This is to certify that the
thesis entitled

NETWORK INTRUSION AND THE CRIMINALIZATION PROCESS

presented by

JACK DREW

has been accepted towards fulfillment
of the requirements for the

M.S. degree in Criminal Justice

N. Mark Lowe
Major Professor's Signature

August 20, 2003
Date

NETWORK INTRUSION AND THE CRIMINALIZATION PROCESS

By

Jack Drew

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

School of Criminal Justice

2003

ABSTRACT

NETWORK INTRUSION AND THE CRIMINALIZATION PROCESS

By

Jack Drew

Previous research indicates that the actions of computers hackers have become frequent and costly, yet many victims choose not to report security violations to the police. This study uses Turk's Theory of Norms Violation (1966) to explain and predict how organizational responses to network intrusion affect the criminalization process. A purposive sample of 145 security professionals belonging to the American Society for Industrial Security (ASIS) International was developed to collect data about organizational perceptions of hackers. Members living in Michigan were mailed a questionnaire and 19 usable responses were returned. Organizations were found to have experienced network intrusions committed by unknown individuals, with network attack being the most common form of victimization. Turk's premises failed to predict the propensity of organizations to criminalize offenders. Results suggest that organizations are keen to work with authorities to reduce cyber crime, an observation that should encourage both groups to seek closer cooperation in the future.

ACKNOWLEDGMENTS

This work would never have reached completion were it not for the support of many kind individuals. First, I would like to thank the members of my committee - Professors Mahesh Nalla, Christina DeJong, and John McCluskey - who not only advised me but also encouraged me throughout the entire research process. I was extremely lucky to work with such a fantastic set of people.

Second, I am grateful to Professor Nalla who acted as a mentor during my graduate studies. His kindness and patience were much appreciated, especially when it came to giving me more time to draft sections of this thesis! I think he saw something of a kindred spirit in a fellow international arriving on American shores to undertake graduate studies. But whether we talked about academic matters or sport, he always made me feel welcome.

Third, I would like to thank Terry Berg, Kelly Carter, and Peter Plumber of the Michigan Attorney General's Office. Kelly, in particular, kept her word and released data collected by the High Technology Crimes Unit. Although I choose not to use all of it, I was a happy beneficiary.

Fourth, my family and friends (everywhere) deserve a special "thank you" for encouraging me to pursue my life goal of working in law enforcement. Of friends at MSU, Christina Harzman helped me to enjoy American life. On the thesis front, not only did she generously spare stamps so that I could post surveys, she always took an interest in how I was progressing.

Last, but by no means least, I would like to mention my paternal grandparents. Although they passed away thirteen years ago, it is due to their forethought and generosity that I could afford to study in the United States. To receive such an opportunity was a blessing and one I will always be thankful for.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Premise

Business magnate Bill Gates once remarked that "no one gets to vote on whether technology is going to change our lives" (1996:11). The reliance we place on computers is a case in point. Administration and commerce, recreation through training all depend on computers in the Information Age. Whether battling virtual demons or making a holiday reservation, the choices we make are processed, stored, and recalled digitally.

A key factor behind the computer's rise to prominence has undoubtedly been its networking capability. Information sharing is facilitated by computers talking across networks designed to be fast and reliable. Built to be robust yet flexible, the technology driving today's Internet, the Transmission Control Protocol/Internet Protocol (TCP/IP), grew from a military plan for bunkers across the United States to maintain contact post-Armageddon (Comer, 1995). Distance is no obstacle. All that prevents us from receiving the information we desire is elapsed time.

This utility, a product of mankind's creative energies, is not without social hazard. Nowadays computers are involved in crimes such as fraud, harassment, privacy violation, theft and vandalism. Especially pernicious acts include the manufacture and distribution of child pornography, and the solicitation of minors. Furthermore, computers can hold critical information in cases of violent crime such as abduction, assault, homicide and rape (Casey, 2000).

To better categorize what is a wide range of crimes, Stephenson (2000) uses the term "cyber crime" to distinguish networked crime from standalone computer crime. Unlike a conventional crime that binds offender and victim in the same physical location,

cyber crime suggests that a system of internetworked computers makes remote crime possible. An example of this phenomenon is network intrusion, or hacking, and it is simply defined as "access [to] computers without approval or authority" (Kovacich & Boni, 2000:63).

Unfortunately, while network intrusion sounds innocuous, the consequences of this virtual crime are real and often damaging. The Australasian Centre for Policing Research (2000) list the following challenges to police investigations of networked computer crime:

- Anonymity in the digital realm
- Global reach of networks and scope for extensive victimization
- Execution of crimes at high speeds
- Potential for criminals to traverse jurisdictions and exploit sovereignty issues
- Ephemeral evidence that is easy destroyed and difficult to capture.

With enforcement activities compromised, confidence in computers and the systems they maintain also suffers. This is an important consideration. The United States has built and implemented a popular tool used by 165.8 million of its citizens, not to mention countless others around the globe (CIA, 2003). As a community, the next challenge is to demonstrate technical and social innovation in equal measure. To realize this ideal it is necessary to better understand how the protagonists in cases of network intrusion - hackers - are viewed and responded to.

Objective and Scope of Research

Articles on networked crime include a number of recurrent themes. A common focus is the media's portrayal of hackers and hacking incidents. Driven by the belief that

the general public finds innovative crime a novelty, the media gives high visibility to computer crime (Parker, 1983). It is through media reports that we shape our perceptions of hacking and a hacker's profile (Goodman, 1997). Unfortunately, this coverage is often inaccurate resulting in exaggerated reports of financial losses and the actions taken by hackers (Dierks, 1993). This problem is compounded by the moving pictures industry which likes to portray hackers as being either benign and/or endowed with technical abilities bordering on the fantastic. Thus, hackers are depicted as latter day Robin Hoods and interest in their activities is sustained (Fiery, 1994).

Similarly, the efficacy of legal statutes is questioned. A major assumption is that laws should serve as both a punitive measure and as a deterrent to potential offenders. Given this rationale, the dearth of successful prosecutions suggests that existing laws addressing computer crime are inadequate. Furthermore, new legislation reflects a desire only to establish relations of property and authority rather than any effort on the part of law makers to actually capture and prosecute offenders (Michalowski & Pfuhl, 1991). In contrast, others suggest that the United States Congress has been updating laws to keep pace with technological advances. But a dilemma exists in developing laws that are applicable at state, federal and international levels (Bakewell, Koldaro, & Tjia, 2001).

There is also a belief that while police should care about investigating computer crimes, they do not. This is largely due to the internal culture of police departments that ascribes a higher priority to violent and drug-related offences than to computer related mischief. Moreover, the costs associated with purchasing forensic equipment and training police officers only serves to discourage investment in specialist computer units. Any case for securing greater funds is undermined by underreporting of computer offences

and a reluctance by police chiefs to spend on agendas that will not provide clear returns. Finally, a lack of public outcry from businesses and citizens, unless it is to criticize law enforcement violations of privacy, reinforces the view that funds are better spent on reducing visible crime (Goodman, 1997).

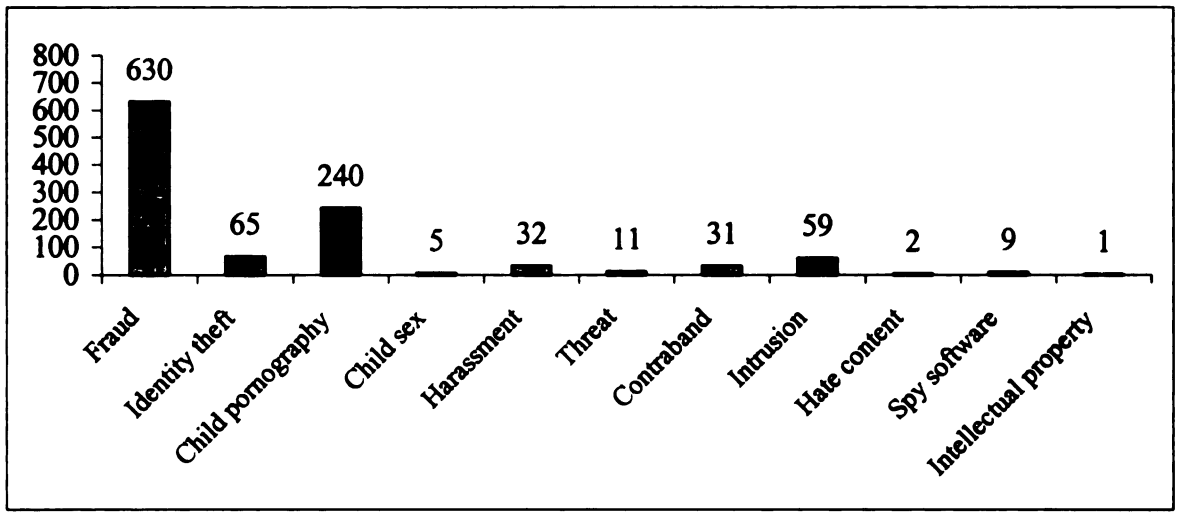
This synopsis is not intended to denigrate the efforts of authors but to point out that as intuitively appealing as their ideas may be, none of these concepts are formally tested. Additionally, there is considerable misunderstanding of the role that victims play in computer crimes. Indeed, very little is said about victimization in the general literature. To comprehend network intrusion it is necessary to recognize that until an incident is reported, no crime has officially occurred (U.S Department of Justice, 1967). In other words, contact with a law enforcement agency is the first step towards a case entering the criminal justice system.

With these thoughts in mind, the study aim is to understand exactly how organizations, which are sizeable targets for hackers, respond to incidents of network intrusion. Principally, *what decision-making process takes place within organizations that shapes their responses to network intrusion?*

The scope of the research extends to public and private organizations that operate in the state of Michigan. Organizations in Michigan, as a unit of investigation, are targeted principally because of their diversity. Michiganders work in a range of industries including construction, education, farming, health care, hospitality, mining, professional services, public administration, trade and transportation (U.S. Census Bureau, 1997a). Additionally, the Michigan legislature successfully voted to create a dedicated police forensics unit, with statewide powers of investigation, in 1998 (State of Michigan,

2003a). Since then, the legislature has continued to tighten state laws addressing computer malfeasance (State of Michigan, 2003b) and this action, as Figure 1[1] shows, has enabled authorities to investigate a variety of complaints involving computers. In summary, Michigan includes a range of targets for hackers but the state's criminal justice system is also prepared to respond to incidents of network intrusion.

Figure 1. Complaints received by law enforcement agencies in Michigan, 2000 through July 2003 (N=1085)



Merit of Research

The benefits of pursuing this work are twofold. Firstly, research dedicated to the issue of cyber crime is limited. Previous studies have tended to be exploratory in nature and have seldom been designed as empirical tests of criminological theories. The next

[1] The High Technology Crimes Unit, a division of the Michigan Attorney General's Office, upon special request, provided the data listed in Figure 1.

step in the scientific process is to see whether network intrusion can be explained by an existing theory.

Secondly, any study of crime represents an opportunity for law enforcement officials and policy-makers to learn more about current trends. An independent study such as this may confirm existing knowledge or uncover new findings. In principle, as the cumulative body of research grows, practitioners enhance their understanding of contemporary issues and are better able to revise strategies that address social problems (Neuman & Wiegand, 2000).

TURK'S THEORY OF NORMS VIOLATION

In much the same way alchemists attempt to transmute matter, individuals seek to infuse their communities with equitable traits. As long ago as 500B.C., the ancient Greeks discussed issues such as ethics and justice. In this way they hoped to reach common agreement on values like honor and virtue, truthfulness and wrongdoing. Underpinning this acceptance of shared values was the belief that consensus promotes solidarity within a democratic society (Beirne & Messerschmidt, 1995).

Industrialization during the nineteenth century brought a different perspective to this debate. While early mechanization freed people from the land, the prospect of working on the factory floor awaited them. Toiling long hours in poor conditions for meager wages, some wondered if the human lot had genuinely improved. Among the disbelievers were Karl Marx and Frederick Engels, architects of modern socialism. Their view was simple: society was ruptured because of a division of labor and private ownership that created conflict between its citizenry. Writing in 1847, Marx and Engels argued capitalism was leading to "the exploitation of one part of society by the other" (1998:59).

Contemporary notions of power structures are keenly disputed. First published in 1956 by C. Wright Mills, *The Power Elite* articulates the view that a select few dominate American society. Occupying strategic positions at the top of the economic, military and political domains, the elite is able to make wide reaching decisions that impact upon the people at large. Furthermore, in order that decisions are enacted cleanly, advisers and spokesmen are employed by the elite to distract the general public who remain impotent.

The unquestioning acceptance of capitalism by the American people is a central theme of *The Affluent Society*. Despite flourishing economic conditions at the time of book's release in 1958, John Galbraith argued for social balance. Too often he suggests, private goods are treated as a necessity while public goods are regarded as a luxury,

> It is scarcely sensible that we should satisfy our wants in private goods with reckless abundance, while in the case of public goods, on the evidence of the eye, we practice extreme self-denial (2001:48).

Challenging what he describes as the "Conventional Wisdom" (2001:21), accepted beliefs divorced from social reality, Galbraith adds that the relegation of public services leads to limited opportunity, poverty and social disorder.

The rebuttal to these ideas came in 1962 when Milton Friedman wrote *Capitalism and Freedom*. Friedman makes three points about competitive capitalism. First, a division of labor is necessary to effectively use available resources. Second, there is no such thing as democratic socialism because socialism, by definition, does not allow individual freedom. Third, capitalism decentralizes political power,

> The characteristic feature of action through political channels is that it tends to require or enforce substantial conformity. The great advantage of the market, on the other hand, is that it permits wide diversity. It is, in political terms, a system of proportional representation (1982:15).

Prescribing the role of government in a free society, Friedman insists that the state should act only as a mediator where differences occur. Moreover, the extent of paternalism, as exercised by the state, should be left to the judgment of the people.

These ideals highlight the differences of opinion concerning the role of the market and levels of state intervention. However, events during the 1960s only served to boost and quash expectations of equal opportunity in the United States. Along with legislation increasing legal rights for minorities, reformist leaders such as John Kennedy and Martin Luther King Jr. were assassinated. Moreover, the war in Vietnam and the civil riots that took place towards the end of the decade underlined the schisms present in American society (Cullen & Agnew, 1999).

Increasingly, authors wrote about social injustice. Among their number were the conflict criminologists whose goal was to unmask the "motives, strategies, and tactics of those in power" (Lilly, Cullen, & Ball, 2002:132). Inherent in conflict criminology is the understanding that crime is a political concept. Behaviors deemed legal or illegal reflect the power structures in society and so the criminal justice system perpetuates the interests of the powerful. In such an environment,

> The system is largely set up to process poor and minority offenders – most of whom could find no meaningful place in the labor market – while ignoring the illegalities of rich and corporate offenders (Cullen & Agnew, 1999:296).

Consequently, conflict theorists are critical of the mechanisms they believe promote social division (Beirne & Messerschmidt, 1995).

Legality of Norms

In his explanation of the criminalization process, Austin Turk (1966) maintains that criminality is not a behavior but rather an assignment of status,

> A person is evaluated, either favorably or unfavorably, not because he *does* something, or even because he *is* something, but because others react to their perceptions of him as offensive or inoffensive (p. 340).

This occurrence reflects a dichotomous society consisting of authorities and subjects. Authorities announce and enforce classes of acceptable behavior. Subjects must conform to, yet may violate, these norms.

To illustrate the dynamic relations between authorities and subjects, Turks states that norms fall into two categories. Cultural norms define standards of expected behavior; they are explicit statements. Social norms reflect real patterns of behavior; they are implicit expectations. This highlights a need for authorities to communicate a norm clearly and subjects to be aware of norms. However, Turk insists that subjects learn to defer to authority through socialization. This is important because it is only when subjects accept a norm that it may be considered a legitimate one.

Naturally, not all subjects do accept legal norms. In the case of norm resistance, Turk predicts that conflict between parties will take place, then authorities intervene to interpret the situation and to apply sanctions. Violators are negatively evaluated and deprived of "something significant...including such intangibles as self-esteem and assumptions about personal identity and sanity" (1966:345). These actions ensure that the legality of the authorities and their norms are recognized.

The Realism of Moves

The theory of norms violation states that the actions of conflict parties determine the extent of sanctioning. It is therefore possible to predict conflict outcomes. Initially, parties adopt a position from a range of alternatives. Their choice can change but it is

assumed that they will attempt to move to an optimum position. In accordance with this goal, a favorable move is one that increases the probability of achieving a successful outcome. For authorities this might be law enforcement, whereas for subjects this could mean the preservation of non-criminal status.

Turk describes this phenomenon as the "realism of moves" (1966:344) and he acknowledges a number of factors that influence the decision-making process. Chief among variables impacting upon decisions are the level of organization within a party and the degree of sophistication a party has. For example, a party that is cohesive, has only a few members, and speaks with a single voice is more likely to make realistic moves than a large collective with ineffective leadership. Similarly, a party that employs sophisticated tactics improves its chances of achieving a desirable outcome and, from the perspective of norm resistors, of avoiding conflict altogether.

Turk's Propositions

Completing the work, Turk lists propositions for testing each of his ideas explaining criminality. The five main premises are:

1. Conflict is most likely to occur when there is high congruence between cultural and social norms for authorities and subjects.
2. Authorities who are greatly offended by an illegal attribute or behavior are more likely to criminalize violators.
3. Authorities are more likely to sanction subjects who attach great importance to an opposing norm.
4. Criminalization is more likely to occur when authorities have greater control over resources than opposing subjects.

5. The level of success a party achieves is directly related to the realism of moves the party makes.

The first premise suggests that the probability of conflict increases with cultural difference. For this prediction to be true, authorities must care strongly for norms whilst subjects remain entirely indifferent to them. A sign of imminent conflict is the authorities' reliance upon legal positions juxtaposed with opposition appeals to more abstract principles, for example natural justice or individual rights.

The second premise implies that the responses of multiple enforcers will influence the level of sanctions imposed. In terms of punitive measures, those who dictate sentencing powers and are offended by violations will ensure that the penalties associated with criminalization are significant. However, when first-level enforcers (investigators) care about a violation but higher-level enforcers (judges) are less concerned, it is unlikely that a case will pass beyond the first legal stage. Then alternative and possibly unofficial sanctions may be applied against offenders as a form of stigmatization instead of criminalization. On the other hand, when first-level enforcers are indifferent to norms and higher-level enforcers wish to uphold them, the offenders are still likely to be identified and convicted where possible. When none of the authorities care about norm violations, legal steps are unlikely to be taken. This outcome suggests that a social norm no longer exists, or laws are designed without the intention of enforcing them.

The third premise relates to the belief that, once conflict begins, opposition resistance only serves to provoke a response from authorities. Consistent with the first and second premises, authorities must care about the norms violation. Such a response

asserts the legality of the norm or, when criminalization is uncertain, it redefines power structures in favor of authorities.

The fourth premise states that when authorities are more powerful than the opposition, they will seek to criminalize them. Power is defined as access to resources such as knowledge and legal recourse. However, when the power differential is overwhelmingly in favor of the authorities, authorities may seek to avoid criminalization. To do otherwise may cast offenders as moral champions. When there is no noticeable power differential, criminalization will be abrogated in favor of a simple fight for survival.

The fifth premise refers to the realism of moves made by conflict parties. For opposition parties, some moves are considered to run counter to their interests. These include increasing the visibility of an offence, making an offence more offensive, taking any action that unites various enforcers, and yielding power to enforcers. Similarly, authorities should avoid actions that appear to bully the opposition by enforcing deference, and any move away from legal procedures. Furthermore, authorities who add negative attributes to opposition during conflict risk increasing support for the opposition parties.

PRIOR RESEARCH

Previous Studies of Turk's Theory of Conflict

Lanza-Kaduce and Greenleaf (1994) consider the process of applying Turk's norm resistance theory to police-citizen encounters. To explain the interactions between police and citizens in field encounters, the authors review prior research and derive hypotheses for each of Turk's concepts.

For example, norms of deference are operationalized by specifying that, according to extant police literature, citizens will defer to police officers on the basis of an officer's age, gender, and race. Thus, Lanza-Kaduce and Greenleaf hypothesize that "norms of deference will be more likely to give way to overt conflict when authority figures are young, black, and/or female" (1994:612). With respect to the realism of moves, Lanza-Kaduce and Greenleaf propose that police decisions to wait for assistance before affecting an arrest are indicative of the sophistication of authorities. Therefore, "the incidence of norm resistance will be higher when arrests are made alone and without backup" (1994:618).

Lanza-Kaduce and Greenleaf's work shows that Turk's theory can be used in analyses of conflict. Moreover, in a second paper the authors empirically test how deference is a predictor of conflict during police-citizen encounters. In so doing, they defy a common criticism that conflict theory is too abstract to be tested and so it instead relies on unproven assumptions (Beirne & Messerschmidt, 1995). Data were collected from 137 police incident reports on domestic disturbance calls in Charleston, South Carolina, submitted from January 1, 1988, through December 31, 1991. Each incident involved a male reporting officer and a male suspect, and there was some opportunity for

the citizen to resist the officer. Given the age (younger than 30 years, or older) and race characteristics (white, or non-white) of both individuals, a matrix was employed to predict whether the officer's positional authority would be reinforced or reversed.

The study results indicate that in 17 (68%) of 25 cases citizens were correctly predicted as overtly resisting an officer. Yet, in 26 (36%) of 73 cases where positional authority should have been reinforced, resistance still took place. Nevertheless, in a model using reinforcement/reversal of authority to predict norm resistance, operationalizations of sophistication, organization, and deference were found to be significantly related to overt conflict (Lanza-Kaduce & Greenleaf, 2000).

Other conflict perspectives have also been successfully scrutinized. In a qualitative study of the Revised Penal Law of New York State made effective in September 1967, Roby (1969) highlights how political processes shape crime. In particular, her analysis focuses on Article 230, which addresses prostitution, and the implications of moving away from its 1909 incarnation. As readers learn, two aspects of the redrafted law provoked controversy. First, patrons soliciting prostitutes were to be subjected to the same legal sanctions as individuals convicted of prostitution. Second, prostitution was deemed to be a violation rather than a crime. In both cases arguments were advanced to encourage prevention rather than prosecution of prostitutes by equally treating customers and prostitutes alike. This perspective conflicted with previous interpretations of the law which had led to the exclusive targeting of prostitutes by police vice-squads.

With the passing of the new law, a range of responses were exhibited by businesses and civil rights groups, judges, police, and politicians. Ultimately the law was

upheld despite many criticizing its leniency. However, Roby notes that power shifted from one interest group to another and each had an awareness of how various actions influence the formation and enforcement of law. Moreover, actors recognized how actions affected their interests leading them to garner support through public appeals. Roby concludes that "numerous efforts on the part of a relatively small number of interested groups...affect the behavior of other men" (1969:109).

Work by Hagan (1974) examines factors that lead to discrimination in sentencing. The author, having concerns about the findings of earlier judicial studies, uses data from seventeen research articles to recalculate rates of statistical significance. In so doing, Hagan hypothesizes that courts in the United States use extra-legal variables to affect sentence outcomes.

The study results suggest that only a small relationship exists between extra-legal attributes and judicial decisions. Differences did appear in judicial sentencing for inter-racial, capital cases in southern states and social class was related to the outcome of capital cases in non-southern states. However, when attempting to explain the statistical variance, knowledge of the independent variables only increased the prediction of sentences marginally.

In another study of inequality and judicial sentencing, Chiricos and Waldo (1975) explore the relationship between a defendant's socioeconomic status and the severity of prison sentences received. The dataset included admissions summaries provided by adult correctional facilities in North Carolina, South Carolina, and Florida from 1969 to 1973. This yielded 10,488 inmates found guilty of committing any of seventeen specific criminal offences.

However, the research findings indicate that socioeconomic status (education, income, and occupation), the offender's age, previous criminal record, race, and the rural/urban character of the sentencing county had little bearing on sentence length. Chiricos and Waldo conclude that conflict theory fares no better at predicting the demographic characteristics of convicted offenders than other criminological models because

> The fullness of conflict theory in sociology encompasses a host of issues (e.g., alienation, capitalism, social change, ideological development, etc.) that transcend the limited matters of criminal justice (1975:770).

Finally, Jacobs and Britt (1979) use conflict theory to investigate inequality and police killings in the United States. The study rationale suggests that power is derived from comparative differences in resources and those with fewer resources are less able to protect themselves from the threat of state coercion. Therefore, the authors hypothesize that economic inequality and the amount of deadly forced used by police officers are directed related.

For their analysis, Jacobs and Britt use a mixture of publicly available statistics and independently collected figures. Results show that the number of African Americans living in a state, economic inequality, a state's violent crime rate, and population change are all linked to police-caused homicides. However, when controlling for each competing factor, the unequal distribution of economic resources best predicts the use of lethal force by police. As such, "a pluralistic model of the state which ignores differences between the haves and have-nots is incorrect" (Jacobs & Britt, 1979:410).

From this review, we find that previous studies have used a variety of approaches to explore conflict in society. Although the findings are mixed, concepts like inequality and power, and the politicization of crime have been successfully explored. However, while conflict theory has been applied in criminal justice contexts such as policing and sentencing, no one to date has examined how Turk's ideas relate to organizational discretion and the criminalization of network intruders.

Previous Studies of Network Intrusion

Donn Parker draws attention to the challenges of studying networked crime when he writes,

> Few researchers have attempted serious work on this subject because valid information is difficult and expensive to obtain. The principal source of information is from the cases that have been discovered *and* in many instances publicly reported (1983:14).

A major problem is public reports are scarce. In the Land of the Free there is no such thing as mandatory reporting. While the Federal Bureau of Investigation's Uniform Crime Reports are publicly available, the Bureau cannot force local agencies to participate (Maltz, 1999). Furthermore, the Reports do not include an index for computer crimes (Goodman, 1997). Consequently, studies that do focus on computer crime tend to use data compiled from surveys administered to victims. This trend is evident in the following description of research focusing on networked computer crime and network intrusion in particular.

With an emphasis on computer security, Carter and Katz (1995) raise three important issues at the beginning of their work. First, the computer environment changes

extremely quickly and as a result prior research becomes dated. Second, while it is difficult to discover and record network incidents, accurately assessing the monetary value of lost data is a harder task to perform. Third, earlier exploratory studies indicate that in the same way retail stock is mostly stolen by employees, threats to computer security are generally posed by workers with knowledge of internal systems.

To establish levels of victimization, the identity of network intruders, and common protection strategies, Carter and Katz use a purposive sample of the American Society for Industrial Security (ASIS) membership. Restricting themselves to residents in the United States, the authors randomly selected 600 security members from whom 151 (25%) responded. Analysis of the responses show that almost all (98%) of the respondents had been victimized and nearly half (43%) had been victimized more than twenty-five times. Furthermore, while most of the respondents indicated that insiders were to blame for attacks, a growing proportion of attacks came from outside of member organizations. Finally, of the security responses intended to reduce incidents of networked crime, most strategies placed more emphasis on technical issues rather than human factors.

To better understand crimes involving networked computers, the Computer Security Institute (CSI) and the Federal Bureau of Investigation undertook a collaborative project from 1996 through 2002. Each year a survey was administered to some 3,500 corporations and government agencies in the Unites States. 503 responses (14%) were received for 2002 and the findings made publicly available highlight a number of issues related to network intrusion.

Firstly, the number of networked computer incidents reported in the survey is increasing. In 1996, 46% of respondents indicated that they had been the victim of at least one (but less than six) incidents. This figure peaked in 1998, at 61% of respondents and dropped to 34% in 1999. In 2002, survey results suggest that 42% of participants had been victimized.

Secondly, the costs incurred by network incidents have also increased. However, unlike the number of incidents occurring, costs have risen consecutively. In 1997, the total losses of respondents accounted for 20.0 million dollars. By 2002, this figure had risen to 170.8 million dollars. Average annual losses for respondents also increased consecutively, from 0.9 million dollars in 1997 to 6.6 million dollars in 2002.

Thirdly, in 2002, 49% of victims indicated that incidents involved a perpetrator from outside the organization. This figure is the second-highest behind that of 1998, then 74%. When asked who they thought was most behind attacks, 82% of respondents believed hackers committed networked crimes. Additionally, only 14% of respondents said their organization would consider hiring reformed hackers as consultants.

Fourthly, reporting of intrusions remains relatively low. From 1996 through 1998, only 17% of respondents reported network incidents to the police. In 2000, this figure rose to 25%. A year later 36% of respondents approached law enforcement agencies. In 2002, reporting dropped to 34% (CSI, 2002:20-21). The leading reasons for not reporting included a fear of "negative publicity" and that "competitors would use to advantage" (CSI, 2002:21) knowledge of security breaches.

Thompson (1997) adopts a similar line of enquiry in order to establish trends of computer crime in Australia. Working with the Victoria State Police, Thompson sent

surveys addressed personally to information technology managers working at companies selected randomly from the Business Review Weekly's Top 500 list and the Australian Securities Commission's register. Added to this sample were organizations selected from government departments, internet service providers, state transit/transportation authorities, and universities. In total, 310 surveys were mailed out and 159 useable responses (51%) returned.

Thompson's descriptive analysis shows that most organizations (20%) participating in the study had between 1001 and 2000 employees. Moreover, a vast majority (71%) had annual turnover exceeding 250.0 million Australian dollars. 82% of respondents had access wide area or global area networks. 95% of those replying had access to the Internet with 43% having a direct/permanent connection.

In terms of organizational guidelines, 75% of respondents either had a policy detailing the misuse of computer facilities or were in the process of writing one. 54% of the organizations had a policy explaining how to respond to network intrusions and, of these, 50% of these listed sanctions in the policy document and only 23% included provisions for notifying law enforcement agencies. Additionally, 25% of all respondents said they had a policy document describing how evidence of network incidents should be preserved. Only 19% of organizations claimed most of their employees had a working knowledge of current laws on the misuse of computer systems.

When detailing security incidents, 54% of respondents said that the organization had suffered from unauthorized use of computer systems within the last year. The majority (61%) of these incidents numbered five or less. Asked how many of the incidents were from outside the organization, 23% of the total sample group said

outsiders were involved. 33% of all respondents said that insiders were involved in security incidents. 77% of organizations indicated that computer misuse cost 10,000 Australian dollars per incident. The most likely source of security breaches was the disgruntled employee (32%) followed by criminals/hackers (21%).

Finally, the majority of respondents (41%) who had experienced a network intrusion said that they responded by patching security holes. 20% of organizations said they reported the incident internally but another 19% said they contacted a law enforcement agency. The most important reasons for not reporting an incident included internal disciplinary measures taken instead (33%), civil remedy a better option (15%), and fear of wasting time pursuing a claim (12%). Asked for the circumstances under which they would report a network incident, the leading answers were if the incident was detected immediately (30%), a chance of successful prosecution (23%), and a chance of recovering losses (21%). Given an opportunity to receive information on computer crime from law enforcement, 96% of respondents indicated they would find this action useful.

In summary, prior studies suggest:

- Networked crime is a significant problem for organizations
- The proportion of attacks perpetrated against organizations by outsiders has increased
- Law enforcement agencies tend not to receive reports from organizations about network security breaches.

PRESENT STUDY

The purpose of this study is to see how organizations respond to incidents of network intrusion. Rather than simply assess the prevalence of cyber crime, it is important to establish whether network intrusion can be explained in a criminal context. As detailed earlier, one question arises: *what decision-making process takes place within organizations that shapes their responses to network intrusion?*

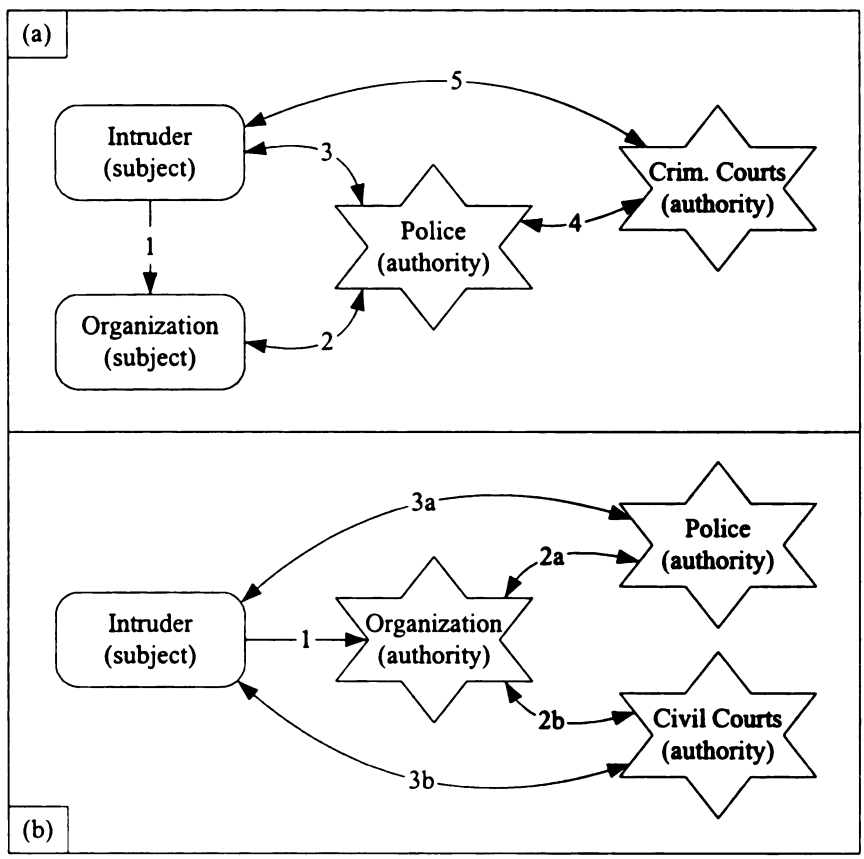
To address this item, Turk's Theory of Norms Violation is operationalized to test its ability to explain and predict outcomes for cases of network intrusion. The choice of theory is grounded upon a firm belief that organizations are not solely disadvantaged by crime, but that they are also empowered by it. Turk's Theory is one that moves away from using a perpetrator to explain why crime occurs. More pragmatically, prior research shows that no one knows with any degree of certainty who and what hackers are. The limit of our knowledge is whether individuals who misuse computer systems have legitimate access to organizational resources or not.

However, personal convictions are not conceived in a moment. Formal and informal studies of research material including academic journals, news media publications, and on-line resources have shaped my views of cyber crime. Moreover, experience gained from working as a computer professional in private and public organizations, and discussions with attorneys and police investigators have helped me to better understand the issues, both legal and technical, associated with networked crimes.

For completeness, the study's null hypothesis is formally stated as follows: the observed difference between organizations that seek the criminal prosecution of network intruders and those that do not is the result of chance variations associated with the

random sampling process. Consequently, cases of network intrusion follow a standard chronology of events, as shown in Figure 2(a), whereby victimized organizations initiate criminal investigations through interaction with the police.

Figure 2. Two perspectives of participant roles in cases of network intrusion



In contrast, this study hypotheses suggest that decisions made by organizations to pursue cases of network intrusion conform to Turk's five conflict premises. Here, incidents of network intrusion follow a pattern that casts organizations as authorities, effectively first-level enforcers, rather than subjects. Figure 2(b) shows this alternative perspective, whereby organizations may seek to conduct their own private investigations,

identify the perpetrator of an intrusion, collect evidence using their own resources. At this point, organizations may then appeal to higher-level authorities such as police to punish offenders (2a), or instead stigmatize hackers by taking civil action against them (2b).

Hypothesis 1

The first hypothesis explores the concept of cultural difference between authorities and subjects. For subjects, the mechanics of network intrusion clearly show that individuals external to an organization do not accidentally access an internal system. In this situation, the act of establishing a connection to a computer server and then attempting to copy, examine, modify, or remove any part of a file constitutes computer misuse. Similarly, attempts to attack computer resources only serve to highlight a hacker's propensity to behave in a malicious manner. Therefore, it shall be assumed that unauthorized access to computer systems is incongruent with norms that address their legitimate use.

In contrast, Turk's Theory suggests an authority that enforces a norm will defend its legitimacy through thought and deed. This principle can be applied to network intrusion by using an organization's willingness to uphold general laws to then predict their desire to criminally prosecute hackers. Thus, we hypothesize that there is a direct relationship between organizations' support for domestic laws and the criminalization of hackers.

For hypothesis 1, the independent variable will be a mean score derived from the responses of each organization to four attitudinal questions:

- "The organization strongly believes in the laws of the land (both criminal and civil)"

- "The importance of criminal and civil laws are reflected in the contracts drawn up during the course of business"
- "The organization enforces contractual agreements and rules regarding employee behavior in equal measure"
- "The organization views hackers as individuals who violate laws that protect the whole of society."

Hypothesis 2

Turk's second premise seeks to explain how the offensiveness of a violation influences authorities' responses. As previous research shows, there are a number of ways that a network intruder can victimize targets. Accessing, modifying, removing, or stealing data, along with attacks that leave systems unavailable are all outcomes of network intrusion. However, a good measure of the offensiveness of a network violation is the amount of damages incurred by a victim. While one can query whether the copying of files really does constitute theft, or whether the removal of files is more serious that their illicit transferal, damages represent a tangible loss. For example, organizations are able to calculate the costs of a critical system rendered non-functional by an intrusion. Similarly, fees will be paid to workers in order to restore systems. Finally, damages are unlimited in their scope since they can range from zero dollars upwards.

Using this operationalization, Hypothesis 2 states that organizations that incur heavy costs from network intrusion will be more likely to criminalize hackers than those that suffer little or no financial loss. Organizational responses to the question, "On average, what is estimated cost of damages caused by each hacking incident?", will be used for the independent variable.

Hypothesis 3

Turk's theory also places great weight upon the determination of subjects to oppose legal norms. It may not be enough that hackers render critical systems unusable or that they steal valuable data. Hackers may also pursue the same targets whose networks they have already infiltrated and victimize them further. Moreover, they may launch separate intrusions from computers in compromised networks with the result that their owners are implicated in a hacker's cyber crimes.

Hypothesis 3 addresses this situation and proposes that organizations who encounter persistent network intruders will be more likely to seek criminal sanctions. The independent variable used for this test will be a mean score derived from organizational reaction to three attitudinal questions:

- "The organization views hackers as individuals who violate laws that protect the whole of society"
- "The police and courts consider hacking serious, and actively seek to bring culprits to justice"
- "Persistent hackers do spark a response."

Hypothesis 4

The fourth hypothesis explores how the power differential between authorities and subjects affects the criminalization process. Turk defines power in terms of access to resources but says little more. Consequently, researchers have a great deal of discretion when it comes to operationalizing this construct. In the case of network intrusion, a potential measure of power includes money because this resource empowers individuals. For example, if one is unsure how to respond to hackers, independent advice can be

sought and purchased. In turn, hackers who have been arrested can also use money to pay for legal counsel.

However, this interpretation is too simplistic for two reasons. First, not all organizations are profit-making entities and a question such as "What is the annual turnover of the company?" has little relevance to an organization that provides public services. Moreover, the assumption that any or all organizations budget exclusively for network intrusions appears tenuous given how many prefer to respond by simply patching security holes (Thompson, 1997). Second, money has less conceptual relevance once a case enters the criminal justice system because the state carries the costs involved with investigations and court proceedings.

A better measure of power is the size of a party. An organization with a large number of employees is likely to have many resources, if only enough to pay and physically house them. A group of subjects also benefits from greater size because, as Turk himself points out, they use collective support to resist criminalization strategies. Therefore, hypothesis 4 posits that an organization's willingness to convict hackers is directly associated with the number of members the organization has. The independent variable to be used will encompass responses for the question, "Approximately how many workers are employed by the organization?"

Hypothesis 5

Turk's last premise explains how the realism of moves influences conflict outcomes between authorities and subjects. In particular, a party that strives to reach a favorable position must act prudently. Anonymity in cyber space and the global scope of computer networks offers hackers an excellent opportunity to avoid detection. If intruders

wish to avoid the attention of authorities, they will do their utmost to protect their true identities by concealing evidence of their activities and committing crimes outside their jurisdiction.

In a similar fashion, organizations that wish to uphold norms discouraging computer misuse must employ sophisticated tactics. One method involves closer liaison between authorities. For example, in order to promote a united front, organizations will work with police and public attorneys to stay abreast of new laws and procedures that will assist efforts to convict hackers.

Therefore, hypothesis 5 maintains that organizations that liaise with law enforcement agencies, rather than organizations that do not, are likely to criminalize network intruders. The independent variable will again be a mean score derived from the responses to three attitudinal questions:

- "If police encourage representatives to report an incident, the organization will be more willing to report"
- "The organization has had positive working relationships with the police before"
- "If a prosecutor states that the courts will treat hackers harshly, the organization will be more willing to pursue a criminal prosecution."

Table 1 summarizes the variables that will be used in the study hypotheses, along with their measurement scales. For each hypothesis, the same dependent variable will be used and it relates to the extent an organization agrees with the prosecution of network intruders. The exact wording of the survey question is, "Hackers should be criminally

prosecuted", with participants indicating that they either strongly agree, agree, disagree, or strongly disagree.

It is anticipated that a mixture of statistical techniques will be used to test hypotheses 1 through 5. An analysis will begin with a descriptive, univariate analysis of participant responses. Given that many items incorporate a four-point scale, a mean score will be calculated for all questions conforming to this pattern. A factor analysis and reliability test will also be performed to establish each scale's consistency.

Table 1. List of proposed variables for testing the study hypotheses

Variable	Variable name	Measurement
Y	Criminalize	Ordinal
X_{H1}	Cultural congruence	Ordinal
X_{H2}	Offensiveness	Ratio
X_{H3}	Resistance	Ordinal
X_{H4}	Power	Ratio
X_{H5}	Sophistication	Ordinal
$Control_1$	Victimized by hackers	Nominal

To assess the bivariate relationship between independent variables, a cross-tabulation will be included to compare predicted and expected counts among variables. Moreover, a Chi-Square statistic will be calculated to see how unlikely observed values are if the null hypothesis is true.

Finally, multivariate logistic regression will be performed to test each hypothesis. The purpose of this exercise will be to control for another variable, prior victimization by hackers, since organizations that have never suffered a network intrusion may have a more idealistic view of taking action against hackers than those who have been victimized. The dependent variable will be coded so that an organization either supports criminalization or it does not. One tail significance tests, using a 95% confidence interval, will be used to determine if the study hypotheses have any relevance to network intrusion.

Data

The units of analysis for this study are organizations, private and public, that operate in Michigan. Organizations are identified for the study because they represent significant targets for hackers, as established in previous research (Carter & Katz, 1995; CSI, 2002). Furthermore, the State of Michigan, replete with a criminal justice system geared towards combating network intrusion (State of Michigan, 2003b), is home to a variety of organizational interests.

Demographic estimates suggest that there are 9.9 million residents living in Michigan. As outlined earlier, Michiganders are employed in a range of industries including construction, education, farming, health care, hospitality, mining, professional services, public administration, trade and transportation. Of these sectors, the largest employers tend to be providers of hospitalities, manufacturers, and retailers with 0.3 million, 0.8 million, 0.5 million workers respectively. Local government workers also number 0.3 million (U.S. Census Bureau, 1997a; U.S. Census Bureau, 1997b).

Instrument

A questionnaire, detailed in the Appendix, has been generated to gather data for testing the study concepts. There are two dimensions to the instrument. Firstly, questions are asked to ascertain the prevalence of network intrusions discovered by organizations in Michigan. Responses received will also enable a comparison of data for Michigan with national findings from the CSI study. In this way, the study will provide a general impression of Michigan's experience of hacking activities.

Secondly, the survey asks about organizational responses to network intrusion. Since this theme is integral to the study, the majority of the questions fall into this category. Moreover, the questionnaire was designed to specifically measure organizational attitudes towards hacking. However, rather than simply obtain answers that state, "we believe X and we do Y", the questions are also intended to uncover why X is a core belief and why Y is done.

Hacking is a sensitive issue for victims. Organizations that have lost data or suffered systems unavailability often do not want reports to circulate in the public domain. Previous research studies support this view (Carter & Katz, 1995; Thompson, 1997; CSI, 2002). Therefore, the instrument begins with an introduction outlining its purpose, that is to assess the impact of hacking upon organizations in Michigan and how those organizational responses affect the state's legal system.

The instrument is comprised of sixty-seven questions. To more effectively organize the instrument, seven sections are listed with a name and a brief description of what the section questions attempt to examine. The first section seeks to collect demographic information about the organization including details such as what the

specialization of the organization is, whether it is profit-making or not, and where it is located.

The second section briefly asks about the scope of the organization's computer network resources and who manages them. The section does not focus on the specific nature of the technology as questions that do might be misconstrued as being intrusive. However, of interest is whether an organization has an open, public-facing network, a key factor when seeking to analyze how organizations view network intrusions. Another item, omitted by previous studies but queried in this survey, asks if computer resources and computer security is managed by groups internal to the organization or external to it.

The third section seeks to establish how frequently the organization has suffered from network intrusion. The severity of intrusions is categorized by the actions taken by hackers, namely modification, theft, and attack. The remaining items deal with unavailability of systems and the average cost of damages caused by a network intrusion.

The fourth section briefly asks if organizations describe how investigations of network intrusion should be investigated and how digital evidence should be handled. It is worth noting that Thompson (1997) also asks these questions with a view to highlighting if an organization details internal protocols. Finally, the section asks if senior management actively participate in the investigation decision-making process. The answers to this question should prove interesting because it will indicate the extent that the upper echelons of management are aware of network intrusion and have personal discretion to "hush things up".

The fifth and longest section addresses an organization's preference for criminal or civil legal action. All of the major studies have focused on this subject but the

questions asked here explore organizational perceptions of hackers, litigators, prosecutors, police, and the media. Additionally, respondents are asked about the importance of laws within the organizational context. This item is extremely important for evaluating Turk's Theory of Norms Violation. The answers presented to the study participants take the form of a four-point scale (Strongly Agree, Agree, Disagree, Strongly Agree). This approach was chosen instead of a five-point scale because of a conscious desire not to see surveys completed with "undecided" answers.

The sixth section studies the organizational perceptions of how government and industry liaise to reduce network intrusion. A range of issues are covered including views about the appreciation other entities have of network intrusion, the sharing of information between law enforcement groups and organizations, and state policies addressing cyber crime. In short, this section intends to offer some insight into what strategies might better improve responses to network intrusion in the future.

The seventh section consists of attitudinal and categorical questions. Organizations are asked who they believe hackers are, if hackers are becoming more skilful, what type of intrusion is considered most serious, and what type of networked crime is most likely to provoke a legal response. Finally, participants are asked if they agree with a wide range of statements that summarize their views of hacking.

Method

That organizations are not single entities, but instead consist of people, creates an obstacle to the acquisition of data for this study. Organizations cannot articulate why its representatives take certain actions. Of course, organizations can release statements that explain what those actions should be but they have no voice to explain the rationale for

the creation of these directives. Therefore, in order to study organizational responses to network intrusion, it will therefore be necessary to interview members of target organizations.

One method for generating a study population is purposive sampling. This technique involves the specific selection of cases on the basis that a study is exploratory, or there is limited access to research data. In other words, "a researcher may use purposive sampling to select members of a difficult-to-reach, specialized population" (Neuman & Wiegand, 2000:198).

Using purposive sampling to gather study data, members of the American Society for Industrial Security (ASIS) International were surveyed and data collected about the organizations for which they work. ASIS International has a membership of approximately 33,000 professionals who are responsible for security matters. These individuals include managers and directors of security, along with consultants and other specialists such as architects and attorneys (ASIS, 2003). Member addresses are listed in the publication "Dynamics", which is updated and distributed annually.

Sampling of members living in Michigan, as listed in the ASIS International directory released during May 2003, involved checking every job title. Only those persons who were listed as "Coordinator", "Director", "Manager", or "Supervisor" and held positions that related to "Investigations", "Prevention", "Protection", "Safety", and "Security" were included in the final sample. Duplicate members of organizations were then removed from the newly created list, so that only one response could be received for an organization. Furthermore, officials from police or public safety organizations were taken out of the sampling frame.

However, this process dramatically reduced the total study population. Therefore, in order to create a contingency for a low number of responses, data were also collected for a second population. A random sample was generated of organizations listed in the "Michigan Business Directory 2003." The Michigan Chamber of Commerce (MCC) produces this information resource annually and it includes more than 37,000 organizations that maintain professional links with the Chamber. As with the ASIS sample, the final MCC sample, which consisted of 296 organizations, was checked to ensure that duplicate entries were removed.

Once the two sample lists were ready, study subjects were sent a copy of the survey instrument, along with a return envelope that has postage paid. In the case of ASIS members, each letter was addressed personally. In the case of the MCC sample, letters were addressed to the "Director of Security." Regardless of which sample they came from however, subjects were invited to participate in the study and asked to respond within two full weeks of receiving the questionnaire. After two weeks had passed, individuals for whom no response had been received were sent a reminder asking them to send their instrument within the week. Five weeks after the original dispatch, the study was closed.

Of 148 ASIS members sent letters, 3 letters were returned undeliverable and 19 usable responses were received. Therefore, the response rate for ASIS members was 13 per cent. In the case of MCC subjects, 129 letters were returned undeliverable and 10 usable responses were received. This exercise yielded a response rate of just six per cent. Consequently, it was decided that the MCC sample should be dropped from the study. Next, a fifth of ASIS members choosing not to respond were randomly selected for

follow-up telephone calls. Of 25 calls made, 24 hit secretaries or voice-mail. Messages were left stating the reason for contact and a request made of the subject to return the call at the individual's earliest convenience. Subsequently, 3 calls were returned from subjects who explained that two individuals had changed jobs since May and one felt unqualified to complete the survey. For the single call that was collected, the non-respondent agreed to complete and return the survey. This survey remains pending. Finally, the 19 responses collected for the ASIS sample were coded for analysis.

STATISTICAL ANALYSES

Descriptive statistics

Before formally examining the study hypotheses, the findings section of this report begins with a summary of data values. Tables 2 through 6 focus solely on univariate statistics, in particular the general characteristics of study participants. Attitudinal responses are also described.

In Section 1 of the survey, participants were systematically asked to describe the organization employing them. Answers to four questions are shown in Table 2.

Table 2. General Characteristics of ASIS Respondents (N=19)

Demographics	N=	Percentage*
Core specialization		
Professional services	4	21.1
Retail	3	15.8
Manufacturing	4	21.1
Engineering	1	5.3
Education	2	10.5
Research	1	5.3
Other	4	21.1
Organizational goal		
Profit	12	63.2
Non-profit	6	31.6
Number of workers		
0-100	2	10.5
101-1000	9	47.4
1000+	8	42.1
Years of operational life		
0-3	1	5.3
11+	18	94.7

* Missing cases not reported

First, a range of specializations was represented in the study with the largest being manufacturing (21%) and health, financial, or legal services (21%). Engineering (5%) and research (5%) organizations were the least common. Second, profit-making organizations (63%) appeared twice as much as non-profit organizations (32%). Third, most organizations (90%) employed more than a hundred workers. However, this statistic does not capture the large range of responses. For example, the smallest organization had three workers while the largest organization employed more than sixty-eight thousand individuals. Fourth, almost all of the respondents (95%) indicated that their company had been operating for eleven years or longer.

In Section 2, participants were asked about the extent of computer usage by their organization.

Table 3. Computer Usage Characteristics of ASIS Respondents (N=19)

Demographics	N=	Percentage*
Extent of computer resources		
Intranet	2	10.5
Intranet, Internet	17	89.5
Organization website		
Yes	19	100
IT management		
Internal group	12	63.2
Internal, Contractors	7	36.8
Responsibility for computer security		
Internal group	12	63.2
External contractors	1	5.3
Internal, Contractors	6	31.6

* Missing cases not reported

Table 3 shows that all organizations were reported to have a computer network and most (90%) had access to the Internet. Similarly, all respondents stated that their organization has a website. With respect to the management of computer resources, the majority of organizations (63%) assigned responsibility to an internal IT group and the remainder (37%) complemented their IT group with external contractors. Computer security was generally managed by an internal IT group (63%), though sometimes by external contractors (5%), or a mixture of IT workers and contractors (32%).

In Section 3, questions were asked about participants' victimization by hackers. Most respondents indicated that they were not aware of data modification (53%) or data theft (58%), but network attack (68%) was common, as highlighted in Table 4.

Table 4. Incident History Characteristics of ASIS Respondents (N=19)

Demographics	N=	Percentage
Times hackers modified data		
Never	10	52.6
Once	1	5.3
2-10	2	10.5
25+	3	15.8
Times hackers stole data		
Never	11	57.9
Once	1	5.3
2-10	1	5.3
25+	3	15.8
Times hackers attacked network		
Never	6	5.3
Once	1	31.6
2-10	2	10.5
25+	4	21.1
Systems rendered unavailable		
Yes	1	5.3
No	15	78.9

Of those organizations victimized, respondents said that had data modified (16%), data stolen (16%), or had their network attacked (21%) twenty-five times or more. Few respondents (5%), however, indicated that network intruders rendered key systems unavailable. The question omitted most in the survey also came from this section, with most victimized organizations choosing not to state an average cost of damages caused by each intrusion.

In Section 4, questions were asked about how organizations respond to incidents of network intrusion.

Table 5. Investigations Characteristics of ASIS Respondents (N=19)

Demographics	N=	Percentage
Investigation guidelines		
Security group	2	10.5
IT group	2	10.5
Both	11	57.9
No policy	4	21.1
Evidence guidelines		
Yes	10	52.6
No	9	47.4
Participation by senior management		
Yes	14	73.7
No	4	21.1

Table 5 shows that most organizations (79%) had guidelines indicating who should investigate a suspected hacking incident. This figure was formed mainly by those organizations (58%) with guidelines instructing both their I.T. and security groups to jointly investigate hacking incidents. When asked about the collection and preservation of

digital evidence, approximately half of the respondents (53%) said that their organization had protocol guidelines. Finally, the majority of organizations (74%) were said to have senior management who actively participate in investigation decision-making.

Four questions from the Summary Section centered upon the overall organizational perspective of network intrusion.

Table 6. Summary Characteristics of ASIS Respondents (N=19)

Demographics	N=	Percentage
Hacker profile		
Ex-employees	5	26.3
Current employees	1	5.3
Overseas hackers	1	5.3
Juveniles	9	47.4
Other	2	10.5
Hackers more skillful		
Yes	17	89.5
No	2	10.5
Offence most serious		
Attack	4	21.1
Data theft	9	47.4
Data modification	5	26.3
Action likely		
Attack	3	15.8
Data theft	12	63.2
Data modification	3	15.8

Table 6 summarizes responses to these questions. First, participants were asked who organizations thought hackers were. Juveniles (47%) were most commonly marked out as network intruders, followed by ex-employees (26%). Second, most respondents (90%) believed that hackers are becoming more skillful. Third, a majority of organizations

(47%) treated data theft as the most serious hacking offence. Similarly, data theft (63%) was commonly cited as the offence that organizations were most likely to take legal action for.

Forty-five of the survey questions asked respondents to what extent they agreed or disagreed with statements about cyber crime, hackers and the actions of legal authorities in Michigan. Divided into separate sections, the responses to these attitudinal questions provided much of the data for hypothesis testing.

To create a scale for each section, the answers provided were recoded so that they were unidirectional in nature. For example, answers to the statement, "Hackers evade justice because they are able to mount a strong legal defense," were reversed so that agreement became disagreement and vice-versa. Consequently, the initial statement was logically negated and became positively framed in line with other questions, "Hackers do not evade justice because they are able to mount a strong legal defense."

After recoding, factor and reliability analyses were performed (see notes in Appendix B). A factor analysis is used to determine those variables that explain most of the variance in a group of responses. In this way, factors with high loading values can be used for further analyses, including hypothesis testing, while extraneous variables are ignored. A reliability analysis attempts to establish whether a scale is internally consistent. When a high reliability score is calculated, survey items successfully measure the concept they are intended to capture.

The mean response for questions in Section 5 was 1.92. This meant that on average respondents agreed with the survey statements describing legal actions taken by different actors - criminal courts, litigators, the media, offenders, prosecutors, and the

respondent's organization - with respect to network intrusion. The reliability score for the scale was high (Standardized Alpha = .7707). Items with noticeably high factor loadings included the organizational belief that hackers do not evade justice because they offend from outside the United States (.670), that hackers do not evade justice because they are able to mount a strong legal defense (.873), and that hackers do not evade justice because the organization lacks resources with which to pursue a conviction (.732).

Answers to questions in Section 6, which covered government and organizational responses to network intrusion, yielded a mean score of 2.84. This figure falls between agreement and disagreement on a four-point response scale, and it indicates respondents tended to have a negative opinion about the efforts of government and organizations to reduce cyber crime. Additionally, the reliability score for this section was the lowest of all three attitudinal sections (Standardized Alpha = .5095). Two items, government agencies trust partnerships (.692) and government agencies want partnerships (.647), had higher factor loadings than other questions.

The Summary Section of the survey closed with attitudinal questions about the overall perceptions of organizations towards hacking. For example, participants responded to statements touching upon items such as organizational trust of police and the priority the organization ascribes to recovering damages caused by hackers. The mean response for the section was 2.06 and the reliability score for the scale was slightly below 0.6 (Standardized Alpha = .5837). Results from the factor analysis show the items, the recovery of damages as a priority (.602) and the organizational response to hacking depends on the severity of the offence (.624), explained most of the variance in summary item responses.

Finally, secondary factor and reliability analyses were performed upon item means combined specifically to form independent variables measuring Turk's concepts. Table 7 shows the results of the factor analyses for each of three new scales.

Table 7. Factor Analysis for Sub-Scales (N=19)

Concept	Loading	Mean	S.D.
Cultural congruence			
Belief in laws	.876	1.16	0.38
Contracts reflect laws	.958	1.21	0.42
Rules enforced equally	.705	1.26	0.56
Organizational view	.445	1.53	0.51
Mean = 1.29; Standardized Alpha =.7494			
Resistance			
Organizational view	.853	1.53	0.51
Authorities serious	.891	2.16	0.77
Persistent hackers	.448	2.11	0.81
Mean = 1.93; Standardized Alpha =.5978			
Sophistication			
Reports encouraged	.786	1.89	0.57
Good police relations	.708	1.37	0.60
Harsh prosecutions	.492	1.95	0.52
Mean = 1.74; Standardized Alpha =.3847			

First, cultural congruence was found to have a mean score of 1.29, or close to strong agreement with survey statements. The reliability score for the scale was strong (Standardized Alpha = .7494) and there was only one factor loading, the organizational view of hackers (.445), below .75. Second, resistance had a mean score of 1.93 and a reliability score just below 0.6 (Standardized Alpha = .5978). One item, persistent hackers spark response, had a factor loading (.448) much lower than other scale items. Third, the mean response calculated for sophistication was 1.74. The reliability score for

the scale was also found to significantly lower (Standardized Alpha = .3847) than those of cultural congruence and resistance. Moreover, like resistance, sophistication also had one item, seek to prosecute if harsh sentence, with a noticeably lower factor loading (.492) than the other scale items.

From a methodological standpoint, items with low factor scores should have been removed from the new independent variables. The reason for this step is that neither item accurately measures the concept, cultural congruence and resistance respectively, as it was designed to. However, in order to maintain consistency with the methodology stated initially and to preserve three-item scales, both variables were retained for bivariate and multivariate analyses.

Bivariate statistics

While univariate statistics focus on single measures, a bivariate analysis examines the relationship between two different variables. It is also possible to test if a relationship between two variables is causal. In other words, do systematic changes in variable X lead to a predictable change in variable Y? The following section compares organizational traits with victimization trends and organizational responses to hacking. Finally, the study hypotheses are exposed to the first of two formal tests.

In order to assess how organizations in Michigan have been victimized by hackers, Table 8 crosstabulates organizational traits by incident history. Figures for incident history consist of binary "yes/no" categories, as opposed to complete frequencies, for data modification, data theft, and network attack respectively. Of these three categories, network attack was reported as the most common network incident.

However, organizations operating for more than eleven years was the only category where network attack was more likely than not (13 yes:5 no). This statistic contrasts with data modification (9:9) and data theft (8:10) for which differences in victimization rates were almost indiscernible.

Table 8. Crosstabulations for General Characteristics of Respondents by Incident History (N=19)

Variables	Modified data		Stolen data		Attack	
	Yes[a]	No	Yes	No	Yes	No
Core specialization						
Services	2 (10.5)	2 (10.5)	2 (10.5)	2 (10.5)	3 (15.8)	1 (5.3)
Retail	0	3 (15.8)	0	3 (15.8)	1 (5.3)	2 (10.5)
Manufacturing	3 (15.8)	1 (5.3)	3 (15.8)	1 (5.3)	3 (15.8)	1 (5.3)
Engineering	1 (5.3)	0	1 (5.3)	0	1 (5.3)	0
Education	2 (10.5)	0	1 (5.3)	1 (5.3)	2 (10.5)	0
Research	0	1 (5.3)	0	1 (5.3)	0	1 (5.3)
Other	1 (5.3)	3 (15.8)	1 (5.3)	3 (15.8)	3 (15.8)	1 (5.3)
Total*	9 (47.4)	10 (52.7)	8 (42.2)	11 (58.0)	13 (68.5)	6 (31.7)
Organizational goal						
Profit	6 (33.3)	6 (33.3)	6 (33.3)	6 (33.3)	7 (38.9)	5 (27.8)
Non-profit	2 (11.1)	4 (22.2)	2 (11.1)	4 (22.2)	5 (27.8)	1 (5.6)
Total	8 (44.4)	10 (55.5)	8 (44.4)	10 (55.5)	12 (66.7)	6 (33.4)
Number of workers						
0-100	1 (5.3)	1 (5.3)	1 (5.3)	1 (5.3)	2 (10.5)	0
101-1000	3 (15.8)	6 (31.7)	2 (10.5)	7 (36.8)	6 (31.7)	3 (15.8)
1000+	5 (26.3)	3 (15.8)	5 (26.3)	3 (15.8)	5 (26.3)	3 (15.8)
Total	9 (47.4)	10 (52.8)	8 (42.1)	11 (57.9)	13 (68.5)	6 (31.6)
Years of operational life*						
0-3	0	1 (5.3)	0	1 (5.3)	0	1 (5.3)
11+	9 (47.4)	9 (47.4)	8 (42.1)	10 (52.7)	13 (68.4)	5 (26.3)
Total	9 (47.4)	10 (52.7)	8 (42.1)	11 (58.0)	13 (68.4)	6 (31.6)

*Missing values not included
a = N (%); Totals may not equal 100% due to rounding

When taking into consideration all types of network incident, organizations specializing in manufacturing (3:1, 3:1, 3:1) and education (2:0, 1:1, 2:0) accounted for the most victimization. However, non-profit organizations (2:4, 2:4, 5:1) were found to be less victimized than their profit seeking counterparts (6:6, 6:6, 7:5). Moreover, organizations with less than a thousand workers experienced fewer network intrusions than the largest collectives, which consistently reported higher incidents of data modification (5:3), data theft (5:3), and network attack (5:3).

Table 9. Crosstabulations for Government-Organization Responses by Business Objective (N=19)

Variables	Profit Making		Total
	Yes[a]	No	
Views of hacking do not differ by sector			
Do not differ	4 (22.2)	2 (11.1)	6 (33.3)
Differ	8 (44.4)	4 (22.2)	12 (66.6)
Law enforcement understands threat			
Understands	2 (11.1)	1 (5.6)	3 (16.7)
Misunderstands	10 (55.6)	5 (27.8)	15 (83.4)
Government agencies trust partnerships			
Trust	6 (33.3)	5 (27.8)	11 (61.1)
Mistrust	6 (33.3)	1 (5.6)	7 (38.9)
Government agencies want partnerships			
Want	9 (50.0)	4 (22.2)	13 (72.2)
Avoid	3 (16.7)	2 (11.1)	5 (27.8)
Adequate inter-company, information sharing			
Adequate	1 (5.6)	1 (5.6)	2 (11.2)
Inadequate	11 (61.1)	5 (27.8)	16 (88.9)
Mandatory state laws not required			
No laws	5 (27.8)	2 (11.1)	7 (38.9)
Laws	7 (38.9)	4 (22.2)	11 (61.1)

a = N (%); Totals may not equal 100% due to rounding

Another crosstabulation, detailed in Table 9, shows how perceptions of inter-organizational efforts to combat cyber crime are distributed by business objective. This analysis examines whether profitability objectives engender increased criticism of, or support for, government initiatives combating cyber crime. The data highlight three patterns. First, respondents tended to answer negatively. Second, column totals show that the attitudes of non-profit organizations towards survey items were consistently aligned with those of profit seeking organizations. Third, responses for each item category were distributed in a 2:1 ration across both types of organization.

In particular, most profit seeking organizations (10:2) disagreed with the statement suggesting law enforcement agencies have an adequate understanding of threats posed by cyber crime. Similarly, most non-profit organizations (5:1) also disagreed with the survey statement. Again, almost all profit seeking organizations (11:1) disagreed that there is enough sharing of information between companies to fight cyber crime. Likewise, most non-profit organizations (5:1) felt that information sharing was inadequate. Finally, a majority of profit seeking organizations (7:5) agreed that mandatory state laws are required to force organizations operating in Michigan to publicly disclose unauthorized security breaches. Two-thirds of non-profit organizations (4:2) also voiced support for mandatory laws.

For the first test of the study hypotheses, three of the five independent variables measuring Turk's concepts - cultural congruence, resistance, and sophistication - were recoded into new categories. For each variable created by combining attitudinal responses, the mean score extending from 1 (strongly agree) to 4 (strongly disagree) was divided into the following range: 1.00 through 1.99 represented a high measure, while

values 2.00 through 4.00 were marked as a lower measure. The independent variable used to represent power, the number of organizational workers, was also recoded. Organizations with more than a thousand workers were categorized as having a high measure of power, while those with a thousand or fewer workers were marked as having a lower measure.

A shortage of responses for the item, "On average, what is the estimated cost of damages caused by each hacking incident?", created difficulty with operationalizing offensiveness. The item, "Have hacking activities resulted in the unavailability of key systems or data?", was instead used so that Hypothesis 2 did not have to be dropped from the analysis. However, while this item reflects the seriousness of hacking activities, its substitution was not flawless because almost all respondents (94%) indicated that key systems were not rendered unavailable. This is an important detail to consider when reading the results of hypothesis testing.

Table 10 crosstabulates the independent variables operationalizing Turk's concepts by the study's dependent variable, the willingness of respondent organizations to prosecute hackers. Furthermore, a competing measure, organizations previously victimized by hackers, was also matched against organizational willingness to prosecute. Total columns show that the observed counts for each concept reflect strong support for the prosecution of hackers. However, cultural congruence (13:0) and sophistication (9:4) are the only instances where a high measure of each concept dominated responses.

Reflecting this trend, the Chi-Square statistic, a comparison of observed counts with the number of counts expected if the null hypothesis is true, of both cultural congruence (4.84) and sophistication (2.17) is high. It is possible that these figures are

inflated because of empty cells but they are not high enough to be statistically significant. In other words, the study data does not include enough unexpected counts, high concept measures combines with a strong willingness to prosecute hackers, to justify rejection of the study's null hypothesis.

Table 10. Crosstabulations and Chi-Square Values for Turk's Premises by Willingness to Prosecute (N=19)

Variables	Prosecute hackers		Chi-Square	Association
	Strongly agree	Other		
Cultural Congruence			4.84	1.00a
High	13 (68.4)	4 (21.1)		
Lower	0	2 (10.5)		
Total	13 (68.4)	6 (31.6)		
Offensiveness			.49	.17b
Yes	1 (6.3)	0		
No	10 (62.5)	5 (31.3)		
Total	11 (68.8)	5 (31.3)		
Resistance			.28	-1.26a
High	7 (36.8)	4 (21.1)		
Lower	6 (31.6)	2 (10.5)		
Total	13 (68.4)	6 (31.6)		
Power			.28	-.26a
High	6 (31.6)	2 (10.5)		
Lower	7 (36.8)	4 (21.1)		
Total	13 (68.4)	6 (31.6)		
Sophistication			2.17	.64a
High	9 (47.4)	2 (10.5)		
Lower	4 (21.1)	4 (21.1)		
Total	13 (68.5)	6 (31.6)		
Victimized by hackers			.28	.12b
Yes	6 (31.6)	2 (10.5)		
No	7 (36.8)	4 (21.5)		
Total	13 (68.4)	6 (31.6)		

*<.05
a = Gamma; b = Phi

A second dimension to the Chi-Square statistic is the measure of association. These measures, which vary depending upon the measurement level of categorical variables, show the direction and strength of the relationship between two variables. Two measures used for hypothesis testing are shown in Table 12. First, the phi coefficient was calculated for variables measured on a nominal scale including offensiveness and prior victimization. As the results show, phi values were much closer to zero than one. Thus, the relationship between the offensiveness of hacking activity and the willingness to prosecute (.17), along with prior victimization and the willingness to prosecute (.12), was weak.

Second, the gamma coefficient was calculated for ordinal-level variables such as cultural congruence, resistance, power, and sophistication. The negative measure for resistance (-1.26) suggests that as the determination of hackers to offend increases, organizational willingness to sanction them decreases. Similarly, the negative gamma value for power (-.26) shows that as organizational resources increase, the willingness to sanction hackers decreases. In contrast, cultural congruence has a positive value (1.00) which means that organizations that closely adopt legal norms are more likely to prosecute hackers. Likewise, the positive gamma value for sophistication (.64) means that organizations liaising with law enforcement agencies will also be likely to report hackers to legal authorities. However, it should be noted that all gamma measures calculated in this analysis were not found to be statistically significant.

Multivariate statistics

In order to examine how the study variables combined to predict respondents' willingness to prosecute hackers, a binary logistic regression model was developed.

Cultural congruence, resistance, and sophistication were recoded so that the value of each variable was a mean score of the original responses to attitudinal questions. Offensiveness, power, willingness to prosecute, and prior victimization were maintained as categorical variables. Thus, the model consisted of six independent variables, or partial coefficients, used to explain a single dependent variable.

Table 11. Regression Analysis I for Turk's Premises and Prior Victimization (N=19)

Variables	B	S.E.	Odds	Tolerance	VIF
Cultural congruence	4.404	3.366	81.811	.404	2.47
Offensiveness	-3.180	60.512	.042	.620	1.61
Resistance	-2.813	2.501	.060	.437	2.29
Power	.071	2.007	1.074	.635	1.57
Sophistication	1.241	2.966	3.458	.459	2.18
Victimization	-1.067	2.286	.344	.520	1.92

*<.05
Cox & Snell R-Square = .356; Nagelkerke R-Square = .500

Table 11 shows the results of each variable entered into the model. The two R-Square values suggest that the study variables, including the competing victimization variable, combine to explain somewhere in the region of 36 to 50 per cent of the variance in the dependent variable. Moreover, the independent variables, including the control variable for prior victimization, did not have antilog (odds) values found to be statistically significant. This effectively means that Turk's concepts do not reliably predict the propensity of organizations to report network intrusions.

Additional findings in Table 11 highlight a major challenge to building a reliable model. Namely, the odds value for cultural congruence is much larger (81.8) than the remaining values. If this value were to be true, then knowledge of cultural congruence would increase the likelihood to predicting the willingness of organizations to prosecute

hackers by eighty-one times. Another possibility is that the model suffers from collinearity problems such that independent variables influence the values of other independent variables.

To test for multicollinearity, tolerance and variance inflation factor (VIF) values were calculated for the regression model. Table 12 shows that for each independent variable, the tolerance value is lower than 0.1. Furthermore, none of the VIF values listed exceed 3.0. Given these thresholds, it is unlikely that a collinearity problem exists between study variables. The absence of significant linear correlations, as shown in a matrix presented in Table 12, also supports this position.

Table 12. Correlations of Independent Variables (N=19)

Variable	V_1	V_2	V_3	V_4	V_5	V_6
V_1	.	.098 (16)	.402 (19)	-0.55 (19)	.402 (19)	-.055 (19)
V_2		.	-.293 (16)	-.228 (16)	.258 (16)	.333 (16)
V_3			.	.080 (19)	.136 (19)	-.136 (19)
V_4				.	-.136 (19)	.352 (19)
V_5					.	.080 (19)
C_1						.

V_1 = Cultural congruence, V_2 = Offensiveness, V_3 = Resistance, V_4 = Power, V_5 = Sophisitication, C_1 = Victimization

Thus, a better explanation for the high antilog and standard error numbers in Table 11 is that the independent variables suffer from a disproportionate range of responses. This is especially true of cultural congruence, where all the values fall between 1.00 and 2.00, and offensiveness, where only a single respondent reported the unavailability of key systems due to hacking activities. This problem is aggravated by a shortage of data and seeking to use six independent variables, three of which are

categorical, in a multivariate analysis. Consequently, variance between cases is dispersed over a wide range of responses and confidence in the model's validity is undermined.

Table 13. Regression Analysis II for Turk's Premises and Prior Victimization (N=19)

Variables	B	S.E.	Odds	Tolerance	VIF
Resistance	-1.039	1.229	.354	.932	1.07
Power	1.112	1.412	3.042	.825	1.21
Sophistication	1.951	1.257	7.034	.932	1.07
Victimization	.247	1.363	1.280	.825	1.21

*<.05
Cox & Snell R-Square = .171; Nagelkerke R-Square = .241

Table 13 displays the results of a second regression analysis with the variables for cultural congruence and offensiveness removed from the model. Here, power (3.0) and sophistication (7.0) are the variables that explain best whether organizations are likely to seek the prosecution of offenders. However, the model as a whole has weak R-Square values and these suggest that only 17 to 24 per cent of variance in the dependent variable is explained by all remaining independent variables.

DISCUSSION AND CONCLUSIONS

The main purpose of this study was to understand exactly how organizations in Michigan respond to incidents of network intrusion. Propositions from Turk's Theory of Norms Violation were operationalized and then tested using data returned by 19 of the 145 American Society for Industrial Security (ASIS) members purposively selected as study participants. No evidence was found to support any of the five study hypotheses, suggesting that organizations do not assume the role of law enforcement authorities and instead are willing to work with police to criminalize network intruders.

A noticeable deficiency of the study is the low sample size. Nineteen responses is simply too low a number with which to make generalizations about the study population, organizations in Michigan. Whether the survey suffered because of its length or a lack of appeal remains unclear, mainly because of the low success conducting follow-up calls. Variance in respondents' answers would undoubtedly smooth out in a larger sample and give the reader a greater sense of confidence when drawing conclusions about the study findings.

It is worth noting, however, that the final response rate for the study was 13 per cent. While this figure falls short of the 51 per cent in responses Thompson (1997) achieved, it is comparable to the 14 per cent the CSI/FBI (2002) study obtained. The key difference between this study and the CSI/FBI survey is that the latter research sampled a significantly higher number of organizations. While it may not be possible to find the funds required to send 3500 surveys by post, future researchers should be prepared to sample at least 1500 organizations in order to obtain a reasonable sample size.

The crosstabulations for organizational characteristics by victimization show rates of network intrusion in Michigan mirror national figures. The final CSI/FBI survey in 2002 found that 42 per cent of participants had been victimized. Similarly, findings from this study found that 42 per cent of organizations had suffered a network intrusion. This repetition in findings lends weight to the view that the victimization rate of organizations in the United States is probably lower than Carter and Katz's observation of 98 per cent. With respect to specific forms of abuse, the least prevalent intrusion was data theft and the most common intrusion was network attack. However, victimization did not feature heavily in any one industrial sector. The only victimology trend evident in the data is that a high proportion of older organizations incurred network attacks.

In terms of responses to intruders, the data suggest that Michigan organizations have policies in place to handle network incidents. Levels of senior management participation in investigation decision-making and guidelines stating who is responsible for conducting an investigation indicate an internal state of preparedness. Furthermore, the number of organizations reporting that they have written guidelines about how evidence should be collected and preserved exceeds the figure reported by Thompson (1997). This trend is probably due to increased reports of hacking released in recent years, although it would be interesting to learn if these protocols were created before or after network intrusions.

When analyzing attitudes towards government initiatives combating cyber crime, the data show that organizations do not perceive the police and courts as being prepared to deal with hackers. This appears not so much an issue of trust but instead competence. Police do pursue and value partnerships with private companies and organizations do

trust the police. But organizations believe that investigations take a long time and law enforcement agencies do not fully appreciate the threats posed by cyber crime. The opinions of private organizations differed little from those of public organizations on this point.

Therefore, pragmatism rather than ideology may explain why Turk's Theory of Norms Violations fails to predict conflict outcomes in hacking cases. While the mean score for the cultural congruence scale was close to strong agreement, indicating that organizations support the norm of sanctioning hackers, not all respondents strongly agreed that hackers should be prosecuted. As such, do organizations mean what they say? An unfortunate consequence of asking subjects if their organization is law-abiding was that responses tended to be positive. Respondents may also have believed that there was a hidden moral imperative not to present themselves like hackers, who break the law. Although it is unknown if this factor was influential, the point remains that it is easier to agree with anti-hacking sentiment than to necessarily take steps to prosecute offenders.

This is a harsh assessment and organizations may genuinely believe in defending laws. Indeed, a large proportion of respondents agreed that state laws are required to force organizations to report unauthorized security breaches. However, bivariate findings suggest that hackers who are determined to oppose legal norms dealing with network intrusion do not incur sanctions. Similarly, organizations with large resources do not necessarily seek to prosecute intruders. In both cases, a range of factors -- foreign hackers avoiding detection and extradition, internal bureaucratic obstacles towards reporting, the risk of negative media attention, intrusions that were simply not disruptive, or some other unknown -- could explain why organizations do not seek conflict with offenders.

Interestingly, almost half of the study respondents believed most hackers are juveniles. From a practical perspective, shaping laws to prohibit abuses committed by children is difficult and emotive. Moreover, cyber crime represents a break with tradition. Would authorities in Michigan be prepared to prosecute a Californian child charged with defacing a business website in Michigan? On the one hand, the offence does lead to property data being physically altered. On the other hand, the execution of the crime is remote and transferring a child across America, to face sanctioning for a crime that does not cause physical harm, would undoubtedly require resolve on the part of legal authorities. The complexity of this issue demonstrates that there are forces the police cannot control alone and that charges of incompetence by organizations are unwarranted.

Nevertheless, by successfully investigating difficult cross-jurisdictional cases, the actions of police would counter the criticism that they do not care about network intrusion. But it should be noted that these efforts would be aided by organizations accurately accounting for damages incurred by network incidents. Only three respondents indicated how much the estimated cost of damages was for each hacking incident. This finding may reflect Carter and Katz's argument that it is harder to assess the monetary losses than to establish that intrusions have occurred. Organizations may also not desire to disclose such information but if they cannot produce an accurate record for investigators, legal attempts to prosecute offenders – whether they are children or other individuals – could be seriously undermined.

Thus, there still remains scope for exploring Turk's theory further. This study follows a trend of victim-based surveys and it omits the views of other key actors, such as police and attorneys, which are equally as important. If data could be acquired or made

publicly available, it would be interesting to examine what police believe with respect to cooperation from organizations, official investigations, and rapport with higher-level enforcers such as prosecutors. Furthermore, another study could be performed with a study population that includes more than one state. In the meantime, however, with computers continuing to occupy a central position in society, it appears that network intrusion is unlikely to cease.

APPENDICES

APPENDIX A

APPENDIX A

Computer Network Intrusions Survey

The aim of this study is to extend the scope of existing knowledge with respect to what is broadly termed as computer "hacking". The widespread growth of computers, and particularly computer networks, has presented a new means of committing crime. Unfortunately, the magnitude and frequency of this problem is unknown. Moreover, it is unclear how organizations respond to hacking incidents. Answering this questionnaire may assist in determining current hacking trends and how organizational responses to these activities impact upon the legal system in Michigan.

To this end, the following survey consists of sixty-seven questions. The survey should take approximately twenty-five minutes to answer. We ask that you return the completed survey to the MSU School of Criminal Justice in the enclosed postage pre-paid envelope.

Your participation in this survey is completely **VOLUNTARY.** You can refuse to answer any questions and you may discontinue at any time. The investigators listed below will ensure that your responses remain strictly **CONFIDENTIAL.** Your privacy will be protected to the maximum extent allowable by law. By returning the completed survey you indicate your consent to participate in this study. **We would appreciate it if you can return the survey within two weeks after receipt.**

If you have questions about the study, contact Mahesh Nalla (560 Baker Hall, East Lansing MI 48824; phone: (517) 355-2228; email: nalla@msu.edu). In case you have questions or concerns about your rights as a research participant, please feel free to contact Ashir Kumar, MD, Michigan State University's Chair of University Committee on Research Involving Human Subjects by phone: (517) 355-2180, fax: (517) 432-4503, email: ucrihs@msu.edu , or regular mail: 202 Olds Hall, East Lansing, MI 48824.

Thank you for your assistance and support of this research project. Sincerely,

Mahesh Nalla, Ph.D. (Professor)
School of Criminal Justice
Michigan State University
East Lansing, MI 48824-1118
Tel: 517-355-2228
E-mail: nalla@msu.edu

Jack Drew (Graduate Student)
School of Criminal Justice
Michigan State University
East Lansing, MI 48824-1118
Tel: 517-355-3881
E-mail: drewjack@msu.edu

Part 1. Organizational background: *this section seeks to collate basic demographic information about the organization for which you work.*

1. What is the core specialization of the organization?
   a. Professional services
   b. Retail
   c. Advertising
   d. Manufacturing
   e. Engineering
   f. Education
   g. Government
   h. Research
   i. Other

2. What is the business objective of the organization?
   a. Profit
   b. Non-profit

3. Approximately how many workers are employed by the organization?
   _____

4. How many contracts (e.g. patients treated, business projects) does the organization service each year?
   _____

5. How long has the organization has been operating for?
   a. Less than a year
   b. 1-3 years
   c. 4-10 years
   d. 11+ years

6. What is the ZIP code for the organization's base of operations in Michigan?
   ZIP: _____

Part 2. Computer usage: *the following questions briefly examine the computer network resources used by your organization.*

7. Does the organization use a network of computers for business operations?
   a. Yes – Intranet
   b. Yes – Intranet and Internet access
   c. No network

8. Does the organization have a website?
   a. Yes
   b. No

9. Who manages the organization's information technology?
   a. Internal group
   b. External contractors
   c. Both

10. Who manages the security of computer resources belonging to the organization?
    a. Internal group
    b. External contractors
    c. Both

Part 3. Incident history: *the following section contains questions relating to the frequency and severity of computer network intrusions experienced by the organization for which you work.*

11. In the last 5 years, have hackers modified or attempted to modify data belonging to the organization?

a. Never
b. Once
c. 2-10 times
d. 11-25 times
e. 25+ times

12. In the last 5 years, have hackers stolen or attempted to steal data belonging to the organization?

a. Never
b. Once
c. 2-10 times
d. 11-25 times
e. 25+ times

13. In the last 5 years, have hackers attacked or attempted to attack network resources belonging to the organization?

a. Never
b. Once
c. 2-10 times
d. 11-25 times
e. 25+ times

14. Have hacking activities resulted in the unavailability of key systems or data?

a. Yes
b. No

15. On average, what is the estimated cost of damages caused by each hacking incident?

US$: _____

Part 4. Investigations: *this section seeks to establish if the organization has formal instructions outlining how a suspected hacking incident (an attack from* outside *the network) will be investigated.*

16. Does the organization have written guidelines that specifically identify who should investigate a computer security incident?

a. Security group
b. I.T. group
c. Both
d. No policy

17. Does the organization have written guidelines that indicate how digital evidence should be collected and preserved?

a. Yes
b. No

18. Does senior management actively participate in investigation decision-making?

a. Yes
b. No

Part 5. Legal action: *from experiences gained during your current tenure, to what extent would you agree with the following statements? SA=Strongly Agree, A=Agree, D=Disagree, SD=Strongly Disagree.*

19. Organizational representatives spend time participating in local community projects (i.e. not just commercial sponsorship).

SA A D SD

20. The organization strongly believes in the laws of the land (both criminal and civil).

SA A D SD

21. The importance of criminal and civil laws are reflected in the contracts drawn up during the course of business.

SA A D SD

22. The organization enforces contractual agreements and rules regarding employee behavior in equal measure.

SA A D SD

23. Media scrutiny of the organization's activities does not have any influence upon strategic decisions.

SA A D SD

24. Media reports of police success when catching hackers does not lead to aggressive police treatment when an organization reports a network intrusion.

SA A D SD

25. The media portray prosecuted hackers as criminals rather than victims.

SA A D SD

26. The organization views hackers as individuals who violate laws that protect the whole of society.

SA A D SD

27. Hackers aged less than 18 years evade justice because they face a juvenile rather than adult trial.

SA A D SD

28. Hackers evade justice because digital evidence held against them is inadequate.

SA A D SD

29. Hackers evade justice because they perpetrate crimes from outside the United States.

SA A D SD

30. Hackers evade justice because they are able to mount a strong legal defense.

SA A D SD

31. Hackers evade justice because the organization lacks time or money with which to pursue a conviction.

SA A D SD

32. The organization is more likely to lodge a civil suit if a hacker mounts legal resistance.

SA A D SD

33. The police and courts consider hacking serious, and actively seek to bring culprits to justice.

SA A D SD

34. If police encourage representatives to report an incident, the organization will be more willing to report.

SA A D SD

35. The organization has had positive working relationships with the police before.

SA A D SD

36. If a prosecutor states that the courts will treat hackers harshly, the organization will be more willing to pursue a criminal prosecution.

SA A D SD

37. Even if a litigator states that a strong case exists for recovering damages, the organization will be more willing to take the matter to the criminal courts.

SA A D SD

38. Former experiences gained from hacking incidents serve as an incentive for seeking a criminal prosecution.

SA A D SD

39. In the case of hacking, the organization would clearly prefer to approach the criminal courts as opposed to the civil courts.

SA A D SD

Part 6. Government-organizational responses to hacking: *to what extent does the organization agree with the following statements? Please answer SA (strongly agree), or A (agree), or D (disagree), or SD (strongly disagree).*

40. Top management not well versed with computer technology will be more reluctant to adopt an aggressive stance towards fighting cyber-crime ___

41. There is a fundamental difference between how the corporate sector views cyber-crime and that of governmental policing agencies ___

42. Law enforcement agencies do not have an adequate understanding of threats from cyber-crime ___

43. There is a greater need for police to cooperate with the private sector to fight cyber-crime ___

44. There is a greater need for the private sector to cooperate with police to fight cyber-crime ___

45. Governmental agencies do not trust partnerships with private companies ___

46. Governmental agencies are not interested in developing partnerships with the private sector to develop strategies to deal with cyber-crime ___

47. There is not enough sharing of information between companies to fight cyber-crime ___

48. The Michigan State Government needs to allocate greater resources to fight cyber-crime ___

49. Mandatory state laws are required to force organizations that do business in Michigan to publicly disclose any security breaches by unauthorized persons ___

50. It is essential to have a cohesive cyber-security policy announced by the Federal tier of government ___

Part 7. Summary: *the final section asks questions about the overall organizational view of hackers and hacking.*

51. What category does the organization believe most hackers fall into?
    a. Ex-employees
    b. Current employees
    c. Individuals living outside the U.S.
    d. Youths under 18 years
    e. Other – please specify _____

52. Are hackers becoming more skillful?
    a. Yes
    b. No

53. Which hacking incident does the organization consider the most serious?
    a. Attack
    b. Data theft
    c. Data modification

54. Which hacking incident is the organization most likely to take legal action for?
    a. Attack
    b. Data theft
    c. Data modification

In summary, please answer SA (strongly agree), or A (agree), or D (disagree), or SD (strongly disagree) for each of the following statements about the organization's view of hacking:

55. Hackers should be criminally prosecuted ___

56. Criminal courts treat hackers leniently ___

57. The organization does not trust the police ___

58. Criminal investigations take too long ___

59. Recovering damages is a priority ___

60. Civil trials are a waste of money ___

61. Media scrutiny of any public trial is damaging ___

62. Hackers are better left alone ___

63. Response will depend on severity of attack ___

64. Only persistent hackers spark response ___

65. A smarter security policy is the best response ___

66. Organization is too busy to care ___

67. Hacking has never been a problem ___

APPENDIX B

APPENDIX B

Table A. Factor Loadings[2] and Mean Scores of Legal Action Perceptions (N=19)

Item	Factor	Means	S.D.
1. Participation in local community projects	.381	1.38	.62
2. Belief in laws	.327	1.13	.34
3. Contracts reflect laws	.289	1.19	.40
4. Contracts and rules enforced equally	.210	1.31	.60
5. Media scrutiny does not influence strategy	.296	2.56	.96
6. Media reports does not lead to aggressive police treatment	.229	1.94	.44
7. Media portray hackers as criminals	.122	1.88	.81
8. Organization views hackers as violators	.353	1.50	.52
9. No justice evasion due to juvenile status	.390	2.69	.79
10. No justice evasion due to weak evidence	.589	2.56	.81
11. No justice evasion due to alien status	.670	2.63	.81
12. No justice evasion due to good defense	.873	1.94	.57
13. No justice evasion due to limited resources	.732	2.44	.73
14. Civil action if hackers legally resist	-.503	2.19	.91
15. Authorities consider hacking serious	.230	2.06	.77
16. Report if police encourage it	-.429	1.88	.62
17. Positive relationships with police	.196	1.31	.48
18. Seek to prosecute if harsh sentence	-.427	1.88	.50
19. Prosecute instead of damages recovery	-.562	2.06	.57
20. Former experiences promote prosecution	.149	1.94	.44
21. Preference for criminal, not civil trial	-.376	1.88	.62

Mean = 1.92; Standardized Alpha = .7707

[2] Loaded on a single factor, without forcing.

Table B. Factor Loadings[3] and Mean Scores For Government Perceptions (N=19)

Item	Factor	Means	S.D.
1. No reluctance by top management	-.556	3.00	.84
2. Views on hacking do not differ by sector	.436	2.83	.71
3. Law enforcement understands threat	.418	3.17	.62
4. No need for greater police cooperation	.227	3.44	.62
5. No need for greater private cooperation	-.164	3.44	.62
6. Government agencies trust partnerships	.692	2.33	.77
7. Government agencies want partnerships	.647	2.17	.62
8. Adequate inter-company, information sharing	-.332	3.11	.58
9. No need for greater resource allocation	-.343	3.17	.71
10. Mandatory state laws not required	-.434	2.61	.85
11. Cohesive Federal policy is essential	.365	1.94	.73

Mean = 2.84; Standardized Alpha = .5095

[3] Loaded on a single factor, without forcing.

Table C. Factor Loadings[4] and Mean Scores For Summary Perceptions (N=19)

Item	Factor	Means	S.D.
1. Hackers should be criminally prosecuted	.509	1.32	.48
2. Criminal courts treat hackers leniently	.343	2.68	.67
3. Organization trusts the police	-.230	1.53	.61
4. Criminal investigations are timely	.358	2.63	.68
5. Recovering damages is a priority	.602	2.05	.62
6. Civil trials are not wasteful	-.115	2.11	.46
7. Media scrutiny is not damaging	-.004	2.53	.61
8. Hackers are not better left alone	-.412	1.68	.75
9. Response depends on severity	.624	1.84	.50
10. Persistent hackers spark response	.271	2.11	.81
11. Smarter security policy is best	-.226	2.11	.74
12. Organization is not too busy to care	.176	1.53	.61
13. Hacking has never been a problem	.149	2.74	.87

Mean = 2.06; Standardized Alpha = .5837

[4] Loaded on a single factor, without forcing.

REFERENCES

American Society for Industrial Security International. (2003). About ASIS: The Faces of Security Today. [Online] Available http://www.asisonline.org/about/index.xml, June 4, 2003.

Australasian Centre for Policing Research. (2000). The Virtual Horizon: Meeting the Law Enforcement Challenges – Developing an Australasian law enforcement strategy for dealing with electronic crime. Payneham, SA: Australasian Centre for Policing Research.

Bakewell, E. J., Koldaro, M., & Tjia, J. M. (2001). Computer Crimes. The American Criminal Law Review, 38(3), 481-524.

Beirne, P., & Messerschmidt, J. (1995). Criminology. Orlando, FL: Harcourt Brace & Company.

Carter, D. L., & Katz, A. (1996). Computer Crime and Security: The Perceptions and Experiences of Corporate Security Directors. Security Journal, 7(2), 101-108.

Casey, E. (2000). Digital Evidence and Computer Crime: Forensic Science, Computers and The Internet. San Diego, CA: Academic Press.

Central Intelligence Agency. (2003). The World Factbook 2002. [Online] Available http://cia.gov/publications/factbook/index.html, April 19, 2003.

Chiricos, T. G., & Waldo, G. P. (1975). Socioeconomic Status and Criminal Sentencing. American Sociological Review 40(6), 753-772.

Comer, D. E. (1995). Internetworking With TCP/IP Volume 1: Principles, Protocols, and Architecture. Upper Saddle River, NJ: Prentice Hall.

Computer Security Institute. (2002). 2002 CSI/FBI Computer Crime and Security Survey. [Online] Available http://www.gocsi.com/forms/fbi/pdf.html, April 19, 2003.

Cullen, F. T., & Agnew, R. (1999). Criminological Theory: Past To Present Essential Readings. Los Angeles, CA: Roxbury Publishing Company.

Dierks, M. P. (1993). Computer Network Abuse. Harvard Journal of Law & Technology, 6(2), 307-342.

Fiery, D. (1994). Secrets of a Super Hacker. Port Townsend, WA: Loompanics Unlimited.

Friedman, M. (1982). Capitalism and Freedom. Chicago, IL: University of Chicago Press.

Galbraith, J. K. (2001). The Essential Galbraith. New York, NY: Houghton Mifflin Company.

Gates, W. H. (1996). The Road Ahead. New York, NY: Penguin Books.

Goodman, M. D. (1997). Why The Police Don't Care About Computer Crime. Harvard Journal of Law & Technology, 10(3), 465-494.

Hagan, J. (1974). Extra-Legal Attributes and Criminal Sentencing: An Assessment of a Sociological Viewpoint. Law and Society Review 8(3), 357-383.

Jacobs, D., & Britt, D. (1979). Inequality and Police Use of Deadly Force: An Empirical Assessment of a Conflict Hypothesis. Social Problems 26(4), 403-412.

Kovacich, G. L., & Boni, W. C. (2000). High-Technology-Crime Investigator's Handbook: Working In The Global Information Environment. Woburn, MA: Butterworth-Heinemann.

Lanza-Kaduce, L., & Greenleaf, R. G. (1994). Police-Citizen Encounters: Turk On Norm Resistance. Justice Quarterly,11(4), 605-623.

Lanza-Kaduce, L., & Greenleaf, R. G. (2000). Age and Race Deference Reversals: Extending Turk on Police-Citizen Conflict. Journal of Research in Crime and Delinquency,37(2), 221-236.

Lilly, J. R., Cullen, F. T., & Ball, R. A. (2002). Criminological Theory: Context and Consequences. Thousand Oaks, CA: Sage Publications.

Maltz, M. (1999). Bridging gaps in police crime data. Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics.

Marx, K., & Engels, F. (1998). The Communist Manifesto: A Modern Edition. New York, NY: Verso.

Michalowski, R. J., & Pfuhl, E. H. (1991). Technology, property, and law: The case of computer crime. Crime, Law and Social Change, 15(3), 255-275.

Mills, C. W. (2000). The Power Elite. New York, NY: Oxford University Press.

Neuman, W. L., & Wiegand, B. (2000). Criminal Justice Research Methods: Qualitative & Quantitative Approaches. Needham Heights, MA: Allyn and Bacon.

Parker, D. B. (1983). Fighting Computer Crime. New York, NY: Charles Scribner's Sons.

Roby, P. A. (1969). Politics and Criminal Law: Revision of the New York State Penal Law on Prostitution. Social Problems 17(1), 83-109.

Sherizen, S. (1996). Can computer crime be deterred? Security Journal, 6(3), 177-181.

State of Michigan. (2003a). Governor Jennifer M. Granholm: Biography. [Online] Available http://www.michigan.gov/gov/0,1607,7-168--57920--, 00.html, June 4, 2003.

State of Michigan. (2003b). The Michigan Penal Code (Excerpt): Act 328 of 1931. [Online] Available http://michiganlegislature.org/documents/mcl/pdf/mcl-750-145d.pdf, June 4, 2003.

Stephenson, P. (2000). Investigating Computer-Related Crime. Boca Raton, FL: CRC Press LLC.

Thompson, D. (1998). 1997 computer crime and security survey. Information Management & Computer Security, 6(2), 78-101.

Turk, A. T. (1966). Conflict and Criminality. American Sociological Review, 31(3), 338-352.

U.S. Census Bureau. (1997a). 1997 Economic Census: Summary Statistics for Michigan 1997 NAICS Basis.
[Online] Available http://www.census.gov/epcd/ec97/mi/MI000.HTM, April 20, 2003.

U.S. Census Bureau. (1997b). Michigan QuickFacts from the US Census Bureau. [Online] Available http://quickfacts.census.gov/qfd/states/26000.html, April 20, 2003.

U.S. Department of Justice. (1967). What is the sequence of events in the criminal justice system? [Online] Available http://www.ojp.usdoj.gov/bjs/flowchart.htm, June 2, 2003.