In a response to the increase in computer related security and crime occurrences, the Hong Kong government has passed a series of legislative acts to address this problem. Kennedy (2001) reports on the actions of the Inter-departmental Working Group on Computer Related Crime in strengthening existing legislation to more effectively to deter computer security outbreaks in Hong Kong.

Caelli (2002) argues that the original design of the personal computer fostered a culture of non security, in that systems were designed with minimal security controls. As the use of the PC and distributed systems increased, the need for governmental intervention as a catalyst for protection was necessitated. Government involvement in the contemporary information environment should be twofold. The first level supports the idea that government must structure acceptable legislative actions to address the validity of electronic transactions and enforce a floor level of minimum security standards. Caelli's second view of legislation is for the government to define a set of "professional qualifications as well as a process to support accreditation of information security professionals." In other words determine educational and regulatory standards for security practitioners.

Walden (2004) presents the case that countries need to structure laws to combat computer security crimes given the complex nature of the infractions and the cross jurisdictional entanglements these cases contain. With many computer crimes occurring in country A while the perpetrators may be in country B, the rules of evidence, legal procedures and investigative prerogatives all vary. This causes the system of legislation to be less than effective as a deterrent. Walden suggests a set of legislation modeled upon the UK's Computer Misuse Act of 1990.

Gerard, Hillison and Pacini (2004) discuss how the US government has made a pronounced effort to gain the upper hand on identity theft issues. Various laws have been enacted to help alleviate the problem. A similar approach would be required to handle the issue of computer security with one important caveat—business organizations must ramp up their awareness and internal controls with respect to security. The business controls will augment the role of the legal system in addressing computer security concerns.

As the broad and pervasive nature of computer crime and security threats continues to increase, the judicial system must respond through the effective design and implementation of legislation. The following section provides a brief discussion concerning computer laws.

COMPUTER LAWS

Increasingly, society is turning to the legal system to support computer security goals. The approach in the legal system has been fractured—particularly after Easterbrook's speech (1996). Easterbrook argued that just as there was no need for a "Law of the Horse," there is little need for "cyberlaw." The underlying principles of law should be

applied to situations regardless of whether the computer is involved. Other writers, such as Lessig (1999) have argued that cyberspace contains unique features that require new laws. The various arguments are interesting but the details are beyond the scope of this paper. In any case, cyberspace at a minimum requires new definitions to clarify objects and actions. For example, is a cached copy of an electronic item a violation of copyright laws? Consequently, as noted by several authors such as Lampson (2002) and Landwehr (2001), Congress has passed several laws to prohibit various actions with respect to computers.

Table 1 lists the primary sections of the U.S. Code that are used in the federal prosecution of computer crimes. This list is provided by the Department of Justice. The most important set of computer laws is embodied in 18 USC 1030, which was largely created by the Computer Fraud and Abuse Act of 1984 and modified several times. This section defines and outlaws most attacks on computers. Crimes charged under these sections represent the purest form of computer fraud.

Table 1: Computer Crime Regulations in the United States Code.

US Code	**Law**
18 USC 1028	Identity Theft and Assumption Deterrence Act of 1998
18 USC 1029	Fraud and Related Activity in Connection with Access Devices
18 USC 1030 ***	Computer Fraud and Abuse Act of 1984 (and others)
18 USC 1362	Communication Lines, Stations, or Systems
18 USC 2510	Wire and Electronic Communications Interception
18 USC 2701	Stored Wire and Electronic Communications and Transactional Records Access
18 USC 3121	Recording of Dialing, Routing, Address, and Signaling Information
18 USC 1341	Frauds and swindles
18 USC 1343	Fraud by wire, radio, or television
18 USC 2512	Manufacture, distribution, possession, advertising of interception devices prohibited
	Cyber stalking
18 USC 875	Interstate communications
18 USC 2261A	Interstate stalking
47 USC 223	Obscene or harassing phone calls
	Copyright
17 USC 506	Criminal Offenses/Copyright
18 USC 2319	Criminal Infringement of a Copyright
18 USC 2318	Trafficking in counterfeit labels
17 USC 1201	Circumvention of copyright protection schemes
17 USC 1202	Integrity of copyright management information

Primary source is U.S.Department of Justice: http://www.usdoj.gov/criminal/cybercrime/fedcode.htm

Several other sections of the Code are sometimes applied in technology-related crimes. For instance, 18 USC 1028 makes identity theft illegal, but it also applies to the manufacture, use, and sale of physical identities; such as forging driver's licenses. Similarly, crimes related to "access devices' (largely telephones), are defined in 18 USC 1029. Again, this section is also used to prosecute crimes that never involved the computer, such as fraud committed using phone calls. Likewise, several other sections concern issues involving communication systems, such as 18 USC 3121 and 18 USC 2512 that address the recording and interception of phone calls and other communications. As shown in the table, three sections of the code address cyber stalking and harassment involving computers or interstate phone calls. Finally, 17 USC 506 and related sections encompass criminal activities involving copyrights. In particular, the DMCA makes it a crime to circumvent copy protection devices.

Table 2 shows some of the major laws that were passed to create and modify the various codes. This table also includes some of the privacy laws, which are not listed in Table 1. The main purpose of Table 2 is to draw attention to increasing activity in recent years with respect to technology and computer related legislation. Additionally, if you even casually follow the Congressional discussions, it is clear that computer crime and associated privacy

concerns are important ongoing topics. Many bills are introduced each year regarding various computer aspects (such as access, use, theft, fraud) even though few have become laws.

Table 2: Primary Federal Computer and Privacy Acts.

Year	US Code	Act
1970	15 §1681	Fair Credit Reporting Act
1974	20 §1232g	Family Educational Rights and Privacy Act
1974	5 §552a	Privacy Act
1984	18 §1029-2030	Computer Fraud and Abuse Act
1986	18 §2510	Electronic Communications Privacy Act
1987	15 §271-278 40 §759	Computer Security Act (federal computers)
1988	18 §2701	Video Privacy Act (Bork Bill)
1994	18 §2721	Driver's Privacy Protection Act
1994	47 §1001	Communications Assistance for Law Enforcement Act
1996	42 §201	Health Insurance Portability and Accountability Act
1998	15 §6501	Children's Online Privacy Protection Act
1998	17 §1201	Digital Millennium Copyright Act (non-circumvention)
1998	18 §1028	Identity Theft and Assumption Deterrence Act
1999	15 §6801-6810 15 §6821-6827	Graham-Leach-Bliley Act (privacy and fraudulent access to financial information)
2001	18 §1	USA Patriot Act
2002	18 §1030	Cyber Security Enhancements Act (Homeland Security)
2003	15 §1681	Fair and Accurate Credit Transactions Act
2003	18 §1037	CAN-SPAM Act

For a list of state laws, see http://nsi.org/Library/Compsec/computerlaw/statelaws.html

MODEL

The primary hypothesis to be tested is whether the U.S. judicial system is capable of effectively handling computer crime cases. This hypothesis is best addressed by participants in the legal system (particularly attorneys and judges). In building a model to address this question, several additional details can be examined, such as relative opinions of the various branches of the legal system. The model framework applied to this study is consistent with Structural Equation Modeling (SEM) applications (see Muthen, 2002; Muthen and Muthen, 2004; Post and Kagan, 2005).

With a limited number of cases of computer crime arising each year, it is difficult for attorneys to specialize in the subject. In fact, it is likely that only a few attorneys and judges have acquired experience with cases of this nature. And in 11 years, only 23 federal computer crime cases have gone to trial, and two of those were non-jury trials. Consequently, there is minimal national experience with trying these cases. Certainly, defense and prosecuting attorneys have the skills and the ability to understand and apply laws to varying situations. But, it still takes time to learn the intricacies of the laws, develop and test strategies, and find ways to explain complicated technology-related concepts to juries.

The U.S. legal system, like others, is built on several components (e.g., prosecutors, defense attorneys, judges, juries, investigators). To address and handle complex technical cases involving computer crime means that all of the judicial components need an acceptable level of knowledge. Ultimately, the question involves the distribution of knowledge. If one component is more advanced, or substantially weaker than the others, the outcomes are unlikely to be "fair" or even effective. To obey laws, people have to understand at least the basic elements and to have faith that they are rationally adjudicated and enforced. A systematic model is applied to this study to determine a series of questions pertaining to the components of the judicial system and the relative degree of knowledge associated with computer security concerns.

Model Background

Figure 1 shows the basic model. This model assumes that the laws are accurately written and that the punishment systems are effective. That is, those elements lie outside the scope of this particular research, which focuses on the detection and prosecution of cases. With this focus, the five main components of the process are: (1) investigators, (2) prosecutors, (3) defense attorneys, (4) judges, and (5) juries or potential jurors. The level of knowledge and experience of each component should ultimately affect the deterrence effect of the various laws applied to particular infractions. For example, weak investigations could result in fewer crimes being detected, or losing cases because of problems such as breaking the chain of evidence. Similarly, if attorneys (prosecution or defense) are unable to explain a case to jurors (because of lack of knowledge by attorneys or by jurors), the deterrence effect is altered.

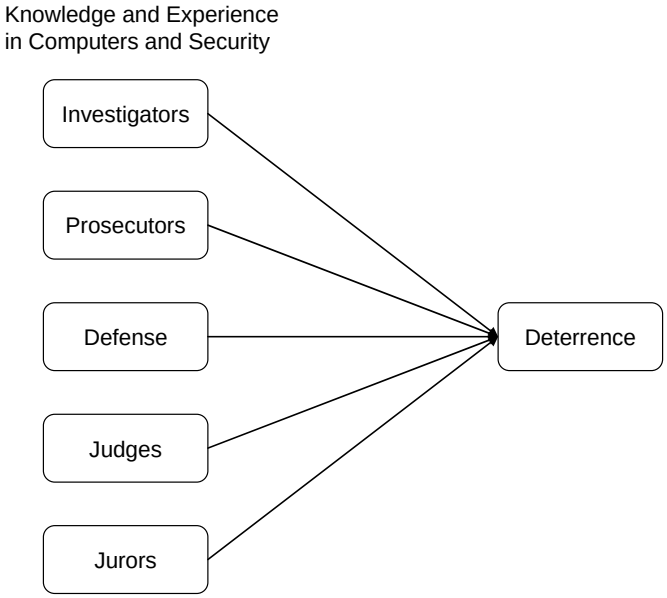

Figure 1: General Model.

(The legal system can be an effective deterrent only if each primary component has sufficient knowledge and experience in computer security. But, some elements might be more important than others.)

This model can be used to investigate several questions. The primary hypothesis is whether the judicial system can effectively and fairly prosecute and deter computer crime. More specifically, we would like to know if there are serious shortfalls in any of the individual components (judges, defense, prosecution, investigation, and jurors). These individual hypotheses can be tested by observing the values of the individual items projected in the model (see Figure 1). A second hypothesis is to identify whether some of the components are more important than the others in providing a deterrent. If so, it would make sense to strengthen those components first. These effects can be measured by estimating the strength of the relationship between knowledge variables and the deterrence variable. The model can also be used to identify whether some types of laws might be more amenable to deterrence than others. These effects can be evaluated by examining the constituent elements of the deterrence factor variable. In other words, what is the impact on overall deterrence of computer crimes from the elements of the judicial system based on the knowledge acquisition of the components?

A third set of hypotheses involves the type of computer crime. It is conceivable that some types of crime will be easier to identify, prosecute, or defend than others. For example, it is technically difficult to identify participants of SPAM, and it is likely to be difficult to quantify and explain damages to jurors. Of course, the null hypothesis is that each of the types of crime have the same challenges.

Each of the elements in Figure 1 represents a latent variable—because none of the items are directly observable. Consequently, each item is somewhat subjective. Since there is no way to observe the actual values, a survey instrument was created to ask legal professionals to evaluate the current status of these measures.

Survey Instrument

Legal participants—largely in the form of attorneys—were surveyed to determine their self-rated knowledge of computer security legal issues, and their perceptions on the state of the discipline within the legal system. As indicated by the limited number of cases nationwide, finding legal scholars was challenging, and getting responses took considerable effort. In the end, 89 usable responses were culled from a base set of about 150 replies. The contact lists, largely derived from the Martindale-Hubbell directory focused on attorneys, so no responses were obtained from police or investigators. Most of respondents listed themselves as civil attorneys (46), several (30) listed themselves in the "other" category—which was largely educational, a limited number (5) of responses were obtained from current criminal attorneys, and prosecutors (5), along with a few sitting judges (3). The relatively low number of respondents in these last categories makes it difficult to reach statistical conclusions based on the respondent's role within the system. However, all respondents evaluated all five categories, so the overall results are statistically acceptable. To control for differences in individual respondents, the survey also asked for basic background data such as the size of the organization that the participant was employed by.

The principle portion of the instrument was a section (see Appendix for complete instrument) where respondents were asked to rate the main variables of interest on a scale from 1 to 10, where 1 represented the least level of knowledge, skill, or experience. Respondents were asked to rate the five types of roles (investigators, prosecutors, defense attorneys, judges, and potential jurors). As an additional control, they were also asked to evaluate themselves and the organization they work for. Each role was evaluated in terms of four elements: (1) computer knowledge, (2) computer security knowledge, (3) knowledge of computer security laws, and (4) experience with computer security cases.

In terms of deterrence, participants were asked to evaluate the effectiveness on eight specific types of computer crime: (1) external crackers, (2) insiders or employees, (3) computer viruses, (4) identity theft, (5) unsolicited commercial e-mail or spam, (6) spyware, (7) intellectual property theft or piracy, and (8) privacy issues such as those embodied in the Health Insurance Portability and Accountability Act (HIPAA).

A Web site was employed for survey access which also facilitated simplification of data entry and navigation. Participants were primarily identified and contacted through publicly available local and regional lists. Specializations were not used in the initial search. That is, the survey was designed to get input from a variety of attorneys. In the end, few of them identified specialties. Bear in mind that that number of specialist practitioners in computer crime is small. A focus on this group would have biased the results. On the other hand, the respondents had some level of interest in the subject or they would not have completed the survey.

RESULTS

Due to the deliberate effort put in to finding willing participants, the completed results are statistically sound and reliable. The estimated model matches the theoretical model fairly closely and provides some useful results.

Participants and Reliability

Table 3 summarizes the basic background data on survey participants. Not surprisingly, most of the participants were from a larger city—which matches the population distribution of attorneys. The bulk of the practitioners were civil attorneys. In total, the responses from the criminal attorneys, prosecutors, and judges provide a reasonable representation, but probably not enough to analyze the results by role.

Table 3: Participant Backgrounds.

Item	Category	Observations
Job Role	Criminal	5
	Prosecutor	5
	Civil	46
	Judge	3
	Other/Educator	30
Company Size	1-100	15
	101-500	19
	501-1000	10
	1001-2000	10
	More than 2000	28
City Size	Small, rural	1
	Mid-size city	6
	Suburb	7
	Metropolitan	74
Job Experience	Less than 1 year	2
	1-3 years	15
	4-5 years	7
	6-10 years	14
	More than 10 years	50

Most were from a large city, from a variety of company sizes. (The educators affected the size values.)

Internal instrument reliability was measured by Cronbach's alpha (1951). Because of its structure, this instrument is best evaluated in terms of the individual subsections based on separate ratings for computer knowledge (0.69), security issues (0.84), computer laws (0.85), experience with computer security cases (0.84), and the deterrence questions (0.93). Nunnally (1967) reports that Cronbach alpha scores of 0.8 or higher are indicators of internal construct validity with survey based data. Only the computer knowledge question falls below this threshold. This value can be explained by observing that considerable divergence exists in the definition of computer knowledge and skills. The value simply indicates (correctly) that there is disagreement over the meaning of the term and the inherent variability of self-evaluation of those skills. Since the study is not looking for computer programmers or experts, the subjectivity of the definition is acceptable—particularly with the strength of the coefficients in the other sections. In terms of external reliability, the study was pre-tested with a few legal personnel to ensure the participants understood the questions.

With any survey, there is a possibility of non-response bias. The standard method for evaluating this issue was provided by Farber (1948), Mayer (1970), and Armstrong and Overton (1977). The approach is to examine the characteristics of the respondents at various points in time. If the respondent characteristics are similar in the groups, then there is no substantial demographic bias. In this particular survey, two basic groups were created—with a split over the year-end holiday. Three characteristics (role, firm size, and experience) were compared via standard t-tests across these two groups. There was no significant difference (at a 5-percent level) in any of these characteristics. However, in examining these returns, we noted that both groups were overly represented by respondents with relatively long levels of experience. Consequently, a third (stratified random) initiative was used to garner additional responses that targeted a less-experienced group so that the overall panel would more closely represent the population demographics.

Model Estimation

Primary latent variables estimating the knowledge and experience of the various roles were identified through the four primary items asked for each role. These same items were also posed for the individual and the organization. In the structural equation model, these indicator variables identify the latent variables. The eight items on specific types of security issues are used to identify the deterrence latent variable.

Figure 2 shows the primary results of estimation of the structural equation model. The standardized coefficients are displayed for the regression model and for the items on the deterrence variable. To keep the chart readable, the coefficients on the other individual factors are not presented. However, all of those are positive and significant at a 1 percent error level. Cross correlations among those variables are also not shown on this figure. Mean values and intercepts were also estimated. Although the majority of these are significant, they are not displayed on this figure. The Chi-square goodness of fit measure has an error level of 0.052, which is acceptable (greater than 0.05). The root-mean-square-error (RMSEA) is relatively low at 0.043. Other goodness of fit measures are similar, indicating that the estimated model is acceptable.

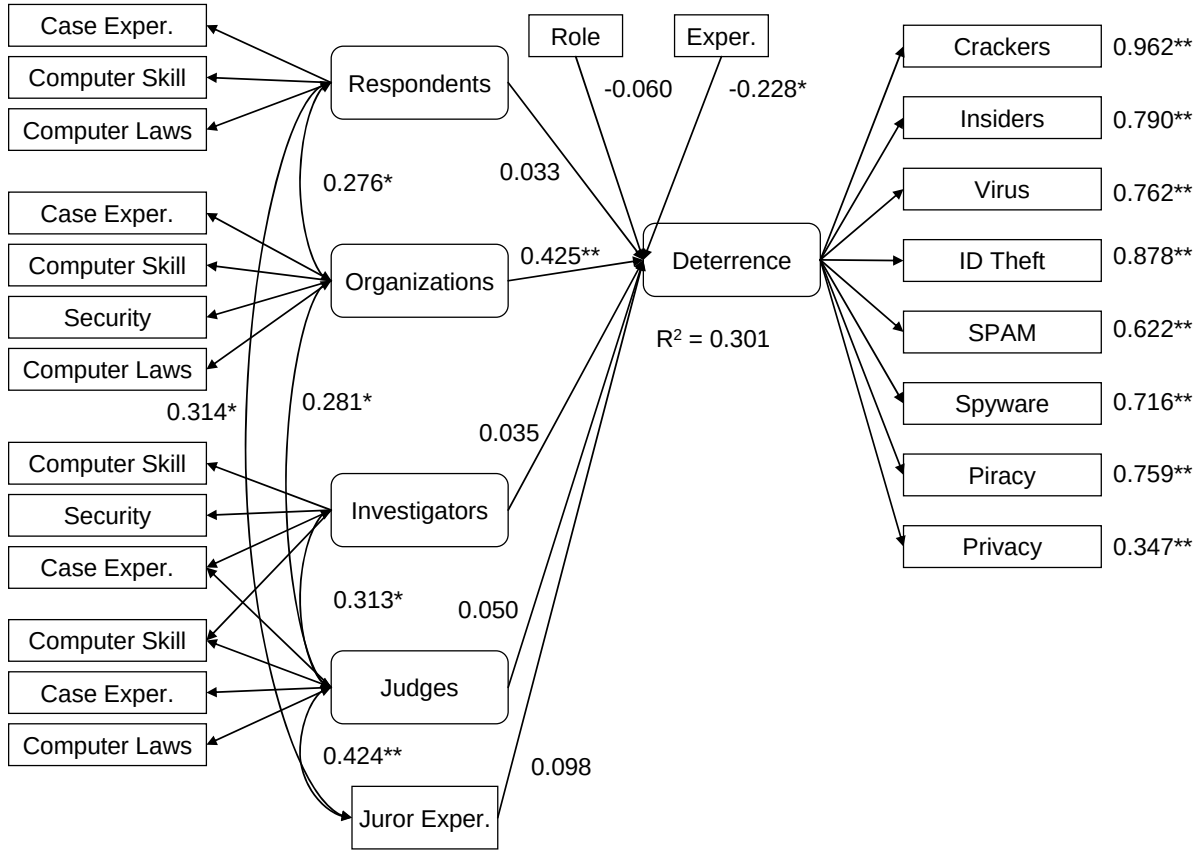

Figure 2: Primary Model Coefficients*.

*The coefficients on the items for the roles (left side) are not shown to save space, but they are all significantly positive at a 1 percent error level. The goodness of fit Chi-square probability is acceptable at 0.052. The model has an RMSEA of 0.043.

Notice that a few concessions were made from the theoretical model. In particular, the latent variables for the two types of attorneys (civil and defense) did not significantly contribute to the model. Although it was possible to estimate the variables independently, they tended to destabilize the residuals and since the variables did not have a significant effect on the overall model, they were removed. Certain confounding issues arose because the respondent and organization variables are measuring similar effects, and the respondent and organization variables are more reliable because respondents are reporting on themselves instead of other entities.

In terms of the identification of the basic factors, case experience is the strongest indicator variable. The other coefficients are also positive and strong, indicating that the latent variables are accurately identified in terms of measuring computer security law knowledge. Higher values of any of the indicators represent higher levels of knowledge.

Overall Knowledge by Role

The easiest way to understand the level of knowledge for the primary roles is to look at the means. Figure 3 shows the mean ratings of security knowledge reported for each of the primary roles. The chart shows the differences grouped by the respondent's role, but remember that three of the roles have a limited number of observations.

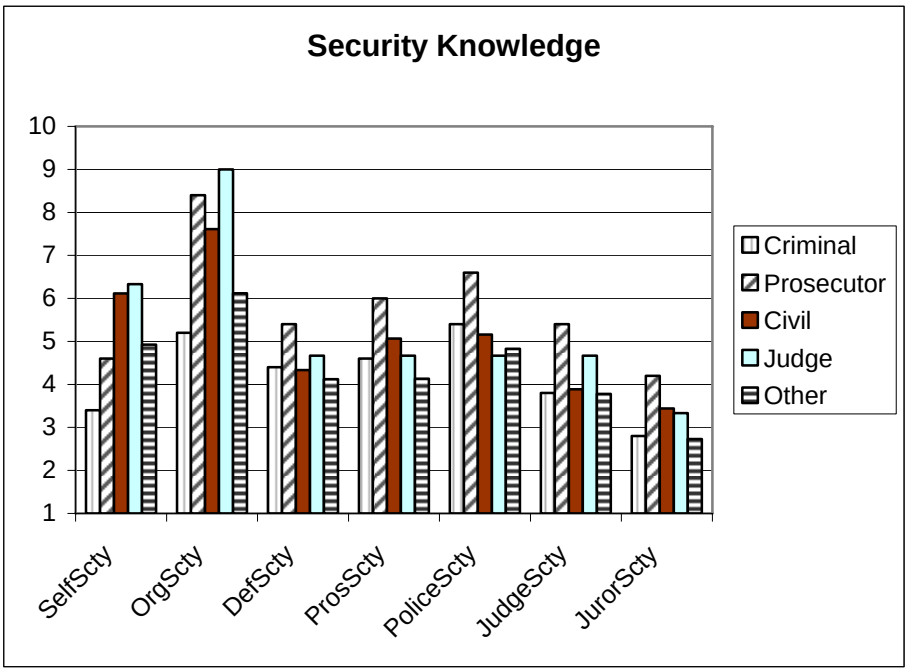

Figure 3: Mean ratings of security knowledge by role.

The differences might be interesting, but this report focuses on the overall values. The pattern shown here is generally representative of the other variables as well. First, note that most of the respondents rated themselves as having mediocre or lower knowledge of security (and computers). On the other hand, most reported that someone within their organization was considerably more skilled. This level of specialization is rational in larger firms—particularly given the relative scarcity of computer crime cases compared to other cases. On the other hand, although most respondents believed that someone with a relatively high skill exists within their organization, this belief did not extend to other organizations. For example, even though prosecutors believe that someone with a relatively high-level of computer security knowledge exists within their organization, the overall average rating for prosecutors is substantially lower than that. The same pattern holds for other categories and roles.

Table 4 presents a view of the overall means, which are useful in evaluating the second set of hypotheses involving the valuation of the individual legal system components. Looking across the roles (defense, prosecutor, investigator, judge, jury) for each specific category (computer skill, security knowledge, computer law knowledge, and case experience), ANOVA results report significant differences. Paired T-tests were used to identify the roles that are significantly higher or lower than the others. The first, relatively simple, result is that attorneys always believe potential jurors have less knowledge. In terms of knowledge of the law and case experience, this belief is undoubtedly true. The results in terms of computer and security knowledge might be true, or this may reflect a general belief that attorneys are trained to expect that juries to have minimal knowledge and must be "educated." On the other hand, the similar belief about judges is harder to explain. Although, if it is true, it would imply that any educational program will have to include judges specifically.

Table 4. Overall Rating Differences*.

Item	Significantly Higher	Significantly Lower
Computer Knowledge		Judges, Jurors
Security Knowledge		Judges, Jurors
Computer Laws	Prosecutors	Jurors
Case Experience	Prosecutors	Jurors

*There are significant differences across the roles (Defense, Prosecutor, Investigator, Judge, and Juror) for each of the major items. The roles with statistically significant (paired T-Tests) results are presented.

A more interesting result is that prosecutors are perceived to have the highest level of computer security law knowledge and case experience. Note that federal crime statistics (Federal Justice Resource Center, Administrative Office of the U.S. Courts) show about 80 percent of computer crime cases are settled with guilty pleas. Consequently, only a handful of these cases go to trial in any year. As a result, defense attorneys are unlikely to specialize in the field and rarely see cases. Similarly, it is rare for any given judge to handle a computer crime case. On the other hand, prosecutors in large cities could allocate training money to a few classes. Although training funds are often limited, with a couple of hundred federal cases a year in the United States, at least a few prosecutors need to be trained to handle these cases. This pattern is supported by the prosecutors who responded to the survey—as a (small) group, they indicated that they (and other prosecutors) have higher levels of knowledge and experience than the other set other legal role players.

Deterrence Effect of the Judicial System

Various components of the judicial system can be determined as a deterrence effect by measuring the coefficients of the regression model on the deterrence variable. Only two of the coefficients are significantly different from zero, but the results are complicated by the correlations across the independent latent variables. The clearest variable is the negative coefficient (-0.228) on the independent variable measure job experience. Higher values of the variable represent more years on the job. The negative sign means that respondents with more experience believe the judicial system is less likely to provide a deterrent to computer crime. This result might be cynicism developed over time, idealism of youth, or simply a rational perspective gained through experience.

The other significant effect is more difficult to interpret. The coefficient (0.425) on the organization variable is significantly positive at a 1 percent error level. By itself, this states that when respondents perceive a higher level of computer security knowledge and experience within their organizations, they believe the judicial system will be a stronger deterrent to these types of crimes. The interpretation is slightly complicated by the correlations with the other latent variables. Higher levels of organizational value are positively related to higher levels of knowledge with the other categories. In other words, higher levels indicate a confidence in the capabilities of the various participants within the judicial process which leads to a greater belief that the judicial system can deter crime. From a theoretical perspective, this result should be true—since the opposite is undoubtedly true. (If the judicial system has minimal skills, dishonest people would eventually take advantage of this perceived lack of knowledge.)

In terms of answering the primary hypothesis regarding effectiveness of the legal system, the key lies in the regression coefficients that affect the deterrence variable. Only the coefficient from organizations is significant. In particular, respondents do not believe investigators, judges, or jurors can be effective at deterring computer crime. Essentially, only a few respondents—specifically from organizations with case experience—believe the legal system can serve as a deterrent to computer crime. The means (not shown on the figure) also support the conclusion.

Deterrence for Specific Security Issues

The deterrence effectiveness of the judicial system can be examined in terms of specific types of crimes. The third set of hypotheses regarding the types of crime can be evaluated by examining the magnitude of the standardized coefficients on the indicator variables. These values are reported on Figure 2 (on the right-hand side). Notice that all of the values are positive and significant at a 1 percent level, which means they are all reasonable indicators. However, some of the values are substantially higher or lower than the others. The higher values are associated with

crimes that are more likely to be deterred by the judicial system. These types of crimes include external crackers (0.962), identity theft (0.878), and insider attacks (0.790). The common feature of these three items is that this particular crime types are relatively obvious—they often involve money or damages, have identifiable victims, and are relatively easy to explain to jurors. The items with lower values are emphasized by privacy (0.347), spam (0.622), and possibly spyware (0.716). These crimes are more difficult to detect, are likely to be committed by outsiders (from the organization) who can hide fairly easily, and oftentimes it can be difficult to show victims and damages.

INTERPRETATIONS AND CONCULSIONS

Participants were also given the opportunity to provide written comments. Over half (58%) suggested some type of education—particularly for people within the judicial system. A few suggested the need for new laws and better enforcement. One directly stated that some of these types of crimes are not being prosecuted because of a lack of resources—particularly trained investigators and prosecutors. Based on the level of the overall ratings, along with these comments, it is clear that increased education and training is needed. Some work is being done in various areas—particularly programs for training investigators to follow defined procedures when collecting evidence. Some large organizations provide training for prosecutors—where one or two individuals could specialize in these types of cases. But, almost no work is being done in training defense attorneys (or attorneys for civil cases), or judges. Additionally, the level of knowledge of computer laws within the potential jury pool is minimal. Based on the respondent perceptions, most of the attorneys believe potential jurors have almost no knowledge of any of the technical or legal issues associated with computer crimes. This situation will make it difficult to prosecute (or defend) these types of cases. Even if a prosecutor has solid evidence, if the case is complex, it will be difficult to press the case to a jury trial. From a defendant's perspective, the situation is even bleaker. Because of the scarcity of cases, it will be difficult to find a defense attorney with the technical knowledge and experience to handle the case. Cases that have obvious ties to existing laws and procedures will be relatively easy to handle—particularly those that involve monetary or physical damages. Cases that hinge on technical issues—particularly privacy, spam, or pure data, are going to be considerably more difficult to handle at this time.

Calling for more education is a relatively obvious step. Finding a way to fund it could be more difficult. The situation is even more complex for defense (and civil) attorneys. With relatively few cases at the moment, the need is not obvious, and it is not clear that the training and education will be profitable. At least in the short run, any establishment of educational classes for computer security law will also need to find a way to incorporate defense attorneys and judges at a relatively low cost. However, the cost of time is going to be harder to solve. The lack of experience in handling cases is an even bigger problem. Understanding the technology and the laws is not enough. All participants need practice with the issues to determine which strategies are useful, how best to explain concepts to jurors, and to recognize motivations and actions that are the most important.

For the US judicial systems to become more effective at both handling computer crime issues and be a vehicle for a deterrent to computer security infractions, this system must be driven by a knowledgeable set of players. This implies that attorneys, judges and jury members have a reasonable knowledge base to be conceptually engaged in the legal process and follow the issues at a level of understanding so that effective results will be derived. If any part of the system is not adequately versed in terminology, concerns or the impact of the pervasive aspects of computer security, the system itself is relegated to inaccuracy. This will lead to imbalances that will impact the judicial process itself.

REFERENCES

Armstrong, J.S. and T. Overton. (1977). Estimating Non-response Bias in Mail Surveys, *Journal of Marketing Research*, 14, 396–402.

Bidgoli, H. (2003). "An Integrated Model For Improving Security Management In The E-Commerce Environment,".*Journal of International Technology and Information Management*, 12(2) 119-134.

Caelli. W.J. (2002). Trusted ...or... Trustworthy: The Search for a New Paradigm for Computer and Network Security, *Computers and Security*, 21(5), 413-420.

Carr, I. and K. S. Williams. (2000). Securing the E-Commerce Environment – Enforcement Measures and Penalty Levels in the Computer Misuse Legislation of Britain, Malaysia and Singapore, *Computer Law and Security Report*, 16(5), 295-310.

Cronbach, L.J. (1951), Coefficient Alpha and the Internal Structure of Tests, *Psychometrika*, 16 (September), 297-334.

Dowland P.S., S. M. Furnell, H. M. Illingworth and R. L. Reynolds. (1999). Computer Crime and Abuse: A Survey of Public Attitudes and Awareness, *Computers and Security*, 18(8), 715-726.

Easterbrook, F.H. (1996). Cyberspace and the Law of the Horse, speech at the University of Chicago Law School conference. http://www.law.upenn.edu/law619/f2001/week15/easterbrook.pdf.

Farber, R. (1948). The Problem of Bias in Mail Returns: A Solution, *Public Opinion Quarterly*, 13, 669–676.

Gerard, G. J., W. Hillison and C. Pacini. (2004) Identity Theft: the US Legal Environment and Organisations? Related Responsibilities, *Journal of Financial Crime*, 12 (1), August, pp. 33-43.

Kennedy G. (2001). Computer Crime - Hong Kong - Hong Kong Steps up Efforts to Tackle Computer Crime, *Computer Law and Security Report*, 17(2), 110-113.

Lampson, B.W. (2002). Computer Security in the Real World, *Computer*, 37(6) 37-46.

Landwehr, C. E. (2001). Computer Security, *International Journal of Information Security*, 1(1) 3 – 13.

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach, *Harvard Law Review*, 113, 501-546.

Mayer, C. (1970) Assessing the Accuracy of Marketing Research, *Journal of Marketing Research*, 3, 285–291.

Muthen, B. (2002). Beyond SEM: General latent variable modeling. *Behaviormetrika* 29, 81-117.

Muthen, B., and L. Muthen, (2004) Mplus Statistical Analysis with Latent Variables, User's Guide. Muthen and Muthen, Los Angeles.

Nunnally, J. (1967) *Psychometric Methods*, McGraw-Hill (New York).

Opara, E. U., and J.T. Marchewka. (2006). "Enterprise Integrated Security Platform: A Comparison of Remote Access and Extranet Virtual Private Networks," *Journal of International Technology and Information Management*, 15(2), 39-48.

Post, G. V. and A. Kagan. (1998). The Use and Effectiveness of Anti-Virus Software, *Computers & Security*, 17, 589-599.

Post, G. V. and A. Kagan. (2003) Computer Security and Operating System Updates, *Information and Software Technology*, 45(8), 461-467.

Post, G. V. and A. Kagan. (2005). Systems Development Tools and the Relationship to Project Design: Cost and Budget implications. *Journal of International Technology and Information Management*, 14(1), 1-14.

Roberts, P. (2005) Secure Tokens Won't Stop Phishing, *Computerworld*, March 15.

Ryker, R, M. Khurrum and S. Bhutta. (2005). "Online Privacy Policies: An Assessment of the Fortune Global 100," *Journal of International Technology and Information Management*, 14(1), 15-24.

Schneier, B. (2005), Two-Factor Authentication: Too Little, Too Late, *Communications of the ACM*, 48(4), 136.

Straub, D.W. (1990), Discovering and Disciplining Computer Abuse in Organizations: A Field Study, *MIS Quarterly*, 14(1), 45-60.

Walden, I. (2004) Harmonising Computer Crime Laws in Europe. *European Journal of Crime, Criminal Law and Criminal Justice*, 12(4), 321-336.

APPENDIX

Survey Instrument

Background

1. Choose the category that best describes your current job/role:
    a. Criminal attorney
    b. Prosecuting attorney
    c. Civil attorney
    d. Judge
    e. Investigator or Law enforcement
    f. Other: _____

2. Size of the company or organization you work for in total number of all legal cases handled in a year:
    a. 1 – 100
    b. 101 – 500
    c. 500 – 1000
    d. 1001 – 2000
    e. More than 2000

3. Type of city in which you primarily work:
    a. Small, rural community
    b. Mid-size city
    c. Suburb of a larger city
    d. Large metropolitan city

4. Years of experience in your current career:
    a. Less than 1
    b. 1 – 3
    c. 4 – 5
    d. 6 – 10
    e. More than 10

Do you agree or disagree with the following two statements?

5. **Criminal** cases regarding computer security and privacy are likely to result in fair/reasonable outcomes.
    a. Strongly disagree b. Disagree c. Neutral d. Agree e. Strongly agree

6. **Civil** cases regarding computer security and privacy are likely to result in fair/reasonable outcomes.
   a. Strongly disagree b. Disagree c. Neutral d. Agree e. Strongly agree

The following questions ask for your opinion of the knowledge and capabilities of several groups of people. Evaluate each group based on an average. Enter a number from 1 to 10 in each cell in the grid, with 1 representing the lowest level. Be sure to rate yourself as well.

Question	Self	Your organization	Defense Attorneys	Prosecutors	Investigators or Police	Judges	Potential Jurors
Knowledge of computers							
Knowledge of computer security							
Knowledge of computer security and privacy laws							
Experience with computer security and privacy cases							

Is there someone within your organization who has received specialized training in these areas? (# of people: ____)

For each of these categories, indicate whether you think the legal system will be an effective deterrent to preventing problems in that category. Enter a value from 1 to 10, with 1 representing the low end that the legal system will not be effective.

Category	**Effectiveness of legal system rating 1 to 10**
Theft or destruction of data by external hackers or crackers.	
Theft, fraud, or destruction of data by insiders (employees/consultants).	
Attacks by viruses and worms.	
Identity theft through phishing and similar scams.	
Unsolicited commercial e-mail (spam).	
Spyware, tracking, and related privacy issues.	
Digital content piracy or theft.	
Customer privacy violations, such as that required by HIPAA.	

The final layout was slightly different since it was administered via a Web site.