ABSTRACT

Title of dissertation: AN EXPLANATORY MODEL OF MOTIVATION FOR CYBER-ATTACKS DRAWN FROM CRIMINOLOGICALTHEORIES

Seymour M. Mandelcorn, Doctor of Philosophy, 2013

Dissertation directed by: Professor Mohammad Modarres
Professor Ali Mosleh
Reliability Engineering Program

A new influence model for Cyber Security is presented that deals with security attacks and implementation of security measures from an attacker's perspective. The underlying hypothesis of this model is that Criminological theories of Rational Choice, Desire for Control, and Low Self-Control are relevant to cybercrime and thereby aid in understanding its basic Motivation. The model includes the roles of Consequences, Moral Beliefs such as Shame and Embarrassment together with Formal Sanctions in deterring cybercrime, as well as role of Defense Posture to limit the Opportunity to attack and increase the likelihood that an attacker will be detected and exposed. One of the motivations of the study was the observation that few attempts have been made to understand cybercrime, in the context of typical crime because: (a) an attacker may consider his actions as victimless due to remoteness of the victim; (b) ease to commit cybercrimes due to opportunities afforded by the Internet and its accessibility, and readily available tools and knowledge for an attack; and (c) vagueness of cybercrime laws that makes prosecution difficult. In developing the model, information from studies in classical crime was related to Cybercrime allowing for analysis of past cyber-attacks, and subsequently preventing future IS attacks, or mitigating their effects. The influence

model’s applicability is demonstrated by applying it to case studies of actual information attacks which were prosecuted through the United States Courts, and whose judges’ opinions are used for statements of facts. Additional, demonstration of the use and face validity of the model is through the mapping of the model to major annual surveys’ and reports’ results of computer crime.

The model is useful in qualitatively explaining “best practices” in protecting information assets and in suggesting emphasis on security practices based on similar results in general criminology.

AN EXPLANATORY MODEL OF MOTIVATION FOR CYBER-ATTACKS DRAWN FROM CRIMINOLOGICAL THEORIES

by

Seymour M Mandelcorn

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for a degree of
Doctor of Philosophy
2013

Advisory Committee:

Professor Mohammad Modarres, Chair/Advisor

Professor Ali Mosleh, Co-Chair/Advisor

Professor Sally Simpson

Professor Peter Sandborn

Professor Gregory Baecher (Dean's Representative)

I dedicate this dissertation to the loving memory of my dear aunt,

Jeanette Merves Seltzer

Acknowledgements

This work is the culmination of an intense and intellectually challenging period of my life, facilitated and invigorated by the talents and expertise of many professional mentors. Most notably, I would like to acknowledge Professor Mohammad Modarres, Chair and Advisor, and Professor Ali Mosleh, Co-Chair and Advisor; for their extensive erudition and always apt advice, for their encouragement and unflagging moral support. I would also like to thank Professors Sally Simpson, Peter Sandborn, and Gregory Baecher, for their astute and discerning input, which enabled me to address discrepancies and clarify issues. I appreciate as well the professorship of the University of Maryland's Reliability Engineering Program and of the Department of Criminology and Criminal Justice, who generously shared their knowledge with me.

I thank Stephan Sherman, Associate Director of the Institute for Governmental Service and Research of the University of Maryland, for his support and encouragement. I also thank Robin Parker Cox, Ph.D., who is Director of the Institute for Governmental Service and Research. In reflecting upon the myriad procedural details involved in my research, I owe a special thanks to Patricia Kosco Cossard, Architecture, Planning, and Preservation Librarian at the University of Maryland, for helping me overcome all the referential glitches. I appreciate Dr. Laura Wyckoff's giving of her time, in which we analyzed issues pertinent to criminology.

To my dear parents, Dr. and Mrs. Lyon and Ruth Mandelcorn, thank you for your constant support and encouragement; even when the research plateaued, you inspired me with your determination and confidence. To my dear wife, Faigie, thank you for your encouragement and for standing by my prolonged involvement with this research.

List of Abbreviations

BACS	Bay Area Credit Services
CCSS	Common Configuration Scoring System
CERT	United States Computer Emergency Readiness Team
CMSS	Common Misuse Vulnerabilities Scoring System
CSI	Computer Security Institute
CVSS	Common Vulnerability Scoring System
DC	Desire for Control
DDoS	Distributed Denial of Service
DoS	Denial of Service
FISMA	Federal Information Security Management Act
MADD	Mothers Against Drunk Driving
MIT	Massachusetts Institute of Technology
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSSTM	Open Source Security Testing Methodology Manual
POSIX	Portable Operating System Interface
PSF	Performance Shaping Factors
SSH	Secure Shell
STP	Secure Transfer Protocol
TCSEC	Trusted Computer System Evaluation
TQM	Total Quality Management
USMJ	Uniformed Code of Military Justice
USSS	United States Secret Service
UT	University of Texas

Terminology

Corporate crime which is subtype of white collar crime is illegal acts by corporations or their representatives that are undertaken to further the goals of the organization [1].

Cyber-Attack (Security Attack) is a threat-source using an exploit to take advantage of a vulnerability to cause unintended or unanticipated behavior to occur in software or hardware of a computer system. The goal of this behavior change is to affect the confidentiality, integrity or availability of the system in a way that will benefit the threat-source, and may be detrimental the owner of the target system [2], [3].

Cybercrime "is cyber-crime is "Criminal acts committed using electronic communication networks and information systems or against such networks and systems" [4].

Threat-Source is "intent and method targeted at the intentional exploitation of vulnerability" [3].

Threat is "The potential for a threat-source to exercise a specific vulnerability" [5].

Vulnerability is "A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised – accidentally triggered or intentionally exploited - and result in a security breach or a violation of the system's security policy" [5].

Exploit is "a piece of software, a chunk of data, or sequence of commands that takes advantage of vulnerability in order to cause unintended or unanticipated behavior to occur on computer software or hardware [6].

Likelihood is the probability of a threat exercising a system's vulnerability.

Impact is the loss to of a system's confidentiality, integrity, or availability.

Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event. Its significance to a potential victim is weighed by the tolerance of the victim to this likelihood and impact.

White collar crime is "crime committed by a person of respectability and high social status in the course of his occupation" [7].

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Need for Information Security

Since its very advent, computer technology has had to continuously address the issue of "Information Security", where information is stored, processed and communicated. Cyber-attack/security attack, described and defined immediately below, has been, and is a top concern of nations, industries, and ordinary citizens. Nations worry whether their basic computer controlled infrastructures are secure? Are their economic procedures protected from criminal interference? Are their military installations and communications secured from eavesdropping? Is the power grid safe from intentional disruption, and are water supplies assured. Industries worry about protecting their secrets, unwarranted interference of operations, and about access to their confidential negotiations. Ordinary citizens worry about identity theft and privacy.

These are some recent cases of note.

- Albert Gonzalez' cyber-attacks between October 2006 and May 2008 access to 130 million credit and debit cards from the Heartland Payment System, one of the world's largest credit and debit systems. He gained millions of dollars for himself and his cohorts [8]. See Section 5.6.
- Aaron Swartz during September, 2010 downloaded 4 million articles from the Jstor database, and distributed them freely in order to make a statement of conviction in "freedom of information" [9]. See Section 4.6.2.

The objective of information security is the protection of information and systems from unauthorized access, and from their disclosure, modification, destruction or disruption [10].

1.2 Challenges in Delineating Adequate Information Security

Modeling a system to provide a computer and a network, their applications and associated systems with information security is an integral means to achieve this objective. It provides a framework for various security threats and attacks, and responses to actual attacks. However, such modeling is always difficult because of the unknown and continually changing nature of threats, and new vulnerabilities are exploited every day. These are variously due to the advent of new applications and newer ways of accessing and manipulating information, and new vulnerabilities may be discovered in old applications. Consideration has to be given also to the execution of a required response to a detected attack where a human factor may interfere. Therefo**re,** it has also often been difficult and elusive to detect and hopefully overcome security attacks. Consequently establishing a level or even a relative level of security, or conversely risk, quantitatively for a given system at a given time can be misleading. There may even be doubt in declaring unequivocally that "a" is more secure then "b" as there may be a yet to be discovered vulnerability against a threat yet to emerge [11], [12], [13].

Both the perpetrators of cybercrimes and their victims can be male or female; cybercrimes occur with indistinguishable frequency in relation to gender. This thesis reflects this fact in that its policy is to randomly alternate designations of "his" and "her" throughout the work.

1.3 Factors Required for Information Security Modeling

Often when a successful cyber-attack is reported questions are asked why this attack did occur and whether other computers or systems may be subjected to a similar attack. How safe is a given system from an attack and its consequences? Answers have to be drawn from the following.

- The technical aspects of an attack, namely how was it or how could it be performed, and the vulnerabilities in the system;
- An attacker's tools, and the victim's defenses and why they did not or might not protect the system;
- The motivation of an attacker; and
- The factors that encourage an attacker and those that could deter him.

All of these factors working together will determine whether an attack will occur. The relationship and inclusion of these various factors need to be presented in an organized model that can be used to realistically simulate the many different threats that an information system will be faced with.

This work adds face validity to the depth of the credibility of cyber-security measures, and to the understanding of the factors affecting cybercrime. In addition the work broadens the approach to cyber-security from a solely technology centric perspective to the inclusion of a behavior based perspective. The incorporation of a behavior based approach may enable the highlighting of deficiencies in security measures that would not otherwise appear obvious from a purely technological view.

1.4 What is Cybercrime?

The Commission of European Communities [4] defines cybercrime as “Criminal acts committed using electronic communication networks and information systems or against such networks and systems”.

This definition refers to two kinds of criminal acts.

- One is where the attack is *committed by* an information system or network. The target can be another information system and network, or any physical target. This definition includes crimes like cyber-bullying, child pornography, etc.
- The other constitutes crimes against “such networks and systems”. These are crimes where the *target* is a system or network. The attack does not necessarily have to be initiated by a computer or network.

The implication of the first kind of cybercrime is that the actions of the attack taken by the network or system are not distinguishable from those of typical crime.

In contrast, the second kind of cybercrime will cause either denial of service to the target system or network, disclosing of information, or altering of some aspect of the target system or network; these constitute *cyber-attacks* according to the above Definition of Terms.

This work primarily deals with cyber-attacks that are cybercrimes according to the above definition, and that are mainly against information systems or networks.

1.5 Typical Crime and Cybercrime Differences

Regardless of whether the target of a cyber-attack is an information system or a physical entity, there are additional differences between cybercrime and typical crime.

1. Remoteness of the cyber-attacker – A typical crime criminal is aware of the victim and of the inflicted damage, and is physically close to the victim. Cyber-attacks usually occur over great distances. Most often the cyber-attacker does not physically meet the victim, and often is unaware of the victims. Moral deterrence would seem to play less of a role in deterring a cyber-attacker than in typical crime.
2. Unique power of the cyber-attacker – The cybercriminal has a vast array of easily available tools to launch attacks. Collaboration between cybercriminals is easily accomplished using the anonymity of the Internet. Attacks are easily replicated to allow simultaneous occurrence of numerous attacks.
3. The unclearness of cybercriminal law – Due to the infancy of cyber law many forms of cyber-attacks are not covered by laws. Even where there are defined laws, often they are not enforced. Moreover, the internationalism of the Internet creates jurisdiction problems.

1.6 Model Perspective, the Attacker's Perspective

While modeling of information security from the defenders perspective is common, the approach chosen for this research was to develop a model whose content is mainly from the attacker's perspective. It is the attacker who is motivated to attack, who chooses the target and means of attack, and who carries out the attack. Therefore understanding what motivates the attacker, her actual and perhaps perceived opportunities and, finally, the deterring factors the attacker is aware of are most important for modeling information systems attacks.

However, the theoretical basis of this model was assumed to be based on the hypothesis that typical crime theories could be applied to cybercrime. Indeed, crime theories are mainly from the attacker's perspective. It was then required to demonstrate the relevance of this hypothesis. Also, it was necessary to determine which criminology theories are most relevant to cybercrime, and specifically where they are relevant.

The model's completeness and correctness will be demonstrated through successfully mapping eight case studies which were prosecuted through the United States Courts, and whose judges' opinions are used for statements of facts. Additionally, mapping of data from major Information Security surveys will further demonstrate the correctness of the model.

It was found that careful analysis of Information Security, criminology, social science, logic and philosophy literature applied to this model, provided a number of relevant discoveries on strategies or "best practices" to more effectively protect cyber-systems from attack, stop an attack or at least mitigate the effects of an attack. This model can be used to describe security challenges in the design, implementation, operation, and recovery phases of a cyber-system.

1.7 Road Map

The rest of this dissertation is organized as follows.

Chapter 2, Research Motivation, Approach and Goals, is a continuation of the Introduction. This chapter shows how this work fits into risk analysis for information security by looking narrowly at the likelihood of a cyber-attack that is in fact one part of risk analysis. This chapter also discusses the differences between cybercrime and typical crime that need to be taken in account when comparing and contrasting the literature of these two domains. Finally, the goals of this research are laid out.

Chapter 3, Related Work, gives examples of work done in modeling information security from a defenders perspective. Criminology theories that are relevant to cyber-security are presented in order to establish continuity with the following chapters. Finally, related work which uses criminology theories to explain information security is also presented.

Chapter 4, General Influence Model, presents, describes and discusses the complete model. The nodes are all presented separately, with sources for their existence from literature in criminology, social science, law and philosophy.

Chapter 5, Case Studies, presents eight case studies. The facts for seven of the case studies are primarily based on the statements of facts in the various judges' rulings. For one case, in which Private Manning is alleged to have committed cyber-crimes - this case has not yet been prosecuted - press releases are used as sources of facts, as understood at the time of this writing. The eight cases are graphically mapped to the General Influence Model, with discussions of their essential factors.

Chapter 6, Applications of the Model, offers a number of conclusions about the nature of cyber-attacks and suggestions of best practices that can help a defender in allocating resources to better protect a system.

Chapter 7, Conclusions, consists of a summary of this research, followed by its major contributions. Suggestions for follow-up work are presented.

1.8 References

[1] Clinard,M.,l B., Yeager,P., C., and Clinard, R., 1980, Corporate Crime, Free Press, New York.

[2] Gollmann, D., 2006, Computer Security, Wiley, Hoboken, NJ.

[3] Stoneburner, G., Goguen, A., and Feringa, A., 2002, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology," SP 800-30, U.S. Dept. of Commerce, National Institute of Standards and Technology, Gaithersburg, MD.

[4] Commission of the European Communities, 2007, Towards a General Policy on the Fight Against Cyber Crime: Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Office for Official Publications of the European Communities, Luxembourg.

[5] Stoneburner, G., Hayden, C., Feringa, A., and National Institute of Standards and Technology, 2004, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A," SP 800-27, U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg, MD.

[6] Wikipedia contributors, 2012, "Exploit (Computer Security)," from http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Exploit_%28computer_security%29.html.

[7] Sutherland, E., 1949, White Collar Crime, Dryden press, New York.

[8] Guarino, M., 2010, "Card Hacker Albert Gonzalez Gets 20 Years, but Cyber Crime Rising," The Christian Science Monitor.

[9] O'Neill, B., January 25, 2013, "Only One Person is Responsible for Aaron Swartz's Death, and that is Aaron Swartz," Telegraph.Co.Uk.

[10] National Institute of Standards and Technology, 2012, "Federal Information Security Management Act (FISMA)," from http://csrc.nist.gov/groups/SMA/fisma/index.html.

[11] Anderson, R., Barton, C., Bohme, R., and Clayton, R., 2012, "Measuring the Cost of Cybercrime," 11th Annual Workshop on the Economics of Information Security (WEIS 2012).

[12] Richardson, R., 2011, "CSI Computer Crime and Security Survey 2010/2011," Computer Security institute, from http://gocsi.com/survey.

[13] Atzeni, A., and Lioy, A., 2006, Quality of Protection, Springer, New York, NY, Chap. "Why to Adopt a Security Metric? A Brief Survey".

2 Research Motivation, Approach and Goals

2.1 Motivation

The interest expressed in information security was focused on the NIST "Risk Management Guide for Information Technology Systems" [1] , which approaches the issue of information security as a risk management problem. Therefore, a risk assessment is done. Risk is viewed through the lifecycle of an information system, its initiation, development, implementation, maintenance, and disposal phases. That guide takes into consideration threats, threat sources, motivations, threat actions or means of attack, available protection options, and the costs to implement adequate security in the face of the threats. The final output is a cost/benefit analysis that determines an acceptable level of protection to adequately protect a system [2].

This risk assessment consists of nine successive steps:

1. System Characterization – system boundary/ system functions/criticality, and sensitivity of system and data,
2. Threat Identification,
3. Vulnerability Identification,
4. Control Analysis,
5. Likelihood Determination,
6. Impact Analysis,
7. Risk Determination,
8. Control Recommendation, and
9. Results Documentation.

Step 5, Likelihood Determination, was chosen as the essential subject of this research, which deals with the decision of an attacker to launch an attack. According to that NIST Guide, Likelihood Determination or ratings are based on the following three factors:

- Threat-source, motivation and capability,
- Nature of the vulnerability, and
- Existence and effectiveness of current controls.

Are these the only factors contributing to Likelihood Determination? What are the relationships between the different factors? Do effective controls affect operating capability? Would the lack of vulnerability affect an attacker's performance - opportunity and capability - and motivation?

Some important aspects of the nature of vulnerability are dealt with by Bev, et al. [3] in their paper, "Towards Operational Measures of Computer Security", regarding security breaches caused by the presence of vulnerabilities, which are activated/ exploited. Vulnerabilities, which are faults that can affect the security of a system, can be caused either accidentally, due to a mistake in program design, or intentionally. Intentional faults can be caused maliciously, e.g. by insertion of a Trojan horse during any stage of the life cycle of a system, or non-maliciously, e.g. by a deliberate trade-off between security and operating efficiency. Also, activation of or exploiting a vulnerability can be intentional or accidental.

Modeling accidental activation of accidentally inserted vulnerabilities would be based on modeling such risk cases that primarily deal with the nature and accidental causes of failure. However, the focus of this research was on the intentional exploit and the intentional insertion of vulnerability, e.g. a Trojan horse. These are viewed respectively where the goal of the former is to attack the confidentiality, integrity, or availability of some aspect of the system, and the latter as attacking the integrity of the security assumption of the system.

Now, likelihood can be considered as:

- The likelihood of a successful attack, or
- The likelihood of an attempt to attack, which may be successful.

However, this Guide presents a method to calculate risk, which only addresses the likelihood of a successful attack as a function of its impact. This research is broader in scope, dealing with all attempts to attack.

The importance of considering the likelihood of all attempts to attack is that it will include understanding issues related to information security where unsuccessful attacks occur. Although unsuccessful attacks have no impact and therefore do not contribute to risk (see above definition of risk) nevertheless the following are advantages to include unsuccessful attacks.

1. Analysis of all attacks provides understanding the nature of attacks in general, and related system responses. It provides answers to key questions such as what and how did an attacker attack, and which attacks succeeded and which did not.
2. Even unsuccessful attacks can be considered partially successful as they may give value to the attacker. An example is: unsuccessfully guessing passwords is useful to an attacker as the attacker now has smaller pool of passwords to try [3].

3. Unsuccessful attacks can be viewed as precursors to successful attacks. Understanding precursors is key to predicting rare events that have very high impact levels.

2.2 Approach

This research was limited to the initial decision of a threat-source to launch an attack, which includes the nature of the attack. While the likelihood that the success of an attack is of paramount importance, the effort was focused on an attacker's motivation, and on what can be done to discourage an attack. Determination of the qualitative value of individual attackers was emphasized. There is a huge difference between a professional hacker's and an amateur criminal's targeting a system.

Some issues in making that qualitative analysis are the following.

- Recognizing an attack attempt is very difficult as it cannot be distinguished from the normal flow of traffic. Also, an unsuccessful attack may not leave any trace.
- Obtaining attack data is also difficult because the owners of live systems are reluctant to share their security information with researchers.
- Data that may pertain to an attack is difficult to analyze regarding the attacker's motivation. Indeed, motivation is an important issue that was addressed in this research, which dealt with the attacker's perspective.

The principal approach consisted of drawing from information security literature, as well as from criminal justice, social science and logic literature to develop a model of factors and relationships known to influence an attacker and to affect her information security attack. The model, which enables better comprehension of information security attacks from the attacker’s perspective, is demonstrated by factors, or nodes, and their relationships, or links. The nodes and links, identified from this published literature, sufficiently complete and realistic, represent the human decision process leading to information security attacks. This model, rather than being proved or verified from independent empirical evidence based on controlled experimentation, was verified by the multi-disciplinary literature and by information security surveys. Finally, actual case studies of security attack incidents were presented and analyzed, and were shown to exhibit the fitness and usefulness of the model.

This research was generally focused on attacks performed by individuals, not on corporations, government entities and terrorist groups, which are variously noted. Nevertheless many of the principles, issues and conclusions may well apply to all of these groups.

2.3 Research Objectives

The main objective of this research was to build and prove the correctness of a model that explains why an attacker targets a particular target. This is essentially to learn and provide the factors that determine the nature of an attack. The model integrates such factors that contribute positively as well as negatively, and their interrelationships, to the likelihood that the attacker will attempt to attack a particular target, or not attempt at all. It addresses that early stage that culminates in an attacker’s decision to initiate an attack. The relationship between attacker and target, namely the victim, should thereby be better understood because information security studies have not focused in much detail on that early stage, that of the attacker, but emphasize the defensive perspective and posture.

2.4 Goals of this Research

1. Better understand why and how information attacks takes place.
2. Identify attack factors that are most significant, and those that are controllable.
3. Determine relationships between attack factors.
4. Use this knowledge to strengthen the influence of factors that reduce likelihood of attack, and weaken the influence of such factors that increase the likelihood of attack.

2.5 References

[1] Stoneburner, G., Hayden, C., Feringa, A., and National Institute of Standards and Technology, 2004, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A," SP 800-27, U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg, MD.

[2] Butler, S., 2002, "Security Attribute Evaluation Method: A Cost-Benefit Approach," *Proceedings of the 24th International Conference on Software Engineering. ICSE*, **24**, pp. 232-240.

[3] Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., Dobson, J., Mcdermid, J., and Gollmann, D., 1993, "Towards Operational Measures of Computer Security," Journal of Computer Security**, (2) 2-3**, pp. 211-226.

3 Related Work

3.1 Past Work on Information Security Modeling and Metrics

Many proposed methods to determine the level of security, or risk, of information systems, as well as software reliability, are based on models ranging in complexity from ones entailing only single quantity to numerous measurements or tests.

Attack graphs first proposed by Bruce Schneier [1], one the oldest formal methods of describing security of systems, is based on various attacks. The model contains graphically structured tree notation, essentially a fault tree, with nodes representing attacks, and the root node of the tree is the global goal of the attacker. The nodes are different steps to achieve that goal. The lines between nodes represent the paths that an attack can take until it reaches its final global goal. In order to successfully model all attacks that a system can be subjected to, all possible forms of attacks and possible combinations need to be present in this model. The number of nodes and paths between nodes rises exponentially with system complexity. Several researchers have proposed methods to reduce the number of nodes and their interactions, but this is at the expense of not fully modeling all scenarios [2], [3], [4].

Metrics are used to determine the security state of an information system. One such metric, presented by Ross Anderson, counts the number of flaws discovered over a given period, and predicts from that the number of remaining flaws yet to be discovered. It assumes that a system’s security, risk level, is essentially dependent on its vulnerabilities yet to be discovered after the elimination of the discovered vulnerabilities. An Arrhenius type relation, using mean times between failures, discoveries, predicts the number of remaining flaws and hence reliability or risk level [5].

Another metric, presented by Manadhata et al. [6] and Howard et al. [7] determines the number of attack prone surfaces, i.e. interfaces exposed to outside callers or to possible dangerous instructions in the code. The number of features of a system that are attackable is counted, thereby establishing a security or risk level.

Howard et al. essentially address the potential of an attacker to damage a system, but not the quality of the attack prone surfaces to resist attack. Anderson, while predicting number of future vulnerabilities (having removed those discovered) likewise does not address their quality. Also, both do not address other security issues such as an organization's strength of and adherence to its security policy.

Better and more reliable security or risk level metrics were provided by the National Institute of Standards and Technology (NIST) using three frameworks to measure the risk posed by vulnerability.

Risk, R, of vulnerability is defined as the likelihood, L, of an attack based on the vulnerability, and as a function of the expected impact, I, of the attack.

$$R = L \times I$$

One is NIST's Common Vulnerability Scoring System (CVSS) [8], which "provides an open framework for communicating the characteristics and impacts of IT vulnerabilities". The CVSS scores the severity of known software flaws in an application or in an operating system.

Another related framework developed by NIST is the Common Configuration Scoring System (CCSS) [9] “is a set of measures of severity of software configuration issue vulnerabilities”, and it is to “assist organizations in making sound decisions as to how security configuration issues should be addressed, and can provide data to be used in quantitative assessments of the overall security posture of a system”. While CVSS addresses vulnerabilities that are due to flaws in the software, CCSS looks at the vulnerabilities chosen by an administrator when configuring a system.

The third system of this series developed at NIST is the Common Misuse Vulnerabilities Scoring System (CMSS) [10] that determines the impact and likelihood of those vulnerabilities for which “trust assumptions” were made, that they “can be abused in a way that violates security”. These “trust assumptions” may be:

- Explicit, for example, a designer is aware of a security weakness and determines that a separate security control would compensate for it; or
- Implicit, such as creating a feature without first evaluating the risks it would introduce; and/or
- Involve threats that may also change over the lifetime of software, or a protocol used in software.

What is common to these three tools is that they measure the likelihood and impact of known vulnerabilities, which are due to software, configuration or trust assumptions. A score is calculated to assign the risk level of an individual vulnerability, usually a number from zero to ten with ten indicating the highest risk. The individual assessments that the score is derived from are qualitative, and are based on input from security experts. These tools are very good for comparing one vulnerability to another.

NIST and the National Security Agency (NSA) have developed baseline checklists - guides - in order to further harden and secure operating systems and popular applications above their default settings. This is all part of NIST's "National Checklist Program" (NCP). One such guide is the "Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist" [11]. This guide has different recommendations for standalone host environments, enterprise environments, and for three customized environments. Often these settings are so restricting to the point that they prevent the system from performing its intended function, and then the restrictions have to be relaxed.

These guidelines were developed using best practices, by asking experts in the field for suggestions on restrictions needed to address most known and unknown vulnerabilities. They have been verified partially for future attacks by showing that had they been followed before certain widespread and destructive vulnerabilities were discovered, the system would have been protected. An example is the case of the July, 2001 Code Red Virus which affected millions of computers and caused billions of dollars of damage worldwide. This virus accessed a little used UDP port for SQL servers to affect its victims [12]. Computers which followed guidelines that shutdown unused ports, which included that UDP port, were unaffected by Code Red Virus.

Common Criteria [13] and Trusted Computer System Evaluation (TCSEC), The Orange Book [14], are frameworks whose output gives accreditation that assures that a given system meets a specified level of security. The user of these systems will determine what level of security assurance is required and therefore specify only products that meet or exceed the specified security. However, while there is a standard in place to evaluate the security of the system, there is no standard to evaluate the threat level. Also, the environment can be dynamic, and changes in configuration and usage, and upgrades will cause a system to lose its accreditation.

John McCumber [15] presents a security model that can be visualized as a cube. The cube contains:

1. Security Goals:
    a. Confidentiality,
    b. Integrity and
    c. Availability;
2. Information States:
    a. Storage - data at rest, information stored in memory on a disk,
    b. Transmission - transferring data between information systems and
    c. Processing - performing operations on data; and
3. Safeguards:
    a. Policy and procedures,
    b. Human factors and
    c. Technology.

McCumber's cube looks at the inter-relationship between those impacts the defender wishes to avoid (Goals), which part of the system needs that protection (Information States) and how the defender will actually secure his system (Safeguards). In this way McCumber looks beyond a "checklist" and accreditation, which concentrate on safeguards and vulnerability prediction, and on vulnerability evaluation which concentrates on the threats to the system.

While McCumber's models address interrelationships from the defender's perspective they do not address the attacker's perspective, namely, the attacker's motivation to attack and his available resources to succeed in his attack.

3.2 Typical Crime Theories Pertaining to Model Development

3.2.1 Classical Deterrence

Classical Deterrence theory, which is rooted in classical criminology, assumes that a decision to perpetrate a crime or to abstain from it is based just on maximum benefits and minimum cost, pleasure versus pain. This is a very old theory and can be noted from 18th century publications by Cesare Beccaria (1738-1794) [16] and Jeremy Bentham (1748-1832) [17] on crime principles. Cost, i.e. pain, is defined as formal punishments. The cost factor includes the certainty and swiftness of the punishment, besides its level or severity. According to this theory, and often a public perception, a specific crime can be prevented by raising likelihood, immediacy and severity of its consequent punishment.

Raymond Paternoster, 2010 [18], deals with the deterrence theory of crime, and its history, "its general ill-repute before the mid twentieth century, and subsequent resurgence". The latter is found in the works of Jack P Gibbs [19] and Gary S Becker [20].

3.2.2 Victimological Theories

Victimological theories deal with the relationship between the criminal and the victim. Studies have shown that often a criminal and victim have similarities relevant to the crime. A British Crime Survey, Chambers and Tombs, 1984 [21], showed that 40% of respondents who admitted committing an assault had been previously assault victims.

This can be due to that victimization can create motivation and rationalization to commit crime, Fattah, 1993 [22]. In some cases a delinquent lifestyle has been found to be common to a criminal and victim, Jensen and Brownfield, 1986 [23].

3.2.3 Routine Activity Theory

Routine Activity theory emphasizes a criminal's opportunities to commit a crime, Felson [24]. This theory states that a crime opportunity presents itself coincidentally with "a likely offender, suitable target, and the absence of a capable guardian against the crime". These were outstanding factors in the model development. Felson emphasized that a "likely offender" could be "anybody for any reason might commit a crime", deemphasizing particular motivation. Use of the words "suitable target" instead of "victim" further deemphasizes motivation, particular motivation such as hate. Regarding the third element "absence of a capable guardian against crime", Felson uses "capable guardian" instead of "police" or "criminal justice" to deemphasize the traditional concept of traditional consequences deterring crime. However, one cannot avoid consideration of consequences as a deterrent to a criminal

3.2.4 Rational Choice Theory

The model was very much shaped by Rational Choice theory. This theory offers the perspective that a criminal "makes a choice to committing a crime in order to maximize satisfaction by choosing one of a finite set of alternatives, each with its particular costs and benefits." The choice to undertake specific criminal activity occurs "when the legal options are less rewarding for the individual or when the crime is less punishing", Clarke and Felson, 1993 [24].

However, use of this theory has to recognize the imperfect nature of decision making, Piquero, Exum and Simpson [25]. These are some of the imperfections.

- Imperfect conditions that crime occurs,
- Human beings are imperfect in their decision ability and predictability regarding a single matter, and

Decisions are made, and actions are undertaken with inadequate information.
Section 4.39 contains a discussion about the reason for the appropriateness of Rational Choice theory. Section 4.40 has a discussion about how Rational Choice and other criminology theories tie into the General Influence Model.

Professors Ray Paternoster and Sally Simpson, 1996 [26], applied the Rational Choice theory to corporate crime in a study of 96 MBA students and executives. Actually both types of crime are similar, the former benefiting a corporation, the latter an individual. The goal of their work was to determine if and how much of a role do punishments have in a corporate offender's "rational choice" in deciding to commit a crime involving the corporation.

These 96 participants were given sample scenarios to judge how likely they would commit one of four corporate offenses: (1) price fixing, (2) bribery, (3) manipulation of sales statistics, and (4) violation of Environmental Protection Agency (EPA) emissions. Based on the responses the researchers concluded the following.

1. "The decisions whether to commit corporate crime were significantly affected by perceived incentives and disincentives of the act, the organizational context, and the moral climate of the firm."

2. “The moral climate of the organization also had an effect on expressed intentions.”
3. Formal and informal, Section 4.33.1 and Section 4.36.1, and loss of self-respect consequences had statistically significant effects on likelihood to commit a crime.
4. “Intentions to commit corporate crime are higher when the act was thought to result in personal career advancement, and itself was perceived to be pleasurable (thrill).”

These authors noted that in the past “most empirical studies have found either no or very weak and conditional support for the deterrence of corporate crime”. However, Block, Nold, and Sidak, 1981 [27] had found that certainty and severity of civil sanctions were effective in preventing such crimes. Simpson and Koper, 1992 [28], had previously found in a study of 38 offending companies that the severity of formal sanctions did inhibit corporate offences, but only among a small group of these offending companies that had been once caught previously.

Paternoster and Simpson, 1996 [26], noted that such studies in the past had missed consideration of the effects of certain informal punishments in the case of corporate crime, namely shame and embarrassment which can be a very powerful deterrent for a corporation. Companies generally value a good name and reputation as primary assets. By including consideration of informal sanctions, moral evaluations and organizational factors, they showed that corporate crime also follows the results expected from a rational choice cost-benefit analysis.

Like white collar crime, cyber-crime is generally committed for the benefit of the individual offender and his/her close associates. Therefore, deterrence such as physical and monetary punishment and shame can only be assessed according to the individual attacker's perspective. Exceptions for this computer crime generalization will be crimes committed for political or nationalistic reasons where trust and political expediency issues can dominate.

It is then compelling to note that cyber-crime, is in many ways similar to white collar crime, and accordingly could also utilize Rational Choice theory, as well as applicable aspects of the other crime theories. The victims of both crimes are physically distant from their attackers. Both have unclear laws to define right and wrong, and some laws are untested. Regarding white collar crime, "Importantly, illegal behavior in this context often emerges out of legally grey area places where the law is unclear or when common organizational practices discredit the significance of the violation", Piquero, Exum and Simpson, 2005 [25]. White collar crime according to Kadish, 1977 [29], is "calculated and deliberative, and directed to economic gain". Computer crime, however, is also "calculated and deliberative" although it is not only for economic gain.

Generally, white collar and cyber-crime offenders do not have a previous history in other areas of crime.

Morality and sanctions considerations, with some notable exceptions, are likely deterrents to these crimes.

3.2.5 Situational Crime Prevention

Clarke [30] deals with stressing the creation of conditions external to the criminal that would specifically reduce the opportunities to commit crime. Felson [31] notes in this connection the effectiveness of "making each criminal act appear difficult, risky, unrewarding and inexcusable".

3.2.6 Low Self-Control Theory

Low Self-Control theory has been applied to the understanding certain aspects of crime. Gottfredson and Hirschi [32] present six different traits of individuals who are unable to resist temptations towards criminal behavior.

1. Impulsivity.
2. A preference for simple tasks, oriented towards short term results.
3. Risk-seeking.
4. Physicality, tend to engage in physical activities rather than mental activities.
5. Self-centeredness, insensitive towards others.
6. A bad temper.

This theory and the Desire for Control theory, immediately below, in contrast to the other crime theories emphasize deviant characteristics of a criminal, essentially dealing with the "individual personality" according to Piquero, Exum and Simpson [25]. However they and others found that the Low Self-Control theory could not be successfully applied to white collar or corporate crime: Benson and Moore, 1992 [33]; Geris, 2000 [34]; Reed and Yeager, 1996 [35]; Simpson and Piquero, 2002 [36]; and Weisburd and Waring, 2001 [37]. This conclusion is explained by the following.

1. "Irrespective of their involvement in crime, their lives do not appear to be very different from those of law-abiding citizens……such involvement is often an aberration on a record that is otherwise characterized by conventionality," [37].
2. White collar occupations generally favor individuals who possess traits such as the ability to defer gratification, and willingness to defer to the interest of others.

3.2.7 Desire for Control (DC) Theory

The Desire for Control theory which deals with is a general wish to be in control over everyday life events. Burgher and Cooper, 1979 [38], describe people who are characterized by this desire as:

> "……..assertive, decisive, and active. They generally seek to influence others when such influence is advantageous. They prefer to avoid unpleasant situations or failures by manipulating events to ensure desired outcomes. These persons usually seek leadership roles in group situations."

Such people tend to attribute their successes to "stable" internal factors such as skill, knowledge and effort, and their failures to "unstable" external factors such as bad luck. They choose goals for themselves that they are unable to achieve. Finally, they tend to overestimate their own ability and influence, and thereby create in their mind an "illusion of control". It is because of this "illusion of control" that such people tend to risky behavior in order to achieve their goals.

Piquero et al. [25] contrast corporate criminals according to their high desire for control and low self-control, the former trait causes concern with both the immediate and future impacts of their actions, and the latter only with the present. These authors concluded the following regarding the desire for control trait.

1. It is a positive factor associated with the occurrence of corporate crime.
2. Such a criminal's, or a potential criminal's level of desire for control influences the manner in which his rational choices are made. Since a high degree of desire for control can be accompanied by concern for future consequences, severe and certain informal sanctions deter such criminality when the sanctions are against the individual or the corporation. On the other hand, crime is surprisingly not deterred when the consequences are formal sanctions and applied only against the individual, but are still deterred when they are applied against the corporation.

It has to be cautioned that traits such as low self-control and desire for control associated with criminal behavior are not abnormal. Rather these traits are common traits among normal people and are often desirable traits, but they are prevalent among criminals engaged in particular crimes.

Criminologists such as Cornish and Clarke, 1986 [39], Hiroshi Tsutomi, 1991 cited by Clarke and Felson p. 229, and Sutherland and Cressey, 1974 [40], are very critical about associating criminal behavior with abnormal traits. There are numerous studies and experiments that proved that normal people are capable of extreme acts of atrocity and cruelty: Milgram, 1969 [41]; Zimbarbo, 1972 [42] and Fattah, 1992 [22].

3.2.8 Other Crime Theories

Wilson and Herrnstein, 1985, pp. 63-66 [43] quote and elaborate on Hirschi, 1969, p. 3 [44], to explain three groupings of criminal theories:

1. Strain or motivational theories – people commit crimes because they are unable fulfill their desires using legal methods.
2. Control theories - people commit crimes because their ties to conventional order are broken.
3. Culture deviance theories – people commit crimes because they prescribe to a set of standards not accepted by the rest of society.

Motivational theories assume that one will generally obey societal rules, but will only violate them if otherwise is unable fulfill ones desires. This is a basis of "conscience", where one naturally knows the difference between right and wrong.

Social control theories assume that people learn the differences between right and wrong. This learning can emerge from either religious and/or secular philosophy. When this social control bond breaks down criminal behavior can occur. This will explain why apparently moral individuals will engage in computer crime even when there is not any great reward for that behavior. It can be remoteness from a victim and unclearness of the law which create a weakness in social control bonds that allow criminal behavior to occur.

Culture deviance theories assume that some people in some circumstances learn deviant behavior, often from other offenders. This becomes their morality and therefor they are not inhibited to commit a crime. This explanation maybe salient to explain behaviors associated with "hacker" groups who have their own set of set of rules, "morals".

3.3 Information Security Using Criminology Theories

Ransbotham and Mitra [45] dealt with the essentially two paths that cyber-attacks take place, deliberately targeted and opportunistic-random, which are highlighted subsequently in the model as planned and random attacks. They developed a model applying several typical crime theories, principally Rational Choice, to explain the role of attractiveness of the target to the attacker and effectiveness of counter measures in deterring attacks. A large alert dataset was used, 847 million security alerts between January 2006 and December 2006, to empirically prove parts of this model. They proposed a theory that chance, random, attacks evolve into deliberate attacks - a merging of these paths; that theory was only partially supported by this data set.

Robert Willison [46] used the theory of Rational Choice and situation crime prevention to understand the "insider" threat to information systems. He developed a cost-benefit analysis using the Rational Choice perspective for the "insider" threat, where attacks occur in stages, each sub-attack leading to the final attack. Then, looking at the unique opportunities presented by being an "insider" he presented situation crime prevention to reduce these opportunities. In his conclusions he noted that studies into understanding drunk driving crimes, sexual assault, tax evasion and corporate crime may have relevance in understanding IS crime.

Another group of researchers, Dantu, Loper and Kolan [47], stated that although there is great deal of psychological and criminological research for typical crime, security engineers do not use these studies. They started with three factors that exist in typical crime: (1) skill which includes the knowledge of the attacker, (2) tenacity, a level of effort and persistence of the attacker, and (3) cost to perform the attack. They assumed probabilistic values for each of these factors in cyber-attacks which make it more or less likely that an attacker will attempt to attack a system. They used these factors to build Bayesian Belief Network based on an attack graph for particular attack paths. While the application of the factors to model cybercrime is most intriguing, and is the focus of their paper, how the model factors were derived and their respective levels of importance were not discussed.

3.4 References

[1] Schneier, B., 1999, "Attack Trees: Modeling Security Threats," Dr. Dobb's**,** December.

[2] Ammann, P., Wijesekera, D., and Kaushik, S., 2002, "Scalable, Graph-Based Network Vulnerability Analysis," *Proceedings of the 9th ACM Conference / Computer and Communications Security (CCS '02)*, pp. 217-224.

[3] Mauw, S., and Oostdijk, M., 2006, "Foundations of Attack Trees," Report No. 3935, Springer-Verlag, New York.

[4] Sheyner, O., Haines, J., Jha, S., Lippmann, R., and Wing, J. M., 2002, "Automated Generation and Analysis of Attack Graphs," *2002 IEEE Symposium on Security and Privacy*, pp. 273-284.

[5] Anderson, R., 2001, "Why Information Security is Hard - an Economic Perspective," *Computer Security Applications Conference*, pp. 358-365.

[6] Manadhata, P., Tan, K., Maxion, R., and Wing, J.M., 2007, "An Approach to Measuring a System's Attack Surface," CMU-CS-07-146, Carnegie-Mellon University School of Computer Science Defense Technical Information Center, Pittsburgh PA.

[7] Howard, M., Pincus, J., and Wing, J., 2005, *Computer Security in the 21st Century*, Springer, New York, NY, Chap. "Measuring Relative Attack Surfaces".

[8] Mell, P. and Scarfone, K., 2011, "CVSS v2 Complete Documentation," from http://www.first.org/cvss/cvss-guide.html#n1.

[9] Mell, P., and Scarfone, K., 2010, "The Common Configuration Scoring System," NISTIR 7502, National Institute of Standards and Technology, Gaithersburg, MD.

[10] Van Ruitenbeek, E., and Kent, K., 2009, "The Common Misuse Scoring System (CMSS) Metrics for Software Feature Misuse Vulnerabilities," NISTIR 7517, National Institute of Standards and Technology, Gaithersburg, MD.

[11] Scarfone, K., Souppaya, M., and Johnson, P., 2008, "Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist," Special Publication 800-68 Revision 1, National Institute of Standards and Technology, Washington DC.

[12] Moore, D., Shannon, C., and Claffy, K., 2002, "Code-Red: A Case Study on the Spread and Victims of an Internet Worm," *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment*, pp. 273-284.

[13] 2012, "Common Criteria v3.1 Release 4," from http://www.commoncriteriaportal.org/cc/.

[14] National Security Agency, 2003, "NSA/NCSC Rainbow Series," from https://www.fas.org/irp/nsa/rainbow.htm.

[15] McCumber, J., 2005, *Assessing and Managing Security Risk in IT Systems: A Structured Methodology,* Auerbach Publications, Boca Raton, FL.

[16] Beccaria, C., Voltaire, Parzen, J., and Thomas, A., 2008, *On Crimes and Punishments and Other Writings*, University of Toronto Press, Toronto Ont.

[17] Bentham, J., and Bowring, J., 1843, *The Works of Jeremy Bentham,* W. Tait, Edinburgh.

[18] Paternoster, R., 2010, "How Much do we really Know about Criminal Deterrence?" Journal of Criminal Law and Criminology**, (100) 3**, pp. 765-824.

[19] Gibbs, J., 1975, *Crime, Punishment, and Deterrence,* Elsevier, New York.

[20] Becker, G., 1976, *The Economic Approach to Human Behavior*, University of Chicago Press, Chicago.

[21] Chambers, G., and Tombs, J., 1984, "The British Crime Survey Scotland," Scottish Office, Central Research Unit, H.M.S.O., Edinburgh.

[22] Fattah, E., 1992, *Towards a Critical Victimology,* St. Martin's Press, New York.

[23] Jensen, G., and Brownfield, D., 1986, "Gender, Lifestyles, and Victimization: Beyond Routine Activity." Violence and Victims**, (1) 2**, pp. 85-99.

[24] Clarke, R., and Felson, M., 2004, *Routine Activity and Rational Choice. Vol. 5,* Transaction, New Brunswick, N.J.

[25] Piquero, L., Lyn, E., and Simpson, S., 2005, "Integrating the Desire-for-Control and Rational Choice in a Corporate Crime Context," Justice Quarterly**, (22) 2**, pp. 252-280.

[26] Paternoster, R., and Simpson, S., 1996, "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," Law & Society Review**, (30) 3**, pp. 549.

[27] Block, M., Nold, F., and Sidak, J., 1981, "The Deterrent Effect of Antitrust Enforcement," Journal of Political Economy**, (89) 3**.

[28] Simpson, S., and Koper, C., 1992, "Deterring Corporate Crime," Criminology**, (30) 3**, pp. 347-376.

[29] Kadish, S., 1977, *Encyclopedia of Crime and Justice*, Free Press, New York.

[30] Clarke, R., 1997, *Situational Crime Prevention: Successful Case Studies,* Harrow and Heston, Guilderland, NY.

[31] Felson, M., 1994, *Crime and Everyday Life : Insights and Implications for Society,* Pine Forge Press, Thousand Oaks, CA.

[32] Gottfredson, M., and Hirschi, T., 1990, *A General Theory of Crime,* Stanford University Press, Stanford, CA.

[33] Benson, M., and Moore, E., 1992, "Are White-Collar and Common Offenders the Same? an Empirical and Theoretical Critique of a Recently Proposed General Theory of Crime " Journal of Research in Crime and Delinquency**, (29) 3**, pp. 251-272.

[34] Geis, G., 2000, "On the Absence of Self-Control as the Basis for a General Theory of Crime," Theoretical Criminology**, (4)** February, pp. 35-53.

[35] Reed, G., and Yeager, P. C., 1996, "Organizational Offending and Neoclassical Criminology: Challenging the Reach of a General Theory of Crime," Criminology**, (34) 3**, pp. 357-382.

[36] Simpson, S., and Piquero, L., 2002, "Low Self-Control, Organizational Theory, and Corporate Crime," Law and Society Review**, (36) 3**, pp. 509-548.

[37] Weisburd, D., and Waring, E., 2001, *White-Collar Crime and Criminal Careers,* Cambridge University Press, New York.

[38] Burgher, J., and Cooper, H., 1979, "Motivation and Emotion," Society for the Study of Motivation**, (3) 4**, pp. 381.

[39] Cornish, D., and Clarke, R., 1986, *Reasoning Criminal - Rational Choice Perspectives on Offending,* Springer-Verlag, New York.

[40] Sutherland, E., and Cressey, D., 1974, *Criminology,* Lippincott, Philadelphia.

[41] McLeod, S., 2007, "The Milgram Experiment," from http://www.simplypsychology.org/milgram.html.

[42] Zimbardo, P., 2008, *The Lucifer Effect: Understanding how Good People Turn Evil.* Random House Trade, New York, NY.

[43] Wilson, J.Q., and Herrnstein, R., 1985, *Crime and Human Nature,* Simon and Schuster, New York, NY.

[44] Hirschi, T., 1969, *Causes of Delinquency.* University of California Press, Berkeley.

[45] Ransbotham, S., and Mitra, S., 2009, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," Information Systems Research**, (20) 1**, pp. 121-139.

[46] Willison, R., 2006, "Understanding the Perpetration of Employee Computer Crime in the Organisational Context," from http://openarchive.cbs.dk/bitstream/handle/10398/6463/wp_2006_004.pdf?sequence=1.

[47] Dantu, R., Loper, K., and Kolan, P., 2004, "Risk Management using Behavior Based Attack Graphs," *Proceedings of the ITCC 2004 International Conference on Information Technology: Coding and Computing***, 1**, pp. 445-449.

4 General Influence Model

4.1 Introduction to General Influence Model

The model, essentially a general influence model, was constructed by integrating a cyber-attacker's motivation, opportunities to attack and perceived deterrence, and the various other factors that comprise these three factors, to determine the nature of an attack. These factors are represented as nodes which are often called variables. They may influence the attacker's decision positively, to attack, or negatively, to withhold from attacking. Any one of these factors themselves does not necessarily influence the final goal directly, but rather influences other factors. See Mohaghegh-Ahmadabadi, 2007 [1].

4.2 Structural Essentials of the General Influence Model

The influence model contains two constructs, nodes and links between nodes. The nodes represent the factors that are being modeled, and they are detailed by sub-factors that are also nodes.

An ellipse or circle is used to represent a node, or a pentagon is used for convenience to represent a hierarchy of nodes, and is subsequently expanded into ellipses or circles, Figure 1 .

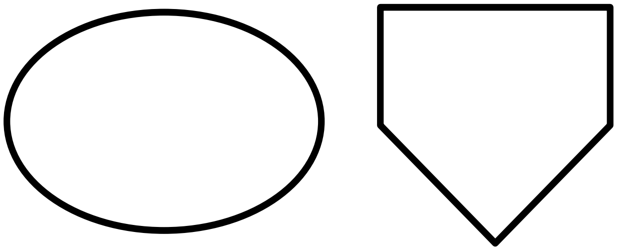


Figure 1: Representation of a Node

The link construct is between two factors, nodes, representing the influence between the two factors, and is a straight line directed with an arrow (factor “B” influences factor “A”), Figure 2. When the link is between a sub-factor and its parent factor, then it is a dashed line with an arrow representing a detail or decomposition of the parent factor (factor “B1” is part of factor “B”), Figure 3.

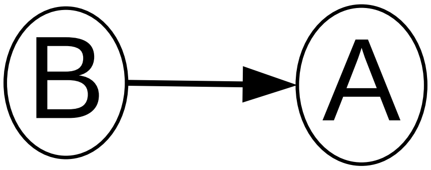
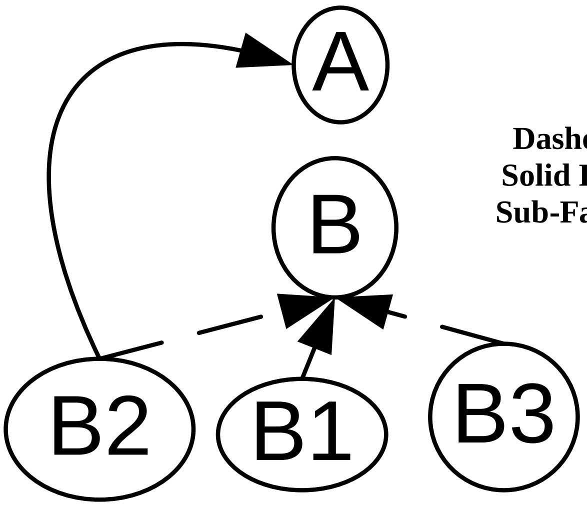


Figure 2: Factor "B" Node Influences Factor "A" Node



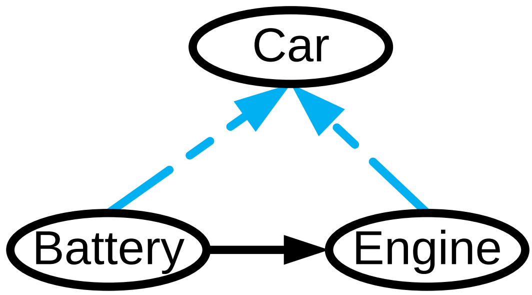
Dashed Line: Parts Relationship
Solid Line: Influence Relationship
Sub-Factor B2 Influences Factor A

Figure 3: Links between Nodes

Adding this higher level of detail to the factors allows for more specific representation of the influence between factors. Here factor “B” is detailed by “B1”, “B2”, and “B3”, and only sub-factor “B2” influences factor “A”.

Details or decomposition of a node can be presented in a number of ways, such as, in the case of a “car” node by the following.

1. Classification. It can be decomposed into “sedan”, “station wagon”, “minivan”, etc., a broken purple link — — → ;
2. “Parts of”. It can be decomposed into its parts - wheels, battery, engine, doors, body, etc., a broken blue link, Figure 4; — — → , and
3. Attributes. It can be detailed by describing some or all of its attributes or properties, e.g. color, speed, popular model, etc., a broken green link — — → .



Car has a Parent-Child Relationship with Battery and Engine.
Battery has an Influence Relationship with Engine.

Figure 4: Relationships between Nodes.

Here on, the word “influence” indicates a relationship where one independent node has an effect on the value of another node. In the case of the car, one part can influence another, the battery can influence the engine and color can influence a popular model.

But, generally, classification and attributes such as station wagon, wheel or speed, do not influence car, where these are defining or parent-child relationships.

4.3 Root Nodes of the General Influence Model

There are three root nodes that determine the nature of cyber-attack, Figure 5. They are:

- **Motivation** - willingness to attack based on perceived gains for or goals of an attacker.
- **Opportunity** - situation or condition favorable for attainment of a goal.
- **Deterrence** – factors that discourage an attacker from carrying out an attack.

The explanations of these root nodes and their sub nodes will follow. This relationship of the root nodes is presented in Felson and Clarke, Opportunity Makes the Thief: Practical Theory for Crime Prevention, 1998 and Felson, Crime and Everyday Life, 1994[1] [2, 3], as pertaining in general to criminal behavior, and is directly applicable to information security attacks.

[1] (Felson, Crime and Everyday Life, 1994) develops Routine Activity Theory and the Basic Crime Triangle consisting of three parts: (1) likely offender (*Motivation*), (2) suitable target (*Opportunity*) and (3) capable guardian (Deterrence)

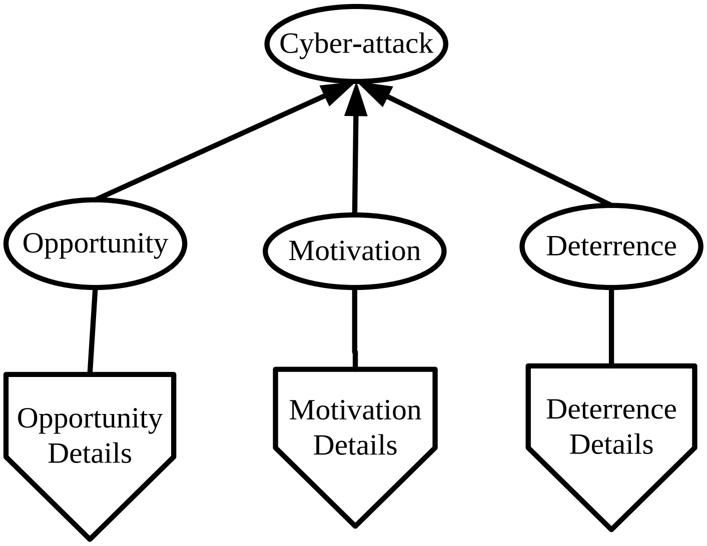


Figure 5: Root Nodes for a Cyber-attack

4.3.1 Attackers

However, the nature of the attacker must be considered regarding these three root nodes, factors, especially motivation. Cyber-attackers are classified in groups to distinguish between their motivations to commit this crime, their ability, and their relationship to the victim(s), Wikipedia [4]. Marcus K. Rogers [5] divides computer criminals into six classes, differentiated by motives and skill level.

1. Script kiddies are individuals with limited technical knowledge and ability. They are generally immature, ego boosting and thrill seeking.
2. Cyber-punks are similar to the script kiddies but have a clear disrespect for authority; they are more sophisticated and technically capable than script kiddies.
3. Hacktivists are individuals who justify their destructive behavior with a civil disobedience label, ascribing political and moral correctness to their behavior.
4. Virus writers are technically savvy; they create exploits, often for the mental challenge and academic exercise, but without a desire to harm others.

5. Professionals are highly skilled; they are willing to sell information and intellectual property to the highest bidder.
6. Cyber-terrorists are soldiers or freedom fighters of a nation or state in the cyberspace battlefield.

The following four cyber-attacker classifications were chosen for this research, similar to those given by Marcus K. Rogers, and also by Stonebruner et al. [6][2].

1. **Amateur -** a computer criminal, also known as script kiddie, is one who may be new to the field of computer hacking, or is not fully committed to it. The amateur does not have advanced computer skills, and lacks a sufficient tenacity level of participation in the crime. An **advanced amateur** has advanced computer skills, but lacks propensity for crime. An amateur's chief goal is satisfaction in meeting a challenge (getting bragging rights), through the means of destruction or disclosure of information.
2. **Professional -** a **c**omputer criminal, essentially a professional version of the amateur. He or she has a propensity for criminal behavior, and has much of the required computer knowledge and skills. This criminal is willing to spend the time and effort in order to achieve the goal of monetary gain or, in the case of the hacktivist, political gain. The professional uses the means of destruction of information, disclosure of information, or data alteration.

[2] NIST Risk Management SP 880-30 classifies information attackers into five classifications: (1) Hacker, cracker; (2) Computer criminal; (3) Terrorist; (4) Industrial espionage attackers for companies and foreign governments; and (5) Insiders.

3. **Terrorist/Government Attacker -** highly motivated and often possessing unlimited resources. He or she is chiefly motivated by political or religious reasons or both. Consequences and morality factors are frequently not adequate deterrents for the terrorist. Here the goal is political domination, through the means of destruction of information, disclosure of information, and blackmail.
4. **Insider Attacker -** a strategically placed person with full accesses to a system, who has decided to use the knowledge and trust that he or she possesses to the detriment of the system. The insider attacker may be simultaneously one of the above mentioned criminals. Typically, this attacker is a disgruntled employee, motivated by revenge. He or she attempts to launch attacks to achieve the goal of retaliation through the means of destruction of information, disclosure of information, or data alteration.

The Low Self-Control and Desire for Control theories applied to crime impact the amateur and professional cybercriminals, who represent most cyber offenders.

The ordinary amateur computer criminal has low self-control. Because he does not have much experience he will act impulsively to test the latest attack methods without fully understanding their ramifications. Also, because of his lack of experience he will "prefer simple tasks" and automated tools to perform an attack. He seeks to prove to himself that he is better than he really is. That is essential to his "risk seeking".

An amateur computer criminal may also have the desire-to-control trait included in his goal in proving that he/she is able to penetrate computer systems and make changes. This control is often a false sense of control, an “illusion of control”, as the amateur does not have the expertise to accomplish his goals. Piquero et al. [7] note having both the “desire for control” and “low self-control” is not a contradiction.

The advanced amateur and professional computer criminals do not display impulsiveness, which is an element of low self-control, as they spend much time planning their crimes. Also, these criminals, who are sophisticated, will not necessarily use simple tasks if they believe that a more complicated operation is more likely to achieve their goals. Physicality plays a very small role in their computer crimes, which are primarily done through software.

On the other hand risk-seeking and self-centeredness are important elements in the professional computer criminal’s behavior. He understands the risks very well and the rewards for the computer crime that he contemplates. Therefor he is very self-centered about the monetary gain that he will acquire from succeeding. But, this blinds him from the risk consequences and moral aversion to committing that crime.

Therefore, it follows that the advanced amateur and professional cybercriminal will synchronize with Rational Choice theory, since each performs a cost/benefit analysis before deciding to launch a cyber-attack.

The advanced amateur and professional computer criminals are very similar to white collar criminals as all are not impulsive, but are future minded. Sutherland’s, 1949 [8], definition of white collar crime as “crime committed by a person of respectability and high social status in the course of his occupation” will apply equally to these computer criminals.

It is reasonable to expect that the desire to control trait could be a part of the professional computer criminal’s profile.

Low self-control explains the ordinary amateur’s cybercrime because of the attacker’s impulsivity, and lack of motivation to enhance her skills or assume risks. Common amateur cyber-crime can also be explained using the Rational Choice theory which assumes that the criminal’s decision making is "bounded" [9] by imperfect information, conditions, and decision makers. The ordinary amateur *is* in fact making a decision to attack a system, provided that there is not much of risk of consequences (certainty) and only minimum effort is required in order to experience the thrill of hacking.

4.3.2 Format of Node Presentations and Explanations

The format used in the presentation of the nodes includes the following.

- **Definition of a node.** This includes an explanation. Most nodes have a white background, being from the attacker’s perspective. A blue background connotes the defender’s perspective.
- **Existence of a node and its causal relationships to other nodes.** This includes showing the existence of a particular node, based on literature in information systems, criminology, and social sciences. Its causal relationships to other nodes are explored. The degrees of these relationships and whether they yield positive or negative effects are also evaluated.
- **Discussion of a node.** Here further discussions include methods from the defensive perspective to minimize the negative consequences of the node, dissenting views on the causal relationships to other nodes, and instances where a node may have different causal relationships.

Some of the presentations on existence of nodes and their causal relationships to other nodes are long, and will be broken up into separate sub-chapters. Also, some nodes will not have a separate discussion.

4.4 Motivation Node

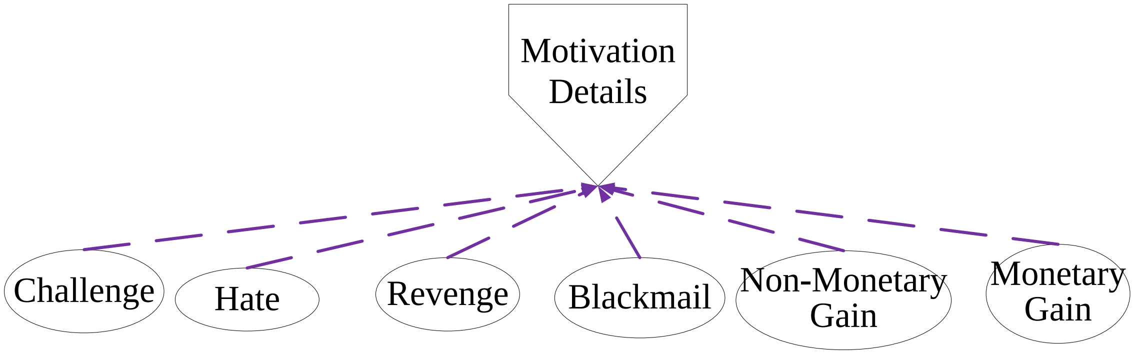


Figure 6: Motivation Node and its Sub-nodes

4.4.1 Definition

Motivation is a willingness to attack based on perceived gains or needs of an attacker. Accordingly motivation is defined in terms of its goal, Figure 6. Marcus K. Rogers [5]stated regarding cyber-crime, “Classifications of motivations must be based upon goals, *rather than upon instigating drives or motivated behavior”* (author’s emphasis). Accordingly, this research was focused primarily on the objective goals of the attacker, rather than on any emotional “needs”.

The following are details of the motivating goals depicted in Figure 6.

1. **Monetary Gain** is a goal that entails direct financial gain for an attacker. An example would be obtaining funds via unauthorized transfer from a bank.
2. **Non-Monetary Gain** is any perceived non-financial gain, such as political power, social enhancement, or sexual favors.

3. **Blackmail** is threatening to damage a system, in order to extract financial, political, or social gain.
4. **Revenge** is the infliction of damage or injury as a response to an actual or perceived hurt.
5. **Hate Crime** is crime motivated by hatred or prejudice.
6. **Challenge** is the test of one's ability to successfully attack a protected system; the achievement of meeting the challenge gives one "Bragging Rights".

Although blackmail, revenge, hate and challenge are included under the rubric of non-monetary gain, they are dealt with separately because of their uniqueness.

However, one would be remiss in disregarding entirely the role that emotional needs play in influencing goals. According to A. Maslow [10] motivating goals satisfy the following hierarchy of needs, in decreasing order of importance, with lower needs on the hierarchy coming to the fore once the higher needs have been met:

1. Physiological needs, often called the hunger needs requirements for human survival; these include air, water, food, clothing and shelter.
2. Safety needs, or the desire for feelings of safety and security in one's environment; these include personal security, financial security, health and well-being.
3. Love needs; these include friendship, intimacy and family.
4. Self-esteem needs; these include the desire for a stable, firmly based, high evaluation of oneself, self-recognition, and self-respect.
5. Self-actualization; this refers to the desire for self-fulfillment, or the tendency to become actualized in what one is potentially.

4.4.2 Existence and Causal Relationships to Information Security Attacks

Consequently, the root node, motivation, and its sub-nodes, Figure 6, are related to one or more of the above needs. The needs, influencing the willingness to attack, will be affected positively or negatively by the opportunity and by the deterrence nodes, which entail the availability or inaccessibility of goals.

The six goals listed in Figure 6 are essentially consistent with Marcus K. Rogers' list of four motivations or goals for computer crime [5].

1. Financial
2. Notoriety
3. Revenge
4. Curiosity

The definition of notoriety can be expanded to include goals of non-monetary gain. Conversely, financial motivation refers to all goals of monetary gain. Revenge includes hate crimes, and curiosity is essentially similar to challenge.

Either goal of monetary or non-monetary gain could include blackmail.

4.4.3 Discussion

The nature of the attacker, one or more of the four attackers in Section 4.3.1, is vital in formulating motivation and its sub-factors, sub-nodes, considering a cyber-attack. The subsequent sections on specific motivation goals will best describe the various facets of motivation.

4.5 Monetary Gain Node

4.5.1 Definition

The goal of this node is financial return for an attacker, encompassing:

- Direct monetary gain, such as through unauthorized transfer of funds;
- Disclosure of information that can be later used for financial gain, for example, through the stealing of credit card information that will be sold or used for lucrative purposes; and
- Obtaining sensitive and private information, e.g. trade secrets, that can be used for competitive advantage.

4.5.2 Existence and Causal Relationships to the Motivation Node

Primarily, the physiological need cited for the motivation node is the basis for monetary gain.

The three aspects of the goal of financial return impact in turn upon the following.

- Confidentiality. Victim's confidentiality is affected by the disclosure of financially potential information, including credit card information and trade secrets.
- Integrity. Victim's integrity is affected by the changing of records, including unauthorized transfer of funds.

Confidentiality and integrity are associated, respectively, with the data disclosure and destruction of information discussed in the means sub-node of opportunity, 4.20.

Monetary gain is a very significant goal for computer crime. Despite this fact, the 2011 CSI survey and Verizon/USSS (United States Secret Service) report [11, 12], showed a decrease in financial fraud attacks. However, the decrease can be explained by the following.

1. Companies are unwilling to report attacks that result in financial loss, since the losses may be an embarrassment to them.
2. The recent discovery and prosecution of large computer crime rings, such as that led by Gonzalez, 5.6 may have only temporarily reduced monetary gain attacks.
3. Financial institutions are taking security more seriously and making themselves more difficult targets for would-be attackers.

A subsequent Verizon Data Breach of Investigation Report [11] showed a strong return to financial fraud attacks, bearing out the assumption that the previous observed decrease was only temporary.

4.5.3 Discussion

Monetary gain crime is frequently made attractive by the availability of extensive underground buyer-seller markets, notably those for credit card information and personal identification information, which aids in identity fraud [13]. Franklin and Paxson [14] in their research of underground markets, suggest countermeasures to remove the marketability of stolen information. Among the anti-profiteering measures is the closing of underground markets by apprehending and prosecuting the market participants, both buyers and sellers. Additionally, these markets can be disrupted by others feeding them false information, thereby breaking mutual trust between participants. Similarly, Michael

Sutton, in his work, “Stolen Goods Market” [15] , suggests disruption of “fencing”, the receiving and selling of stolen goods, as an effective method of reducing marketing crimes.

4.6 Non-Monetary Gain Node

4.6.1 Definition

Non-monetary gain is any perceived gain, such as political power, military advantage, social enhancement or sexual favor where financial return is not a factor, or is only incidental to achievement of a primary goal. Here, the attackers range from governments seeking political power and military advantage, to amateurs, even children, using social media for bullying.

4.6.2 Existence and Causal Relationships to the Motivation Node

Non-monetary gain goals are variously related to one or more of the six needs cited for motivation. Governments’ goals are often comprised of effecting events outside or within their borders, driven by the safety need, whereas attacks by amateurs are driven by any one or more of the six needs cited above.

Although governments vociferously deny responsibility for cyber-attacks, ample evidence of government engagement in cyber-attacks and cyber-warfare exists. Government resources and protection of personnel open the possibilities for very sophisticated attacks, of which determination of origin is difficult or made misleading.

The following is a sampling of just a few notable attacks attributed after the fact to a government source.

- The government and business websites of Estonia were subjected to distributed denial of service attacks, DDOS, in April-May 2007. The Russian government was suspected of being behind these due to an argument over the placement of memorial [16].
- Georgia, in 2008, was under a well-coordinated DDOS attack just prior to a Russian invasion of that country. The Russian military was suspected to have specifically orchestrated the attack for its invasion [16].
- Google e-mail accounts belonging to well-known Chinese human rights advocates were attacked in January, 2010. The Chinese government was suspected as the source of the attacks [17].

A utopian motive for cybercrime, committed by a hacktivist, is another form of the inclusive non-monetary gain goal. A recent example of this is the case of Aaron Swartz who in September, 2010 used anonymous logins onto the Massachusetts Institute of Technology (MIT) network to download a huge cache of articles from the Jstor database. This database is a very large academic repository whose downloads requires subscription. Swartz' intent was to make academic articles free to the public as stated in his indictment filed in the US District Court in Massachusetts, "Swartz intended to distribute a significant portion of Jstor's archive of digitized journal articles through one of more file sharing sites." [17], [18], [19].

On January 11, 2013 Aaron Swartz committed suicide, before his case was tried in court. To many he was viewed as a hero who liberated information from the Jstor database; but the prosecutors insisted that they were doing their job in enforcing the law. Both Jstor and MIT claimed that the decision to prosecute this case was made by only the State's prosecutors [18, 20].

Much of the non-monetary motivated attack phenomenon is indicative of society's transformation to the digital age, concurrent with computerized information technology. Traditionally, non-monetary gain crimes have been committed frontally or mechanically; today they are committed electronically. An example of the harnessing of technology for non-monetary gain would be bullying. Ostensibly fully compliant with the social media's intended facilitating communication between parties, cyber-bullying causes emotional devastation, sometimes even resulting in suicide.

Cyber-bullying affecting youth emotionally and occasionally physically is a widespread and growing issue. In a well-known study completed at the University of California, Los Angeles, at least 72% of 1,454 students aged 12 to 17 years responded that they experienced a minimum of one online bullying incident [21]. Another study featuring a diverse sample of middle and high school students from a large urban center found that 49.5% of the students had been bullied online [22].

4.6.3 Discussion

Each of two groups of non-monetary gain attackers, government and amateurs, is on the opposite end of ability to carry out sophisticated attacks. Government sponsored attackers have unlimited resources, while abusers and bullies generally have limited knowledge of computer systems. In both cases, defenders have difficulty protecting their targets with technical means alone.

A government cyber-attack requires a highly coordinated response, usually directed by the target's government, to stop the attack and minimize its ramifications. Retaliatory sanctions and the perception of counter-attack capability achieve deterrence most effectively. Of course, the ability to respond or retaliate depends upon, as mentioned earlier, the target government's proficiency at identifying the true attack source. Moreover, the target government needs both technical resources and political capability in order to retaliate successfully [16].

In the case of cyber-bullying, it and related cyber-harassment and cyber-stalking necessitate messaging. The National Crime Prevention Council defines cyber-bullying as "the process of using the Internet, cell phones or other devices to send or post text or images intended to hurt or embarrass another person." Electronic filtering is largely ineffective in combatting text messages, because of the difficulty inherent in differentiating criminal traffic from that of a legitimate, beneficial nature. Stopping message crimes, or at least mitigating their effects, involve a range of interventions, from training potential victims to reject messages from unknown sources and to report unseemly messages, to working closely with parents and schools in reporting abuses.

4.7 Blackmail Node

4.7.1 Definition

Blackmail signifies a threat to damage a system in order to extract financial, political, or social gain. Cyber-extortion is a form of online blackmail wherein one person uses the

Internet to demand money or other goods or behavior (such as sexual compliance) from another by threatening to inflict harm onto the victim's person, reputation, or property [23]. Such cyber criminals commonly threaten to launch a denial of service attack unless the victim pays a fee. More recently, cybercriminals have begun to innovate a process entailing encrypting a victim's data, and then demanding a ransom payment in exchange for the key to release the data.

4.7.2 Existence and Causal Relationships to the Motivation Node

Cyber-extortion can be motivated by a monetary or non-monetary gain goal, where the goal is political or social. Like its traditional counterpart, cyber-extortion goes highly unreported inasmuch as companies are fearful of receiving negative attention should their victimhood be exposed. The skimpy reportage of cyber-extortion could explain why surveys rank it low as compared to other types of attack.

4.7.3 Discussion

As with traditional blackmail, disclosing the damaging information may be legal, but threatening to use the information in order to extort gain is criminal. From the standpoint of information security, placing protective measures, which allow only authenticated and authorized access to information, is imperative for removal of opportunity from cyber blackmail. Additionally, a victim's refusal to capitulate to the demands of a cyber-extortionist would mitigate the effects of an attack. Finally, apprehending and prosecuting a perpetrator would deter future attacks.

4.8 Revenge Node

4.8.1 Definition

Revenge is the infliction of damage or injury as a response to an actual or perceived hurt. It is often the goal of an insider, such as an employee who feels that he or she was wronged by the company. Often a single motive does not drive retaliatory crimes, but rather, a combination of motivations spur criminal revenge. Possibly, an insider becomes angered with the company and in an act of retaliation attacks its computer system, disclosing account information and later selling it. Thus, the motivation goal is twofold: revenge, and monetary gain.

4.8.2 Existence and Causal Relationships to the Motivation Node

Revenge is a common theme of insider attacks, as evidenced by one of the case studies presented in this work, Section 5.7. A study performed by the United States Secret Service and CERT (United States Computer Emergency Readiness Team) [24], based upon 52 cases, found 57% of insider attacks to be motivated by revenge. Interestingly, however, insider attacks as reported by companies apparently comprise less than one-half of all attacks. The CSI 2010 report [12] showed fewer than half of all attacks originating from insiders, and similarly Verizon's 2012 report [11] stated that only 4% of all their reported attacks were committed by insiders.

Revenge can also be the theme of outsider attacks, particularly as the motivation for retaliatory moves against companies who have acted unpopular. "Operation Payback" represents a case in point of outsider retaliation against companies [25]. In late 2010, the

United States government secured the collaboration of major credit card companies to suspend the payment processing of individuals' funding Wikileaks. That website had been providing the general public with a steady stream of classified government information, clandestine intergovernmental communications, and other content that could potentially damage the United States' integrity and security. In retaliation, avid Wikileaks fans, incensed at what they perceived as an infringement of the right to free speech, launched "Operation Payback". Hackers avenged these actions by engineering denial of service attacks upon credit card companies who were cooperating with the United States government. The pro-Wikileaks hackers targeted such major companies as Master Card, VISA, Paypal, and PostFinance; each of these companies' sites was temporarily downed.

4.8.3 Discussion

Revenge is often perpetrated at the spur of the moment, a crime of passion. In many societies passion-influenced crime, up to and including homicide, is treated more leniently than felonies committed under other considerations. Furthermore, great motivation for perpetrating crime dulls the offender's ability to choose rationally in evaluating moral and deterrence implications. A classic example of this concept is Shakespeare's Hamlet [26], wherein Laertes' intense need for revenge overcomes morality and fear of consequence. Inversely, Paternoster, 1996 [27], notes that concomitant with high morality is a lack of impact of all other consequences. The practical implication, therefore, for revenge fueled computer attack is that removing opportunities to commit the crime is the most effective means of protecting against such an attack. Specifically pertaining to insider attacks, effective communication does much to prevent the creation of disgruntled employees. Separation of duties, or the spreading of tasks and associated privileges among a number of people, is an effective means to remove or at least mitigate the effects that one disgruntled employee can have on a company’s sensitive information.

4.9 Hate Node

4.9.1 Definition

The U. S. Congress defines a hate crime as a "criminal offense against a person or property motivated in whole or in part by an offender's bias against a race, religion, disability, ethnic origin or sexual orientation" [28]. Hate crimes project the message of non-acceptance to targeted groups within society. This type of crime is unique in that its aim and consequences have social connotations. Hate crime sends messages to entire groups that they are unwelcome and unsafe in the larger community.

Hate crimes have an increasingly more harmful potential as a result of the emergence of the Internet, which provides a vastly expanded access to extremists who wish to threaten others. Moreover, the Internet affords a cloak of anonymity; hate criminals are able to send threatening e-mail messages anonymously or to utilize a false identity. Additionally, designated victims can receive hate messages without prior knowledge or consent.

4.9.2 Existence and Causal Relationships to the Motivation Node

Hate crime as a motivation for crime has been examined by both the academic establishment and by legislative bodies. Hate mongered cyber–attacks generally consist of denial of service or destruction of data.

4.9.3 Discussion

Hate crimes are usually prosecuted as additives to the primary crime, meaning that inasmuch as an animus motive is present, the crime is prosecuted more severely due to its classification as a hate crime. Debate rages as to whether the prosecution of hate crime serves as a deterrent in preventing future crime, or whether it is, in fact, retribution for the hate crime already committed.

4.10 Challenge Node

4.10.1 Definition

Challenge is the test of one's ability to successfully attack a protected system. Curiosity is an additional goal related to challenge. The attacker desires to know something that is hidden, essentially disclosure of information, and what will happen if he causes change, impacting the integrity and availability of the system. The primary intent of challenge and related curiosity as such is not to cause harm or to derive a tangible benefit. However, they may degenerate into harmful goals.

4.10.2 Existence and Causal Relationships to the Motivation Node

Challenge is a very specific aspect of motivation. It accounts for 23% of attacks reported by large organization, and 2% by all organizations – (Monetary Gain: 71% for large organizations, 98% for all organizations) - according to the 2012 Verizon report [11]. This indicates that corporations are generally doing a good job of blocking low level attacks.

4.10.3 Discussion

Challenge and related curiosity actually have fueled much of the rapid advances in the technology of information systems, as they often entail finding new ways to access and manipulate computer systems. Only when their intent is for non-beneficial purposes does it pose a societal problem.

Challenge motivated attackers, hackers, are known as: script kiddies, black hat hackers, crackers, and hacktivists. The stereotype profile of such a hacker is a male teen, less than age 20, and who may lack social skills. But, in fact hackers are found among both males and females of all ages.

- Black hat hackers have considerable knowledge of computer systems, but do not have malicious intent, but only challenge and curiosity.
- Crackers have limited knowledge of computer systems, but their intentions are malicious; black hat hackers are contemptuous of them.
- Hacktivists have advanced skills in computer technology, and their goals are generally political.

4.11 Opportunity Node

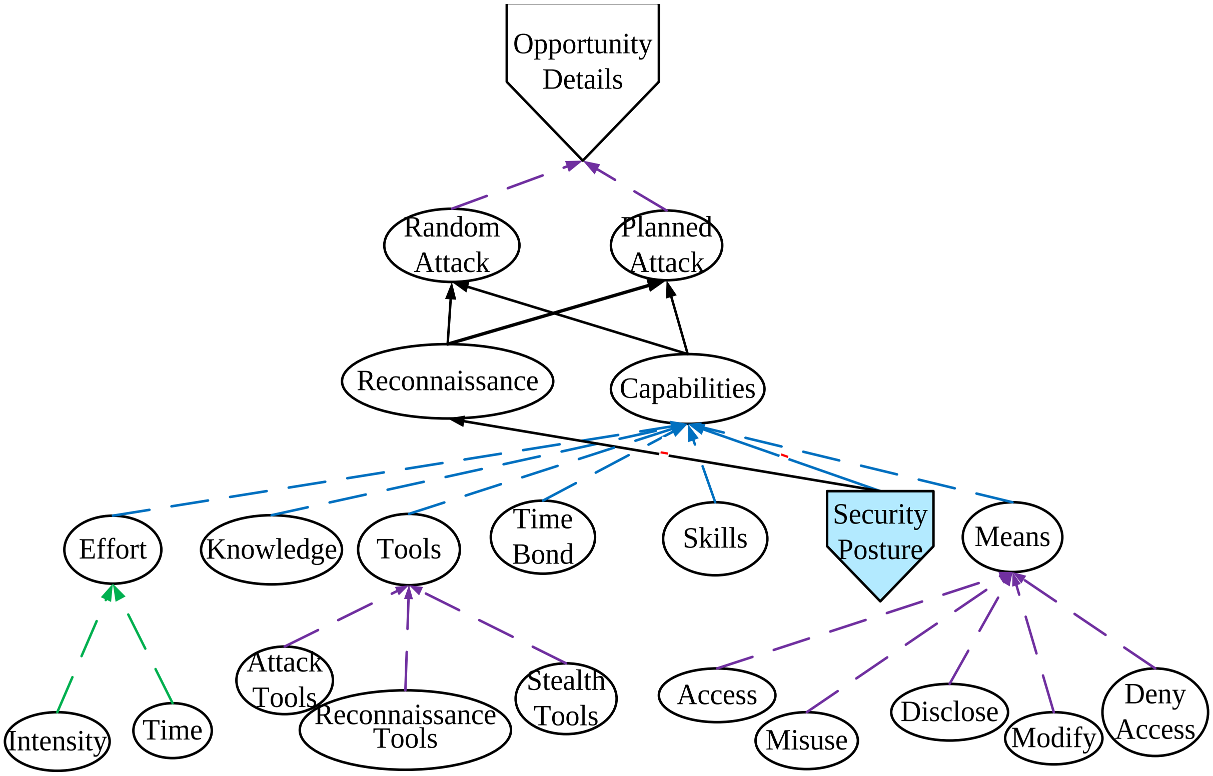


Figure 7: Opportunity Node and its Sub-Nodes

4.11.1 Definition

Opportunity, Figure 7, is defined as "a situation or condition favorable for attainment of a goal" reprisal objective that would be realized from the successful execution of the crime by offender. The favorable situation or condition refers to the vulnerability in the target that can be exploited by the capabilities of the offender.

4.11.2 Existence and Causal Relationships to Information Security Attacks

The reality of the opportunity node as a factor in information security attacks and cybercrime has been well identified and documented. While criminology literature does not deal intensively with cybercrime, criminology theory itself has broad applications to cybercrime. Marcus Felson, Felson, 1994, p. 30 [3], in describing his Routine Activity theory of predatory crimes, notes that the convergence of three elements creates a crime: “a likely offender, a suitable target, and the absence of a capable guardian”. The suitable target of cybercrime refers to the goal of opportunity. Gottfredson and Hirschi, 1990 [29], maintain that crime is created by the convergence of two elements: a motivated offender, and an *attractive opportunity* (author’s emphasis). Similarly, Cornish and Clarke, 1987 [30], explain that Rational Choice theory assumes that offenders respond…to their *opportunities*, cost, and benefits-in deciding whether or not to displace their intentions elsewhere”.

The following characteristics of the opportunity factor, or node, as they relate to information security attacks, have been derived from a listing by Felson and Clarke, in their discussion of “10 Principles of Opportunities and Crime” [2]. These characteristics form a basic resource for the relation of the opportunity node to other influence nodes.

1. Opportunities play a role in causing all crime.
2. Crime opportunities are highly specific.
3. Crime opportunities are concentrated in time and space.
4. Opportunities for crime depend on everyday movements.
5. One crime produces opportunities for another crime.
6. Some “products” (targets) offer more tempting crime opportunities than others.

7. Social and technological changes produce new crime opportunities.
8. Opportunities for crime can be reduced.
9. Reducing opportunities does not usually result in the displacement of crime.
10. Focused opportunity reduction can produce wider declines in crime.

The first principle; namely, that opportunities play a role in causing crime, highlights the causal relationship of opportunity to the commission of information security attacks. The relationship is a positive one, in the sense that greater opportunity correlates with a greater likelihood of crime commission.

4.11.3 Discussion

Regarding opportunity, Felson and Clarke argue about its controllability, substantiating their views on principle 8, “Opportunities for crime can be reduced”, and principle 9, “Reducing opportunities does not usually displace crime.” They also see opportunity as controllable due to the defender’s ability to either protect or discourage it, and due to the fact that other or newer prospects will not necessarily replace the initial opportunities.

In fact, evidence points to reducing opportunity in order to reduce overall crime [31]. One study found that crime against a particular target was not only reduced when the target’s opportunity was reduced, but that the crime was not displaced when other opportunities were made available. The study in question [32] examined suicides in England between 1958 and 1977. From 1958 to about 1965, the number of suicides per year in England remained unchanged, almost half being committed with domestic gas. Then, in the early 1960s, the British government phased out domestic gas. As a result, the percentage of suicides from domestic gas declined, and concurrently, the total number of suicides also declined. These results have been interpreted to mean that as domestic gas with its ease of use decreased as an opportunity, the lack of displacement by less effective opportunities caused the overall rate of suicide to decrease as well. These findings should apply to cybercrime.

Others, Repetto, 1976 [33], and Gabor, 1981 [34], however were less optimistic than Felson and Clarke, and theorized that reduction in opportunity for a particular crime would lead to replacement by another crime. As applied to cybercrime, eliminating opportunity from one target and reducing the likelihood of its being victimized may well result in an increase in attacks on less secured targets. From a societal perspective, the desired overall reduction in related cybercrimes may never occur according to these authors.

In replacing or removing opportunity from individual cybercrimes one must consider the “why” and “how” of the crimes’ original commission; namely, the attacker’s degree of motivation and his capability. These issues will be dealt with subsequently.

4.12 Planned and Random Attack Nodes

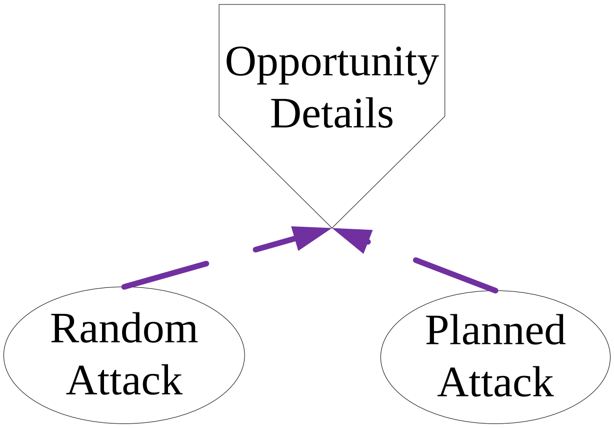


Figure 8: Random and Planned Attack Nodes

4.12.1 Definitions

The opportunity node is composed of random and planned attacks, Figure 8, accordingly related to opportunity by dashed lines as distinguished by Ransbotham and Mitra [35]. Note also a parallel classification in criminology, Felson, pp. 2-7 [3].

1. Random attacks are opportunistic, lacking a specific target. The attacker randomly invades different systems until he achieves a specific goal, such as the obtaining of valid credit card numbers.
2. Planned attacks are deliberate; the attacker targets a specific target. An example is the case of a student targeting his professor’s computer to alter his grade.

4.12.2 Existence

The above definitions of random and planned attacks follow Ransbotham and Mitra's description of these two classes of attack.

- Path of Chance - opportunistic compromise (similar to *Random Attacks)*, and
- Path of Choice - deliberate compromise (similar to *Planned Attacks)*

Like Ransbotham and Mitra, Felson distinguishes ordinary crime from ingenuous or dramatic crime. He contends in discussing "ingenuity fallacy" that most crimes lack sophisticated planning or skill. Insofar as ordinary crime lacks planning, it parallels random attacks as defined above. Similarly he notes a major difference between respective punishments for manslaughter, on one hand, and for homicide, which parallels planned attacks; the difference implies a greater severity where the perpetrator plans to commit the crime. See Stokes v. State [36] where the Florida Supreme Court differentiates clearly between voluntary manslaughter, where even with intent, there was no premeditation; as opposed to homicides, or "designs" that require "an intention formed upon premeditation".

At times, both random and planned attacks converge. Random attacks do not necessarily signify a lack of skill on the part of the attacker; sometimes they signify seeking a particular target. With a skilled attacker, a successful initial random attack that yields a target may inspire subsequent planned attacks upon that target. The initial attacks, although carried out for purposes of gathering information, are done in an invasive fashion, constituting the legal attack definition. For example, a criminal randomly attacks a specific bank's systems in order to unearth their vulnerabilities. After locating the weaknesses, the criminal then specifically exploits the systems. While initial informational probes are components of sophisticated planned attacks, they are in fact considered under the random attacks node in the model.

4.12.3 Causal Relationships

The decomposition of the opportunity node, "a situation or condition favorable for attainment of a goal", into a random attacks node and a planned attacks node is supported by the following.

As noted above, Felson's contention that most crimes are ordinary-defined as non-dramatic, using little skill and involving minimal planning-is on par with the node of random attacks. Indeed, [35], an IT security study, showed that the majority of cyber-attacks are of the random type. A large data set of Intrusion Detection System alert logs, containing 54 million alerts, was analyzed in this study. The logs supplied the dates and times of attack, source and destination addresses, and signatures (identities unique to attacks) of each alert. Experts have been able to distinguish signatures as targeted or untargeted, i.e. planned or random. An essential quote from this study is: "As expected, non-targeted signatures generated a significantly greater number of alerts per signature (235,524 for each non-targeted signature compared to 46,772 for each targeted signature). This study clearly differentiated random and planned attacks, with only one drawback. Since the dataset consisted of only attack data, it did not provide information regarding which type of attack was the more successful. Nevertheless, Felson's 1994 conclusion, pp. 3-5 [3] - quoting data from the FBI's Uniform Crime Reports for 1990 [37] - that most successful crimes lack extensive planning and sophistication, may well be applicable to information security attacks. However, it is unclear from the FBI's data whether the losses from unplanned crime are greater than those resulting from premeditated crime. See Chapter 6 (6) for a discussion on this issue.

Several recent reports on information security note a shift in cybercrime towards a "professional" modus operandi, CSI Computer Crime and Security Survey [12], Symantec Global Internet Security Threat Report and CyberSecurity Watch Survey [38]. This shift is attributed to attackers' motivations reallocating from aspirations of self-aggrandizement to desires for monetary gain. "Professionalism" by definition implies planned attack; absence of professionalism connotes random attack. However, as noted above it is expected that even "professionals" could commence with random attacks that help identify potential targets or vulnerabilities, and then follow through with planned attacks [35].

The differentiation between wholly random attacks and planned attacks which contain an initial random attack component is well illustrated by the following CISCO Report [39].

The report investigates a large class of information security attacks in which e-mail was employed as the attack vector for phishing attacks. The modus operandi of these attacks involved the sending of a large mass unsolicited e-mail, otherwise known as spamming. The spams encouraged their victims to download and thereby install malware, containing viruses and Trojan horses that would further compromise victims' computers. Simultaneously, the spams allowed the attacker to receive personal and financial information about the victims that he could later use or sell.

These attacks were divided into three groups.

The first group, phishing, consisted of traditional mass mailing of spam, in a typical single campaign that sent 1,000,000 messages. As expected, the phishing campaign only generated about 8 victims, since the bulk of the e-mails were stopped by anti – spam. Furthermore, the users had been trained not to open unsolicited email.

The second group, spear phishing attacks, consisted of a much smaller group of e-mails being sent to a targeted group, generally senior management, with a message that had been specifically crafted for each company. The sources of the messages were indicated as being "legitimate", in order to encourage the victim to open and download the malware. While a single spear phishing mailing consisted of only 1,000 emails, as expected it did generate only two victims. Since the victims were highly placed in their respective organizations, the value of this successful attack was *forty times greater* than that of a mass mailing attack. Notwithstanding, a spear phishing campaign costs the attacker four times as much to launch than the more traditional mass mailing campaign.

The third group, Highly Targeted attacks, consisted of very highly customized attacks, directed at specified users or groups of users. These attacks were preceded by a large reconnaissance effort to build a dossier of the intended victims, and they often used zero day exploits, which have no patches available to protect the victim.

Although the CISCO report does not provide any statistics for Highly Targeted attacks, several examples, such as the Stuxnet attack, provide supporting data. The 2010 Stuxnet was the first computer worm to specifically target industrial software and equipment [40]. Previous computer worms had spread indiscriminately and were essentially random; notable cases were the Morris worm of 1988 (Chapter 5) and the Slammer worm of 2003 [41]. In contrast, the Stuxnet worm was able to target the Supervisory Control and Data Acquisition (SCADA) systems of industrial networks, despite the systems' lack of direct internet connection. In character with Highly Targeted attacks, the Stuxnet worm used four zero-day exploits to accomplish its ends. So successful was the Stuxnet, that PC Magazine labeled it "The best Malware ever" [40]. (See cert. org CVE-2010-2568 for one of the vulnerabilities used by Stuxnet).

Possibly even more worrisome is the Flame worm, first reported in May, 2012 [42]. Similar to the Stuxnet worm, the Flame seems to be more advanced. Among a number of zero day exploits, Flame takes advantage of a Microsoft Windows Operating System vulnerability to sanction the worm's creation of unauthorized digital certificates. The worm allows the attacker an unprecedented amount of control over the compromised system while its many stealth techniques make detection very difficult.

Highly Targeted attacks, in order to be perpetrated, require an elevated level of sophistication on the part of the attacker and are exceptionally costly to the attacked. According to the FBI the cost to a victim as a result of a successful Highly Targeted attack varied greatly, but only in a relative sense. A number of the losses were in the hundreds of million dollars range.

Not surprisingly, the recent reports reflect an upswing to more targeted, more lucrative attacks. For instance, the CISCO report cites statistics indicating that from June 2010 to June 2011 the number of mass mailing attacks, or spam messages decreased from 300 billion to 40 billion daily, and cybercriminal benefit correspondingly decreased from $1.1 billion to $500 million. At the same time, the cybercriminal benefit from Spear phishing attacks grew from $50 million to $200 million. Clearly, criminals are shifting from mass mailing attacks to more targeted Spear phishing attacks. Despite the drop in the number of mass mailing attacks and in their value, the authors of the report make note of the fact that the move away from mass mailing attacks occurred more rapidly than the move to more targeted attacks.

These authors assume the presence of crime displacement see Cornish and Clarke [30].

The overall findings of the CISCO report are that while mass mailing phishing attacks, synonymous with random attacks, are greatly more numerous than spear phishing, synonymous with Planned Attacks; the value for the latter attackers and corresponding cost per victim per attack are much greater. It is noteworthy that only the number of random attacks is decreasing, while the number of planned attacks is increasing; this phenomenon reflects a shift in attackers' motivation to monetary gain.

4.12.4 Discussion

Planned and random attacks can be discouraged by effective defensive deterrence measures,

Figure **7**. These include hardening of systems thereby decreasing the attackers' opportunity and deterring future attacks which the attacker perceives as futile. Additionally, random and planned attacks can be further discouraged by effective monitoring and logging which will expose their perpetrators to punishments. These counter measures will be discussed in more detail as they relate to subsequent nodes, 4.21, Security Posture Node.

4.13 Reconnaissance Node

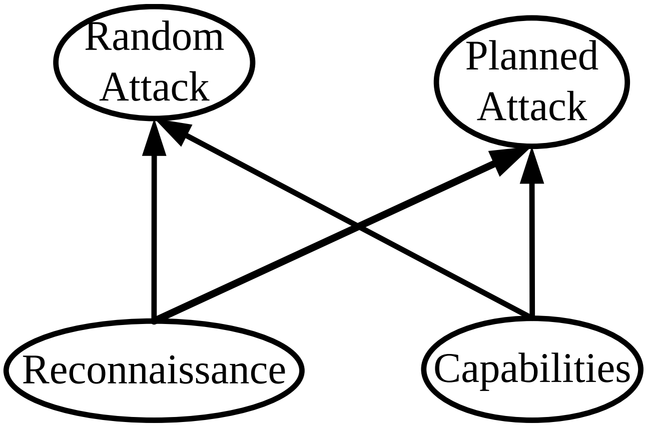


Figure 9: The Reconnaissance and Capabilities Nodes

4.13.1 Definition

Reconnaissance, Figure 9, is the gathering information about a target's value in relation to meeting the attacker's goals and determining the defender's security posture, including vulnerabilities. This information helps the attacker amass knowledge of how, when and what to attack. Valuation of a target and determination of security posture are the objectives of random and planned attacks.

However, informational attacks can result in various legal consequences as will be discussed below:

Any attack by definition implies a cybercrime. Cybercrime is termed by Pavan Duggal [43] as “any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes”.

The OSSTM 3 Manual [44] describes the procedures for security penetration testing of computer systems. Penetration testing utilizes the same procedures employed by a hacker with malicious intent. Herzog classifies these procedures in two broad categories:

- **Data collection** - procedures to collect information about the target, i.e. reconnaissance. The legality of this category is in question.
- **Verification** of testing-procedures that attempt to compromise a computer system in order to test it for vulnerabilities. These procedures are generally considered illegal.

4.13.2 Existence, and Causal Relationship to the Random and Planned Attack Nodes

The relationship of the reconnaissance node with the random and planned attack nodes is shown in Figure 5.

According to widely held belief, coordinated cyber-attacks are preceded by reconnaissance, usually taking the form of probing [44, 45].

Panjwani et al. [46] challenge this, based on a test of attacks on honeypots at a large University. The results failed to show a correlation between probes that are characteristic of reconnaissance and actual attacks.

However, these results can be partly explained by the test bed's location in a University environment where most motivation is for thrills, and where attackers have little fear of being caught or of consequences thereof. In such an environment the attacks would generally be unsophisticated and random, and they would not require prior reconnaissance. Nevertheless, the authors did indicate a probe attack link if attackers used a vulnerability scanner, which is intrusive and presents a comprehensive form of probing, and then proceed to attack.

Furthermore, a study of alert data by Ransbotham and Mitra, 2009, showed a strong linkage of preliminary informal probes to actual attacks. Their data set was obtained from the operations of commercial companies, where attackers are likely to be more sophisticated than mere thrill seekers.

The line influence of the reconnaissance node or factor to planned attack is heavier than the line influence to random attack, due to a generally greater need for precise information about a target and its defenses before the launching of a planned attack. The aforementioned hacking books, in their depiction of different attack methods, buttress the line influence disparity; their authors note that the more sophisticated an attack, the more intricately detailed reconnaissance is required.

The deployment of reconnaissance probes can be overt and hence detectable by the defender or, in the undetectable "stealth" mode, can employ great effort and skill.

4.13.3 Discussion

The field of criminal justice views reconnaissance in its broadest sense as the subject of much debate. Consider the example of an individual's checking doors in a neighborhood to determine if they are locked. Criminal justice here would apply the legal standard of reasonable intent. If a reasonable person would understand the act as demonstrating malicious intent then the act is illegal and therefore punishable under law. Cyber probing presents similar intention issues. Indeed, checking whether a particular service is available on a server may be perfectly legitimate; for an example, when an individual tries to connect to a web or FTP site.

Attempts to prosecute computer probing acts when no information was stolen or compromised, and where intent was not established have yielded mixed results. In the celebrated case of Cohen vs. Mizrahi [47], the defendant who had probed the Mossad Security Agency eluded conviction for cybercrime by the Israeli Supreme Court. On the other hand, the Finnish Supreme Court prosecuted and convicted a seventeen year old of computer crime for mere probing.

4.14 Capabilities Node

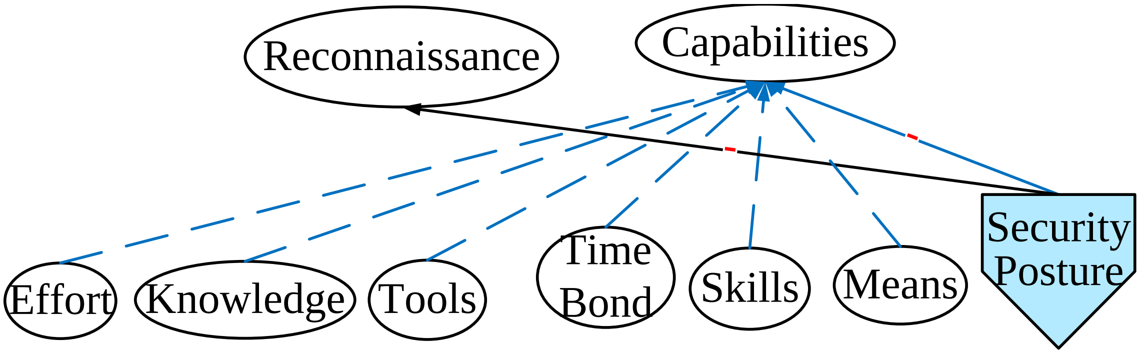


Figure 10: The Capabilities Node and its Sub-Nodes

4.14.1 Definition

Capabilities are the attacker's resources, and the defender's environment, which an attacker exploits in order to accomplish an attack, Figure 10. This node is decomposed into resources and means that an attacker may have, can acquire or can exploit to constitute a threat-source for execution of an attack. The defender's environment (Security Posture, blue) refers to any flaw, omission, vulnerability, or laxity in the defender's safeguards which can be exploited by the attacker's capabilities.

4.14.2 Existence, and Causal Relationship to the Random and Planned Attack Nodes

The NIST Risk Management Guide states [6], "Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." The threat-source refers both to the attacker and to her capabilities. The potential vulnerabilities of the defense also help determine the likelihood of an attack, in addition to the contribution of other factors.

Evidence for the relationship of capabilities to vulnerabilities can be seen in the "Code-Red Internet Worm" disaster. On July 19, 2001, the Code-Red began attacking computers with running Microsoft SQL Servers and with an open UDP port 1433. While computers with closed UDP port 1433s were unaffected, in less than 14 hours the worm had infected more than 359,000 computers at a cost exceeding $2.6 billion [48]. The attacker's resources consisted in this case of a very talented programmer, who was able to access the open ports, essentially vulnerabilities, and exploit them with devastating results.

The capabilities node decomposes into a number of sub nodes that relate to either of two resources: the attacker's knowledge and tools, and to the defender's security posture, vulnerabilities, etc. Capabilities are needed to perform both planned and random attacks; however, because planned attacks are more sophisticated and more focused, they require a higher level of attacker expertise, which links them more strongly to capabilities.

4.15 Knowledge Node

4.15.1 Definition

Knowledge, Figure 10, is the understanding of a target's value, its vulnerabilities and their exploitability. Knowledge is also the understanding of the methods and tools necessary to successfully exploit at the least cost, and of how to avoid detection while achieving the goal of the attack.

Social science studies of knowledge in general aid in understanding the attacker's knowledge and his learning process, which also contributes to his knowledge. Ackoff, 1989 [49] lists five successive components of knowledge, and are applicable to our consideration of attacker knowledge.

- **Data** – Raw data. In the case of the attacker, he discovers a computer operating system and its protective mechanism.
- **Information** – Interpretation of the data to determine the what, who, where, and when questions. In the case of the attacker, he determines which known vulnerabilities are present in the operating system.
- **Knowledge** – Using the data and information to either answer the "how" question or to do something effective. In the case of the attacker, he develops a number of exploits, which are methods to exploit weaknesses, based on his knowledge of vulnerabilities.
- **Understanding** –Using knowledge to gain more knowledge. Here the attacker uses his understanding to determine which exploit will provide the most effective attack.
- **Wisdom** – Extrapolating knowledge and understanding, through the human methods of intuition and experience, to reach a conclusion where no clear-cut rationale exists. The attacker here incorporates, in deciding his method of attack, the short and long term consequences of his exploits.

4.15.2 Existence, and Causal Relationships to Capabilities Node

Using Ackoff's principles the knowledge node can be applied to aid the attacker in the following ways.

- Knowledge includes familiarity with methods that have shown success in launching information security attacks. These methods constantly change with a changing security posture. Methodology knowledge includes understanding tools, exploits, methods for reconnaissance and scanning, inner workings of network communications, access control lists, authorization systems and firewalls. All these knowledge requirements are similar to those required of a successful penetration tester.
- Knowledge is used to help find an appropriate target to fulfill an attacker's goal. If the goal, for example, is the disruption of a large network by causing denial of service (DOS), knowledge to determine if the router being attacked is the primary one of the network. Will the downing of the router adversely affect the entire network? Does that router have backups?[3]
- Knowledge is used to find system weakness or vulnerability that can be exploited via the attacker's acquired methods. This knowledge can be gleaned directly by testing the system to detect vulnerability; hence the reconnaissance link. Alternatively, knowledge of vulnerability can be learned vicariously; for example, certain versions of operating systems are already known to have identifiable vulnerabilities.[4]

[3] In the OSSTM manual, this particular area of knowledge is referred to as:

- Competitive Intelligence - a practice for legally extracting business information from competitors.
- Enumeration – intrusive methods of information gathering about a targeted system.

[4] In the OSSTM manual this is referred to as Vulnerability Research and Verification.

- Knowledge equips the attacker to prevent the detection and recording of the assault. He needs a complete understanding of the target's detection and logging mechanisms in order to devise a detection-proof attack.[5]

Knowledge is a key node of the decomposed capabilities node. Knowledge binds all the nodes (knowledge, tools, skills, time, and effort) comprising the threat-source sector of capabilities. Knowledge itself depends on the reconnaissance node for the value input of a particular target, which then forms the basis for the knowledge to suggest attack methods.

4.15.3 Discussion

As noted above the knowledge node interacts with the other nodes composing the threat-source group of capabilities, and therefore its influence is greater than that of any of these nodes individually. Knowledge, in turn, is controlled by the information it receives from reconnaissance; indeed, without some knowledge of the victim, an attacker cannot strike.

[5] Commonly called "Covering Tracks" in the hacking community, (see Learn Ethical Hacking Tools Free Hacking Tricks How To Hack Hacking Passwords & Email Hacking, 2009)

4.16 Tools Node

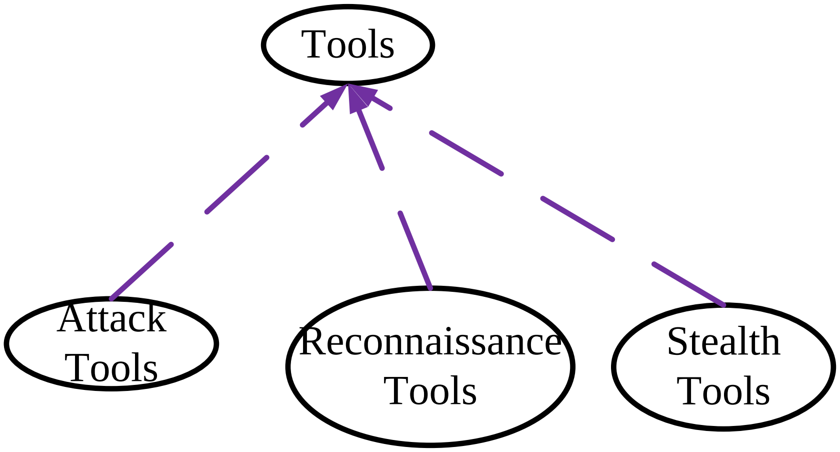


Figure 11: Tools Node and its Sub-Nodes

4.16.1 Definition

Tools, Figure 11, are hardware and software used by an attacker to aid in attacking. These tools can be broadly classified in three groups.

- **Reconnaissance tools** used by an attacker to learn about the assets and defense posture of a defendant. Examples are: port scanners such as Nmap [50], packet sniffers such as Wireshark [51] and Netstumble [52], vulnerability scanners such as Nessus [53], and password crackers such as L0phtCrack [54], Cain & Abel [55], John the Ripper [56] and AirCrack [57]. Much reconnaissance of targets can be done accessing publicly available information with uses of search engines such as Google.

- **Attack tools** consist of hardware and/or software primarily used to exploit vulnerabilities. Examples are vulnerability exploit tools such as Metasplloit and Core Impact, and packet crafting tools such as Netcat [58] and Hping [59].
- **Stealth Tools** are used to hide an attacker's identity, the occurrence of an attack, and its nature. Examples are root kits, encryption tools, and hex and disk editors.

Most tools used by attackers have legitimate uses by IT security professionals to secure and test their own systems.

See sites such as defcon.org, darknet.org and insecure.org which provide hacking tools that can be utilized by both defenders and attackers. (Other means are used to attack security, such as social engineering, personally securing a password to access a victim's computer. Issues about these tools regarding information security are discussed by Ransbotham and Mitra [35], and by Kevin Mitnick [60],

The term "exploit" as a noun in information security refers to an actual code or method that will exploit the vulnerability in a victim's system, see, Terminology, above.

4.16.2 Existence, and Causal Relationship to the Capabilities Node

Every book or reference on information security deals with attack tools. In fact, exploits are sold and traded both legally and illegally.

The United States Computer Emergency Readiness Team (US-Cert) contains the most comprehensive list of exploits and vulnerabilities [61].

In addition to tools being a part of the decomposition of the capabilities node, tools are influenced by the other nodes that make up capabilities. For example to use a tool correctly, knowledge and skill are needed. Also, since a tool may not operate initially as desired, patience and perseverance, effort and time, are needed.

4.16.3 Discussion

Many hacking tools and exploits are freely available on the Internet. This provides much greater ease to commit cybercrime than traditional crime.

An exception is a zero-day exploit which is custom designed to exploit a newly discovered vulnerability by an attacker. Here, there is no patch or counter measure to protect the defender, and therefore such attacks are very effective. However, they require large amounts of research and work on the part of the attacker, and accordingly are very expensive to develop. In fact there is a large underground market for these so called zero-day exploits.

4.17 Skills Node

4.17.1 Definition

Skills, Figure 10, are the ability to apply knowledge as explained above to execute the discovery and attack phases, simultaneously concealing these actions. Skills are generally acquired by training and experience.

Where an attack involves more than one attacker, utilizing different skills, teamwork is essential. This especially calls for leadership quality on the part of the lead attacker.

4.17.2 Causal Relationship to the Capabilities Node

A cybercrime is a human initiated activity which requires knowledge and tools, see above. The attacker requires skills in order to merge his knowledge and tools in order to accomplish his goals.

Note above that skill is a component of capability, and is influenced by knowledge and tools. Skills is also influenced by effort, as the greater the skills the less effort will be required, and the reverse is also true.

4.17.3 Discussion

A defender cannot control directly an attacker's use of skills. Indirectly, however, use of techniques of obscurity, such as changing port numbers to non-standard numbers and the signatures of operating systems, can limit an attacker's ability to acquire the necessary knowledge to effectively accomplish her goal [62].

4.18 Time Bound Node

4.18.1 Definition

Time bound, Figure 10, is the time available to attack undetected and successfully, i.e. the "attack window" in terms of time. For example, a system that is monitored every 30 minutes for intrusions would require an attacker to complete any attack within 30 minutes, or less. Also, successful exploitation of zero-day vulnerability must take place between the time of discovery of the vulnerability, and the implementation of a patch by the defender or software developer [63] [64].

Time bound is affected by password lifetime, i.e. the expiration time when a new password is required. Other barriers to access a sensitive program may be present.

4.18.2 Existence and Causal Relationship to the Capabilities Node

Time bound is influenced by the nature of a vulnerability as some vulnerabilities require less time than others for an attacker to develop an exploit, and thereby have a larger "attack window" until a patch is developed and applied. Also, the magnitude of the "attack window" will be affected by the urgency of the defender to develop a patch, considering the expected knowledge and skill of a potential attacker.

Time bound is also influenced by the policies and culture of a defender. Infrequent application of security updates and infrequent password changes present large "attack windows".

4.19 Effort Node, and the Time and Intensity Sub-Nodes

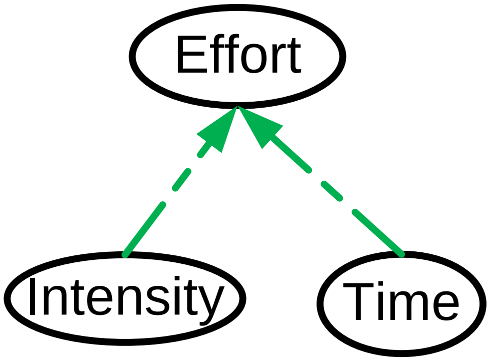


Figure 12: Effort Node and its Sub-Nodes

4.19.1 Definition

Effort, Figure 12, as such is discussed extensively by Littlewood, et al., 1993 [65]. The following two factors, nodes, comprise an attacker's effort, Vroom, 1964) [66].

a. **Time -** "time to perform the task"; and this node also includes frequency of an attacker's actions.
b. **Intensity -** "amplitude of task-related responses".

4.19.2 Existence, and Causal Relationship to the Capabilities Node

Littlewood et al. maintain that an attacker's required effort is an appropriate measure of a system's reliability with regard to malicious attacks, as opposed to experienced time-to-failure. However, that effort is difficult to determine by a defender. Their definition of effort is more expansive than the above as it includes the knowledge and skills nodes, as quoted in their paper.

"This effort could sometimes be time itself, perhaps the time expended by the attacking agent, but it will be only rarely the same time as that seen by, say, the system user or owner. More usually, effort will be an indirect measure of a whole range of attributes, including financial cost, elapsed time, experience and ability of attacker, etc. In particular, such an effort measure can take account of such behavior as learning about a system off-line or by using an entirely different system from the one that is the subject of the attack"

See also Bharat B. Madan et al. [67]. This paper introduces a new security measure based on mean effort-to-failure.

Effort as defined above, as “expended by the attacker”, is a measure of the time and intensity an attacker expends her available knowledge and tools to execute her attack.

4.19.3 Discussion

Effort is difficult to determine by a defender, even according to the simplistic time/intensity definition, especially when considering new attacks. It is essentially a qualitative quantity, as opposed to time-to-failure which is a quantitative measurement, note Littlewood et al.

4.20 Means Node

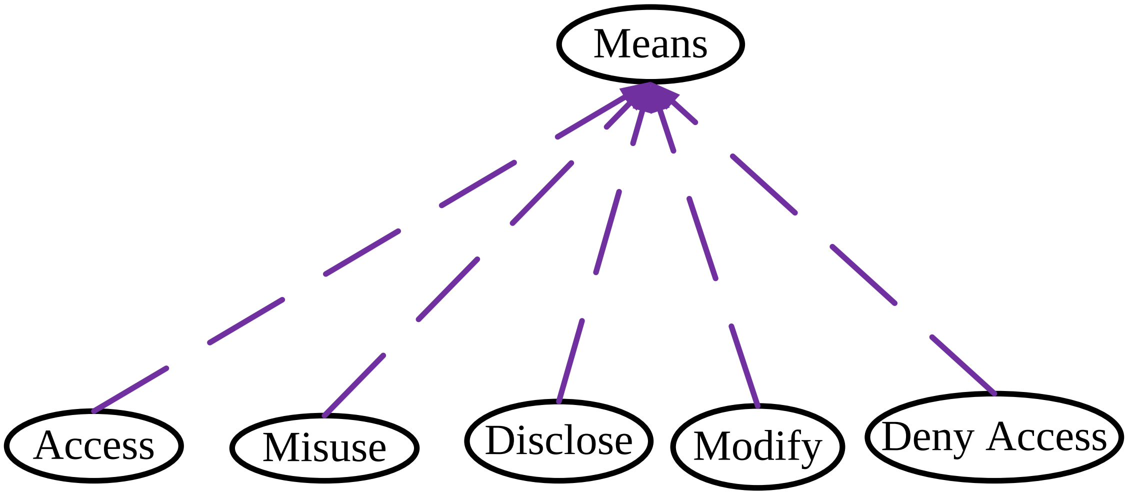


Figure 13: Means Node and its Sub-Nodes

4.20.1 Definition

Means, Figure 13, is the action chosen to attack. It is often defined as a threat-action. Risk Management Guide for Information Technology Systems [6], pp. 13, defines a threat-action as a method by which an attack might be carried out.

4.20.2 Existence, and Causal Relationship to the Capabilities and Motivation Nodes

There are many threat actions listed in the NIST guide because of the very many types of attacks. But here the means node is based on categories where each category represents numerous attacks which have a common feature.

Howard and LeBlanc [68], developed the STRIDE Threat model. STRIDE is an acronym for six threat categories of various attacks that an attacker can choose.

- **Spoofing identity** - an attacker pretends to be somebody else,
- **Tampering with data** - data tampering involves the malicious modification of data,
- **Repudiation** - an attacker denies having performed a malicious action, and cannot be contradicted,
- **Information disclosure** - information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it,
- **Denial of Service (DoS)** - attacks that deny service to valid users, and
- **Elevation of privilege** - a user gains more privileges on a system than is entitled to.

All information security attacks, according to J. Johns [69], can be classified as one or more of the following actions that include those in the STIDE threat model:

- **Access** -unauthorized access which will include using spoofing and repudiation to aid in the attack.
- **Misuse** - unauthorized use of assets (e.g., identity theft, setting up a porn distribution service on a compromised server, etc.),
- **Disclose** - entails maliciously alteration of data,
- **Modify** - unauthorized changing an asset, and
- **Deny access** - entails deprivation of the services of a resource one would normally expect to function, and malicious obliteration or disorienting, information stored in a system.

The means that an attacker will choose to attack depends on the motivation of the attack. For example, when the attacker is motivated for political reasons to damage another country's communication infrastructure, the attacker will likely launch a distributed denial of service attack against the servers that control that country's communications (deny access). When the motivation of the attacker is for financial gain the attacker will attempt to discover credit card information (disclose) and use that information to place fraudulent charges (modify).

Also, the means of an attack is part of the capabilities of the attacker. An attacker who has extensive capabilities, i.e. superior tools, skills and knowledge, could launch a very sophisticated attack that would be hard for the victim to prevent, stop, or recover from. Such an attacker may also have the ability to alter records to prevent raising alarms, and could frustrate forensic analysis of the attack.

4.20.3 Discussion

The means node only involves attacks against computer systems. It does not include attacks that use computer systems to aid criminal or illegal activity. For example, using social media to disseminate false and personal information in order to harass a victim, or using publicly available databases to research information about a target, are not included in any of the means categories.

4.21 Security Posture Node

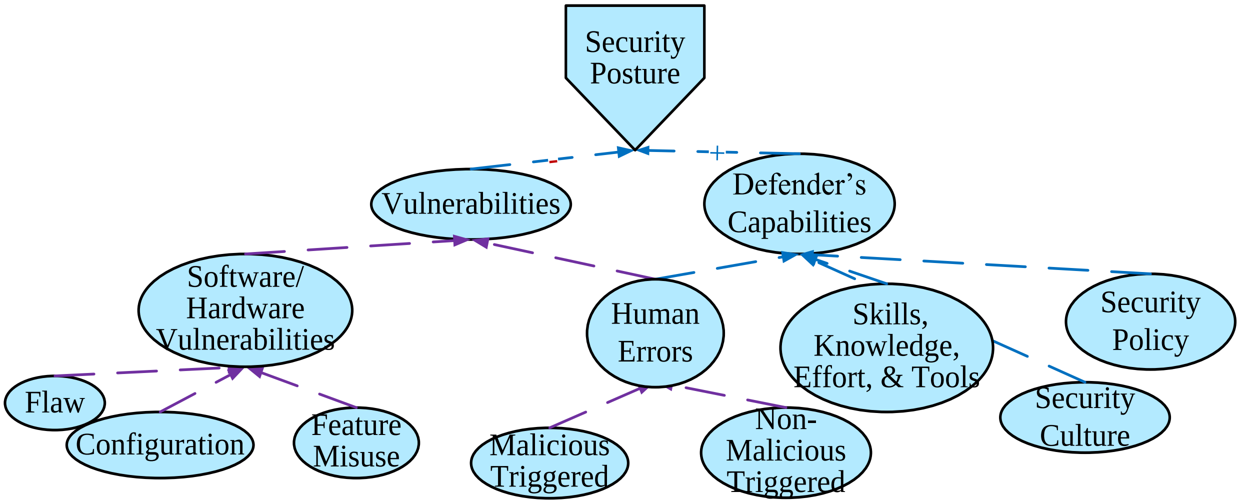


Figure 14: Security Posture Node and all its Sub-nodes

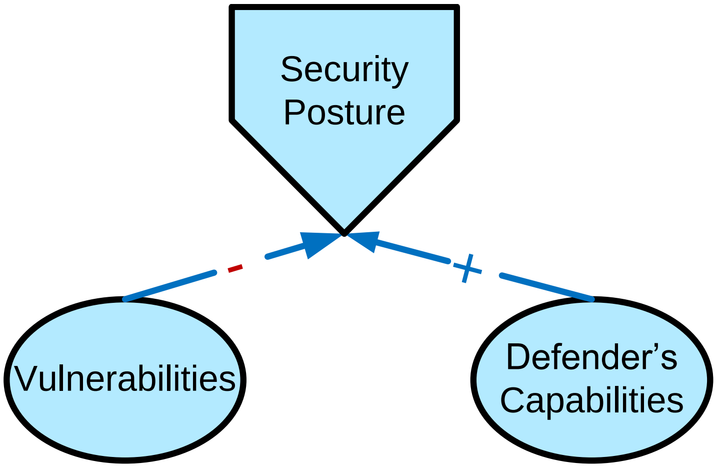


Figure 15: Security Posture and its Top Level Sub-Nodes

4.21.1 Definition

Security posture, **Figure 14** and Figure 15, is a risk level to which a system or organization is exposed from the perspective of a defender, which he has to consider in the context of the model, regarding the likelihood that an attacker will initiate or continue an attack. It consists of those aspects of the of the defender's environment that the attacker can be or become aware of, and accordingly exploit.

1. Vulnerabilities.
2. Defensive Tools –These include firewalls, virus detectors, intrusion protections, and logging and authentication services.
3. Security Policy- This consists of a set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. See POSIX.6.7 [70].
4. Adherence to Security Policy – The individual, human errors and security culture, which impact commitment and compliance to the current security policies.

4.21.2 Existence and Causal Relationship to Capabilities and Reconnaissance Nodes

Information Security can be viewed as a game between attackers and defenders [71]. Attackers attempt to use their resources to compromise the defenses of a defender by exploiting a defender's system's software, hardware and organizational vulnerabilities. The security posture node consists of the complete defensive situation as summarized in the immediately above four items-proactive measures available to a defender, and weaknesses that a defender has to recognize and possibly remove.

As a defender increases his defenses by hardening his systems and removing vulnerabilities an attacker's capabilities to launch a successful attack become increasingly ineffective. Furthermore, as the defender increases the use of technologies that hide identification of his system's software, uses strong encryption for communications and data, and educates the users not to disclose operational information, the ability of an attacker will be weakened in using reconnaissance to gain meaningful information about the target.

4.21.3 Discussion

This node represents traditional information security means that the defender can use and improve her defenses against attacks despite vulnerabilities that he may not be able to address. These security means are mainly in the hands of the defender, depending on available resources, and motivation to defend the system.

Furthermore, a potential attacker's realization of a powerful security posture can deter continued attacks, or even initiation of attacks. This will be dealt with below under the heading of "Deterrence Node"

4.22 Vulnerabilities Node and its Sub-Nodes

The human errors node is dealt with separately, subsequently.

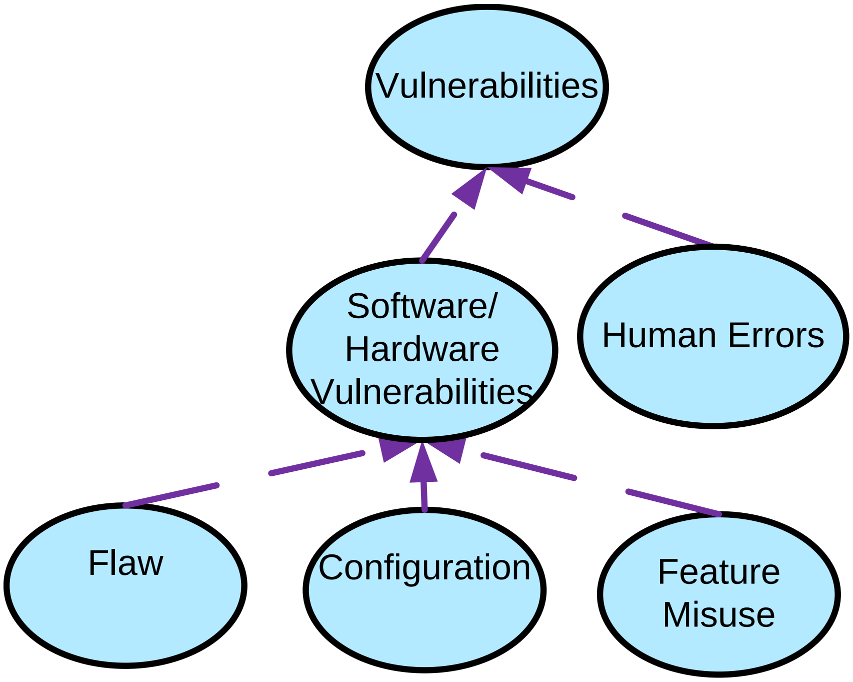


Figure 16: Vulnerabilities Node and its Sub-Nodes

4.22.1 Definition

Vulnerability is as “A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy [6], [72], [73].

4.22.2 Causal Relationships to Security Posture and its Vulnerabilities Sub-Node

If the defenders capabilities are inadequate to remove or patch vulnerabilities, or mitigate consequential effects, the system will be correspondingly more vulnerable to an attack,

Figure 14 and Figure 16, and thus vulnerabilities acquire an additionally negative relationship to the defender's capabilities.

On the positive side, if the defender's capabilities are increased, the security policy could be made more robust. For example, if the defender acquires the capability to encrypt communication, the security policy can specify that certain, sensitive, communications are encrypted. Likewise, defender's capabilities can be used to enforce security policy. For example implementing password complexity and aging effectively enforces security policy.

However, sometimes a defender would elect hide certain capabilities from an attacker for strategic purposes to preferably stop an attack, or mitigate its effects, rather than preventing an attack from occurring altogether.

4.22.3 Existence

The NIST Risk Management Guide deals with vulnerabilities specifically as system and as procedural weaknesses.

- Software/hardware vulnerability, Figure 16, is vulnerability introduced into the software or hardware of a system during its lifecycle, including design, implementation and production. They are well documented in the literature; a comprehensive listing of these can be found in United States Computer Emergency Readiness Team, US-CERT, http://www.kb.cert.org/vuls/.

Usually after vulnerability has been discovered the manufacturer develops a patch for either the defective software or hardware with the goal of distributing that patch before the vulnerability is exploited.

  - However, “zero-day” vulnerabilities and exploits are vulnerabilities that are so new where a patch has not been produced, nor is such a vulnerability widely known, and a defensive mechanism is not immediately available [63]. These exploits can be very effective in the hands of an attacker. But, an attacker usually requires many resources to discover one, and build an exploit around it. However, once this occurs the defender could find suitable patches, or protection. Attackers usually save such an attack for very high value targets.

- Individual factors that leave a system vulnerable to social engineering attacks will be discussed under the human errors node.

Software/hardware vulnerability can be categorized as follows.

- **Software flaw vulnerability** is an unintended error in the design or coding of the software or hardware. Examples are buffer overflow vulnerabilities. These vulnerabilities can usually be corrected by developing a patch that corrects the error in the code [73].
- **Security configuration vulnerability** is the use of a security configuration that negatively affects the security of the software. An example is mistakenly granting all users administrative rights and privileges to a system [74].

- **Feature misuse vulnerability** is where a designer makes trust assumptions that permit the software to provide a beneficial feature, but concurrently introduces the possibility of someone violating these trust assumptions resulting in security compromise. For example, e-mail client software may contain a feature that renders HTML content in e-mail messages. An attacker could craft a fraudulent e-mail message that contains hyperlinks that, when rendered in HTML, appear to the recipient to be benign, but actually take the recipient to a malicious web site when opened [75].

4.22.4 Causal Relationship to Defender Security Posture

Vulnerabilities are the security flaws that weaken the security posture of the defender, and thereby strengthen the attacker's capabilities, Figure 15. Accordingly, security posture - which contributes to risk assessment and likelihood of attack - is affected by the number of vulnerabilities, a quantitative measurement, and the impact of vulnerabilities, which is a qualitative effect [73].

The more vulnerable a system is to attack the greater is its attack surface. To adequately protect her system the defender will need to maximize her capabilities, tools, knowledge, and skills to stop an attack, or mitigate its effects.

4.23 Defender’s Capabilities Node

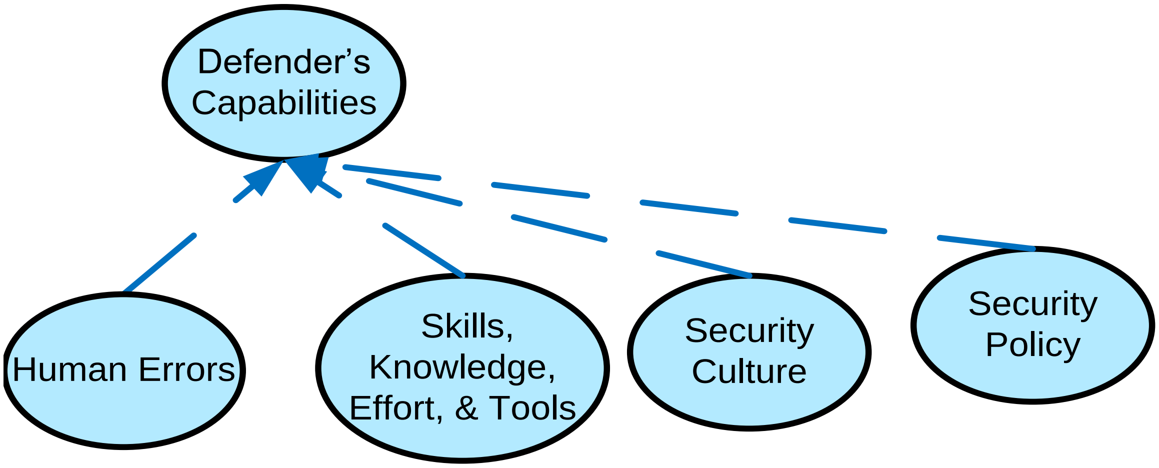


Figure 17: Defender’s Capabilities Node and its Sub-nodes

4.23.1 Definition

The defender’s capabilities node, Figure 17, and constituent sub nodes mirror the attacker’s capabilities node and its sub nodes, Section 4.14, knowledge, skills, tools, time bound, and effort nodes which will apply also to the defender. A noticeable difference between the attacker’s and defender’s capabilities will be in the specific tools or technologies that the defender will use to increase the defenses of the system.

Defensive tools or “Security Technologies” come under three categories based on their primary purposes: to prevent, detect and to recover, according to [76], [77], [78].

- Prevent – Technologies that prevent and protect systems from attack; included in this group are firewalls, antivirus software, SPAM filters, authentication mechanisms, and hardening of operating systems.

- Detect – Technologies that detect attacks as they occur, including network monitoring tools and intrusion detection systems.
- Recovery - Technologies that aid in the recovery after an attack, to mitigate its effects; included are audit and forensic software.

NIST [79] presents three defensive tools categories that are in many ways similar to the above.

- Support - Services/technologies that are generic and underline most information technology security, including identification, cryptographic key management, and security administration services.
- Prevent – Services/technologies that focus on preventing security breaches, including authentication, authorization and access control enforcement services.
- Recovery – Services/technologies that focus on the detection and recovery from a security breach, including audit and intrusion detection services.

4.24 Defenders Skills, Knowledge, Effort, and Tools Nodes

The skills, knowledge, effort and tools of a defender, Figure 17, are very similar to those of the attacker. See 4.14 Capabilities Node. A major difference between an attacker and a defender is that the attacker only has to exploit a single vulnerability to compromise a system, but a defender has to defend against all vulnerabilities. This requires that all users of a system communicate and cooperate in their varying defense measures, thereby mutually providing multiple protective means against various attacks.

In order to build a comprehensive defense, defenders need to be familiar with all the tools that an attacker may use, and have them available to test their own systems. Additionally, defenders must master auditing tools and tools that enforce their security policy.

4.25 Security Policy Node

4.25.1 Definition

Security policy, Figure 17, consists of a set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. See POSIX.6.7 [70].

- Security Policies - The NIST Handbook, Chapter 5 [80] categorizes Security Policies as follows.
    - Program policy – is used to create an organization's computer security program.
    - Issue-specific policies – address specific issues of concern to the organization.
    - System specific policies – are technical directives taken by management to protect a particular system.
- Security Policies are usually written at a high level. The actual details of implementing these policies are guided by three elements.
    - Standards -specify the use of specific technologies. They are usually compulsory and implemented uniformly throughout an organization.

- Guidelines – are similar to standards; they refer to the methodologies of securing systems, but are only recommended actions, and are not compulsory.
- Procedures - embody the detailed steps that are followed to perform specific tasks.

4.25.2 Causal Relationships to Security Posture

Security Policy has to establish conformity in addressing security measures, and deviations would be associated with weak links; noting that security is only as strong as the weakest link [81]. The ability to coordinate the capabilities of the defender and to proactively remove vulnerabilities rests on well formulated and continuously adapted measures to counter ever changing threats. A security policy must be accepted and enforced throughout the community of users of the system. The more robust and enforced the security policy the stronger is the security posture of the defender.

4.26 Human Errors Node

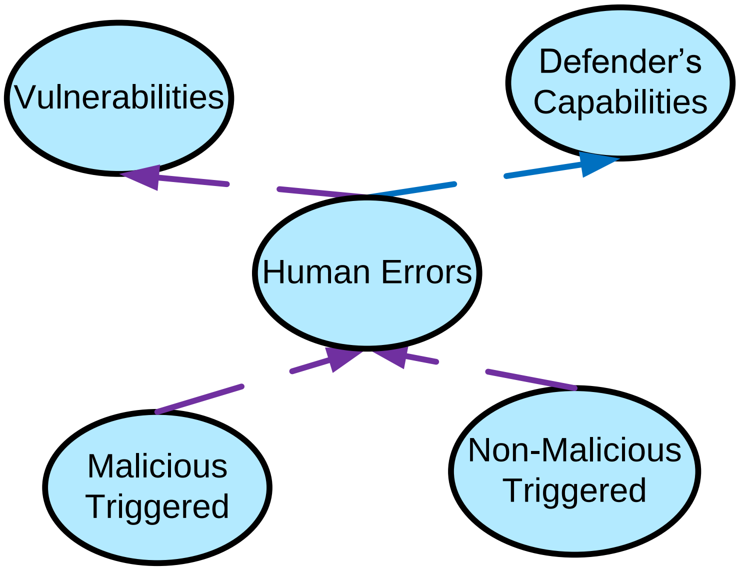


Figure 18: Human Errors Node and its Parent nodes and Sub-nodes

4.26.1 Definition

Human Errors, Figure 18, are due to weaknesses in human nature that can weaken the defensive capabilities of a defender. Furthermore, these human weaknesses can also entail vulnerability in a system where a "social engineer" tricks an operator to compromise a system. Therefore, this node is a sub node of both the defensive capabilities node and the vulnerability node.

4.26.2 Existence

Sara Kramer and Pascale Carayon describe five elements in computer work systems including their information security in which the interplay between them contributes to human errors and violations [82]. They are:

1. **Task** - the task placed on the system manager to monitor, secure, and recover that system;
2. **Environment** - physical access and noise level;
3. Technologies - operating systems, hardware/software Vulnerabilities, and security software;
4. **Organizational** - communications between coworkers and organization security culture; and
5. **Individual** - individual perception of security status and individual experience and training level.

Items 4 and 5 essentially define human related nodes. Items 1, 2 and 3 are for the most part technical, and were dealt with above under Defender's Capabilities, Vulnerabilities and Security Policy.

Defender's human errors causing deviation from security policy can emerge from all five elements, but are prompted by the organizational and individual personal elements. Actual human errors are described James Reason 1990 [83], Figure 19, applying to maliciously and non-maliciously triggered human errors, Figure 18, as:

- **Unintentional errors** which include:
  - Slips - unintended action, and
  - Lapses - unintended inaction; and
- **Intentional errors** which include:
  - Mistakes - inappropriate action, and
  - Violations - deliberate action.

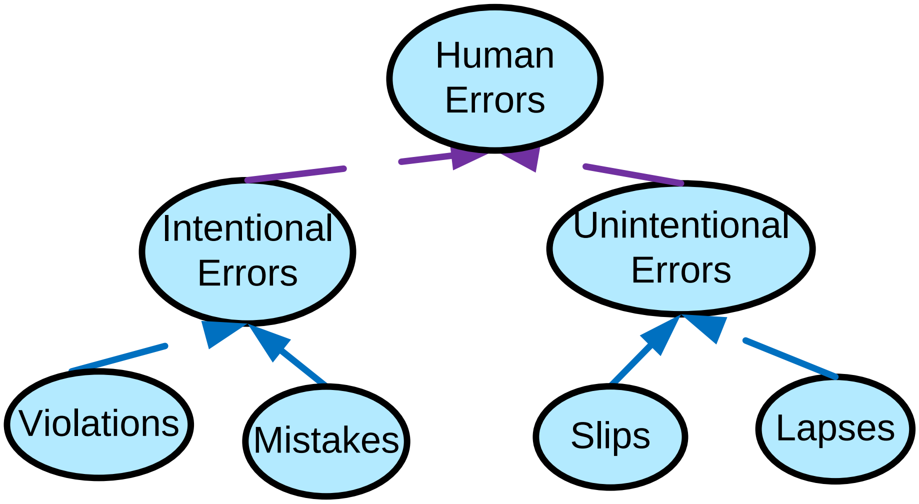


Figure 19: Human Errors and Sub-Nodes

The consequences of these human failures can be active or latent (HSE, 1999).

- Active failures have immediate consequences, and are usually made by front line security personnel when dealing with an active attack. Here, there is little room for error, and the effect will be immediate.
- Latent failures' consequences are not immediate; they remove defensive barriers that could protect a system from attacks. These failures are caused by limitations or shortcomings in system design, and in specific action decisions. They can occur because of inadequate training, supervision, and/or communication.

Human Errors as related to information security are divided into two classes.

- Human errors triggered by non-malicious action due to human failing or unfavorable environment.

- Human errors triggered by malicious action of an attacker, namely a social engineer.

The Human errors node triggered by non-malicious action is a sub-node of the capabilities node. It includes consideration of unintentional and intentional errors, which are without malicious intent but cause deviation from security policy.

These human errors are shaped in the running of a system by the following conditions of the operators [84], [85].

- **Physiological** - fatigue, lack of sleep and hunger,
- **State of health**,
- **Emotional, and mood states** - anxiety, confidence, motivation and personality,
- **Cognitive** - thought processes and biases, and
- **Stress** - such as due to difficult or novel tasks, work load, interruptions and urgent tasks.

These are some examples of the human errors node triggered by non-malicious action, Figure 19.

- **Slips:** A system manager accidently allows unrestricted reading of a secure file.
- **Lapses:** Due to an over-burdened work load a system manager fails to review a security log, and thereby misses early reports of a security attack.
- **Mistakes:** A system manager who fails to understand the purpose of an application choses a weak firewall to protect it.

- **Violation:** A system manager violates a security policy to quickly correct a small and embarrassing problem.

These human errors can cause active failures with immediate consequences or latent failures. In all of these examples the defense capabilities to prevent, stop or mitigate effects of an attack are diminished.

Human errors triggered by malicious action are also a sub-node of the vulnerabilities node.

Since human errors also include weaknesses that a social engineer exploits to his advantage, they can be viewed as a vulnerability much as hardware, software, and configuration vulnerabilities.

This association of vulnerabilities with the human element in information security is essentially because IT systems are truly “man-machine”. As is often with man-machine, the weakest link is a human being. Kevin Mitknet [60], explains: “Savvy technologists have painstakingly developed information-security solutions to minimize the risks connected with the use of computers, yet left unaddressed the most significant vulnerability, the human factor. Despite our intellect, we humans - you, me, and everyone else - remain the most severe threat to each other’s security.”

Thomas R. Peltier [86], lists four human traits that are weaknesses that can be exploited using social engineering. “Social engineering” is a term that describes a non-technical intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures (searchsecurity.com). This can be due to:

- The desire to be helpful,

- A tendency to trust people,
- The fear of getting into trouble, and/or.
- The willingness to cut corners.

These human traits are referred to as performance shaping factors. Similarly, Psychologist Robert Cialdini [87] cites six human weaknesses that leave a system vulnerable to a social engineering attack.

- Reciprocation - manipulating an operator to feel grateful and thus obligated to the social engineer.
- Scarcity - manipulating such a victim into compliance by threatening the availability of something he needs or wants.
- Consistency - human nature traits include the desire to stick to promises, so as not to appear untrustworthy.
- Liking - people are more likely to comply with someone they like.
- Authority - people comply when a request comes from a figure of authority.
- Social validation - people often comply if and when others are doing the same thing.

A social engineer may use these human weaknesses to trick a user into compromising her system.

Human errors triggered by malicious action can likewise be unintentional and intentional errors. Examples of these errors, similar to triggered by non-malicious action, are the following, Figure 19.

- **Slips**: An attacker sends an e-mail that asks the user to click on a hyper link that executes malicious code. The user unintentionally slips and causes the unintended effect.
- **Lapses**: While one attacker distracts a user, a second attacker installs a keyboard reader into the user's PC. The user unintentionally lapses and fails to notice this, and does not stop the attacker from installing the keyboard reader.
- **Mistakes**: An attacker achieves advising a system manager to use an unsecure communication which is inappropriate for the application.
- **Violation:** An attacker poses as person of authority and orders the system manager to violate a stated security policy, thereby granting an unauthorized person to access the system.

In general the immediate goal of the social engineer (malicious trigger) is to gain fraudulent access to a system, or when he already has access to the system, he then desires unwarranted authorization.

A Social Engineer's modus operandi can be described as follows [88].

- **Hunting** – A social engineer aims to cause a human error with minimal interaction with the victim.
- **Farming** – A social engineer aims to cause a human error only after establishing a trust relationship with the victim over a long period of time, and after many interactions.

4.26.3 Causal Relationships to Defense Posture, Security Policy, and Defense Capabilities

The various human elements that comprise human errors accordingly influence defense capability and security policy, and as such contribute to the security posture node.

Included in defense capabilities are tools that a defender uses to protect and recover a system from an information security attack. Specifically, how well the defender, an individual operator, will perform - defender's capabilities node - will very much depend on the human errors mentioned above. This is especially true for a system management team's response to an attempted attack. Human errors may weaken counter measures of the defense, or render them ineffective. For example fatigue may contribute to less aggressive monitoring of systems logs and therefore malicious activity could take place undetected for a long time.

Occurrence of latent failures, contributing negatively to security posture, is in part due to ineffective or weak security policy. As discussed above, latent failures are primarily due to limited training, supervision and communication that are all associated with organizational shortcomings in management and "culture"; these will be discussed subsequently.

It is noted that often a leading cause of failure of any of our systems, power, manufacturing, aviation, defense - of which IT is one - is due to human error weaknesses. This is because they are almost invariably based on many human-machine interfaces.

4.26.4 Discussion

The distinction between the defender's capabilitie**s** node and its sub-nodes, and the vulnerability node and its sub-nodes is that vulnerability addresses inherent weakness in a system as opposed to the capabilities node which deals with both the strengths and weaknesses in a system's protection mechanism. The human errors node is unique that it refers to both the protection of the system and to its vulnerability. It varies with the various human functions being performed on the system, and associations with it. Since human generated actions can be part of the protection of the system - an aspect of man-machine - then human weakness would variously limit its protective capability.

Human errors triggered by non-malicious action can be reduced by:

- Limiting the incidence of human errors that could weaken security, raising alarms and/or limiting security sensitive actions, and
- Creating systems that tolerate human errors and mitigate their effects.

Human errors triggered by malicious action can be reduced by Mitnick:

- Having a strong and enforced security policy that specifically addresses the dangers of social engineering attacks,
- Continuous training of employees on how to comply with the security policy,
- Employee awareness training for potential attacks, and focus on an employee's specific role to protect the system, and
- Testing the effectiveness of training by conducting penetration tests and vulnerability assessments using social engineering methods and tactics to expose any weakness.

James Reason views the human error problem in two ways:

- Personal approach – the burden is on the individual operator or system user.
- System approach – the burden is on the conditions of the workplace and on the organizational process that can enable errors to occur.

This latter approach will be the focus for the following Security Culture Node.

4.27 Security Culture Node

4.27.1 Definition

Security culture, Figure 17, considers both security and safety. Security stresses countering and avoiding deliberate malfeasance. In contrast safety stresses inadvertent errors and mishaps. Therefore the literature pertaining to safety culture is relevant to security culture [89].

M. D. Cooper [90] defines organizational culture as “shared corporate values that affect and influence members’ attitudes and behaviors”. Safety culture is then defined as a sub-facet of organizational culture which relates to an organization’s health and safety performance. Similarly, Cox and Cox, 1991 [91], define safety culture as “the attitudes, beliefs, perceptions and values that employees share in relation to safety”.

The security culture node, is strongly influenced by the visible commitment of management, Jeff Coleman et al., [92], and The British Standard on ‘Information Security Management’ b- BS7799 [93]. This commitment of management, or lack of it, should be perceptible in the formation, implementation and enforcement of a Security

Policy. Strong management support raises the awareness of security and greatly increases the likelihood that the security policy will be adopted and adhered to, is updated on a regular basis, and assurance is provided that financial resources will be committed to have a continuous training and exercise program.

Maynard and Ruigharver [94] developed eight dimensions that define a strong security culture that an organization needs to follow. This was based on TQM (Total Quality Management) guides.

1. Recognition of the importance of security.
2. Security goals need to include a long term plan.
3. Each employee needs to understand her obligations regarding security.
4. Being proactive and flexible to meet security needs.
5. Employees need to feel responsible for security.
6. Cooperation and collaboration is needed in establishing and upholding security standards.
7. Tone of security must be set from the top of the organization.
8. Organization must be aware how external forces and changes will impact security.

4.27.2 Causal Relationships to Posture, Security Policy, and Defense Capabilities Nodes

The relationships of security culture to defense posture are similar to those of the human factors node. There is a particular strong relationship between security policy and security culture both in the formulation of the security policy and in the adoption and adherence to the policy. Companies that have a strong security culture will take input from all its employees in the formulation of a security policy. Upper management will encourage the adoption and adherence to the policy, and employees will be encouraged to bring their security concerns forward. In this way employees will take responsibility for security. A positive security culture environment emphasis on continuous strong leadership, learning, training, and teamwork will affect positively defense knowledge, skills, and tools nodes.

4.28 Deterrence Node

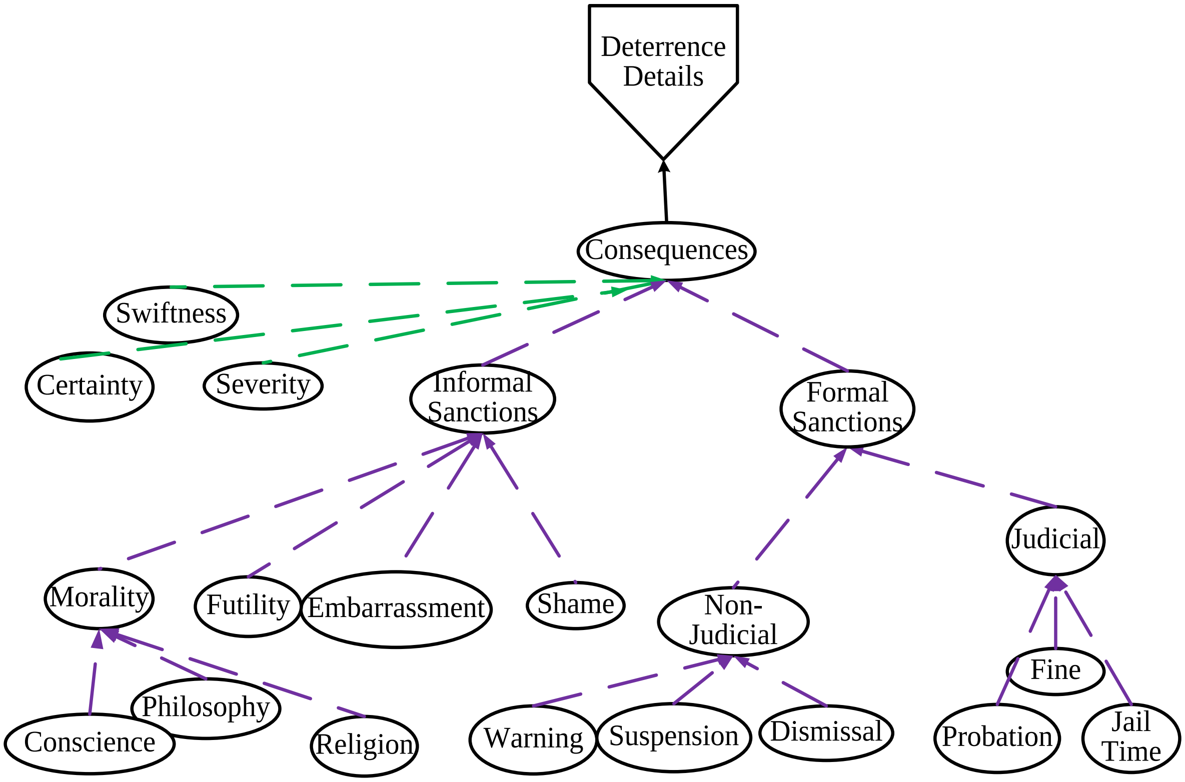


Figure 20: Deterrence Node and all its Sub-nodes

4.28.1 Definition

Deterrence, Figure 20, constitutes factors that inherently discourage an attacker from carrying out an intended attack, essentially decreasing the likelihood of such an attack with respect to the other two major nodes, motivation and opportunity. Consideration of these deterrence factors, especially from the point of view of a potential attacker, requires that they be specifically identified and evaluated for a given situation.

4.28.2 Existence and Causal Relationships to Information Security Attacks

The existence of the deterrence node is shown by each of the theories presented above. In Felson's Routine Activity theory deterrence is "the absence of a capable guardian against the crime". In Clarke's Rational Choice theory deterrence is the "cost" of committing a criminal act that a perpetrator evaluates against the benefit of the crime, under motivation. In the Traditional Criminal theory it is the certainty and severity of legal sanctions that that deter an offender from committing a crime. When considering Situational Crime Prevention, it diminishes opportunity of a would-be offender. These theories essentially impact the sub-nodes that follow.

4.28.3 Discussion

While the Low Self-Control and Desire for Control crime theories do not deal specifically with deterrence, their role is evident. These theories were used by researchers in conjunction with the Rational Choice and Routine Activity theories of crime. See Fattah [95], Nagin and Paternoster, 1993 [96] and Paternoster and Simpson, 1996 [27].

4.29 Consequences Node

4.29.1 Definition

Consequences are actions, essentially punishments, which will prevent or stop an information security attack, or mitigate its effects. (Professor Raymond Paternoster in a private communication)

Consequential actions are not limited to punishments for committing a crime, but include shame, morality and futility.

Even if a consequence only mitigates the effects of a security attack, and an attacker realizes a degree of futility, this can cause deterrence to attempting an attack initially. Consequences are viewed in sociology as mechanisms for “social control”, which are means that society imposes its norms.

4.29.2 Existence and Causal Relationships to Deterrence

Society has always used consequences to discourage crime. The effectiveness of any particular consequence in deterring a crime is the subject of much debate, as will be seen below, especially with Paternoster’s expanded definition.

In its relationship to deterrence, consequences are essentially “how” an attacker is deterred.

4.29.3 Discussion

The effects that a particular consequence will have on deterring an attacker are dependent on three sub nodes: certainty, swiftness, and severity that follow immediately.

4.30 Certainty Node

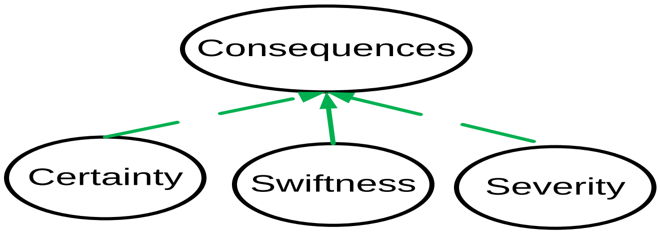


Figure 21: Consequences and its Attribute Sub-Nodes

4.30.1 Definition

Certainty, Figure 21, consists of the probabilities that an attacker will be detected, and subjected to specific consequences.

The certainty of formal sanctions, punishments such as jail, sets in with the occurrence of the entire sequence of: discovery of the crime, apprehension, prosecution and conviction. The certainty of an informal sanction such as shame sets in immediately with the discovery of the crime, Cochran et al., 2008 [97]. The certainty of morality as an issue can occur early when the crime is contemplated. The certainty of futility as an issue is related to an attacker's perception that the attack may not be successful.

Certainty of punishment is often referred to in the literature as risk of punishment.

4.30.2 Existence and Causal Relationships to Consequence

Certainty, like severity and swiftness, is a key sub-node in determining the ability of the threat of a punishment to deter a crime.

This role of certainty is the subject of numerous criminology studies, e.g., Travis and Gottfredson, 1995 [98]; Wilson and Hernstein, 1985 [99]; Nagin and Paternoster, 1994 [96]; Piquero and Pogarsky, 2002 [100]; and Wright et al., 2004 [101].

A significant conclusion of Piquero and Pogarsky, and Nagin and Paternoster is that:

- Certainty, and severity, of punishment is not a deterrent where motivation is high and self-control is low.

In contrast, Wright et al., 2004, concluded otherwise from a data set derived from a longitudinal study, over 26 years, with 1,037 respondents concerning criminal behavior, that:

- Certainty, and severity, of punishment (authors: “high risk, costly”) is a deterrent where motivation is high (authors: “self-perceived criminality”) and self-control is low.

They also concluded from that data that:

- This high risk of punishment is not an issue with people who have low self-perceived criminality, i.e. have high morality.

Wright et al. accounted for the earlier,1994 and 2002, conclusion on certainty - contrary to his - that it was based on responders who were university students who were presumably concerned for the future and consequently had relatively high self-control, and that their responses could be “self-reported intentions to commit crime” and possible boastful trash talk.

According to these contrary conclusions commitment of information security crime by an amateur may not (Piquerro and Pogarsky) or may (Wright et al.) be deterred by high certainty, and severity, of punishment. The ordinary amateur has low self-control, and fits the category of high motivation insofar that remoteness of the victim and perceived vagueness of the law would dull moral inhibition to crime.

The professional information security criminal should be deterred by high certainty, and severity, because his high level of motivation and capability is coupled with high self-control which orients him seriously to future considerations.

4.30.3 Discussion

There is debate in the literature about certainty and severity of punishment, which one is a greater deterrent to crime. This issue is also dealt with specifically in information security studies.

4.31 Severity Node

4.31.1 Definition

Severity, Figure 21, is the level of pain or cost, as perceived by an attacker, caused by a given consequence. It is measureable for formal sanctions, punishments as years in prison or the magnitude of a fine. It is difficult ascribe levels of informal sanctions such as embarrassment or futility because they are subjective.

4.31.2 Existence and Causal Relationships to Consequence

Severity, like certainty and swiftness, is a key sub node in determining the ability the threat of a punishment to deter a crime.

From a public perspective, severity of punishment has been the key factor regarding the effectiveness of punishment. Terms such “Get tough on crime” and “Three strikes and you are out” are aimed at increasing severity, and thereby increasing deterrence to crime.

Severity of punishment by itself has been debatable regarding its deterrent level. Prison time, while it is considered a harsh consequence of crime, does not appear be a strong deterrent because of the prevalence of repeat offenders following incarceration. The Bureau of Justice Statistics, 1987, found that recidivism rates among convicted felons were as high as 67%, and a majority of prison inmates had prior arrest records [102].

4.31.3 Discussion

Many criminology researchers have found that the threat of certainty of punishment is a greater deterrent than its severity. This conclusion was arrived at by Gibbs, 1968 [103], and Tittle 1969 [104], in separate investigations which considered effect of the actual certainty of arrest using data from Uniform Crime Report, and severity using National Prisoner Statistics. Following these studies researchers addressed offenders’ perception of certainty and severity of their punishments, and these were often different than the actual certainty and severity based on reported and statistical data, but are more realistic; but still certainty was found to be the greater deterrent. Paternoster, 1987 [105], found a general consensus for this conclusion in an evaluation 25 studies that were based on offenders’ perception of certainty and severity of punishment for a range of offenses.

However, he did not find these studies to offer convincing conclusions about relationships between certainty and severity, and their effect on deterrence.

Klepper and Nagin, 1989 [106], found from a study of tax noncompliance – they used responses to test scenarios given to 163 students in a Public Business Management school - that detection of the offender, resulting in shame and embarrassment, and severity of the punishment deter that crime.

Pogarsky, 2002 [107], from a survey study of 412 undergraduate students regarding driving home after drinking alcohol, found that in that case severity causes more deterrence than certainty of punishment. This is contrary to conclusions from the aggregated sample approach of Gibbs and Tittle. He further concluded that "that the deterrent effect of the certainty of punishment far exceeds that of the severity of punishment--may be overstated".

There is a number of information security- specific studies have been conducted to determine if fear of severity or certainty of punishment causes deterrence.

Higgins et al., 2005 [108], had 386 students respond to test scenarios to determine whether certainty or severity offers more deterrence to the crime of Software Piracy – downloading and installing unpaid software. The results showed that certainty had a significantly negative link with software piracy. These results are consistent with most criminology studies dealing with deterrence theory.

D'Arcy and Herath, 2011 [109], reviewed a number of studies of deterrence in the information security literature that present contradictory conclusions about the relevance of severity and of certainty of sanctions.

They cite Straub [110], who conducted a survey of over 1200 companies who reported 256 security incidents. Based on the results of this survey he concluded that:

- "IS security is effective. An active security staff and a commitment to data security are effective controls as are activities in which the security staff informs users about unacceptable system use and penalties for noncompliance. Organizations that articulate their policy on abuse and actively enforce this policy should benefit from these activities. Security measures such as security awareness training sessions also reduce loses from abuse."

From these conclusions it was apparent to D'Arcy and Herath that both severity and certainty of punishment are effective in deterring computer crime. But Straub's note of effectiveness of IS security may well be due to the reduction of opportunity.

D'Arcy, Hovav and Galletta, 2009 [111] conducted a study of the likelihood to commit information security crime in the presence of security policies, education, training, and program awareness. It entailed responses from 238 MBA students from two universities, and 269 employees from eight organizations who were given test scenarios of proposed information security attacks. Their conclusions were that security program awareness had little effect on deterring users who are computer savvy, or employees who work offsite. By extension, the finding that making potential insider computer criminals aware of the severity and certainty of punishment fails to deter attacks, it followed that perceived severity and certainty of punishment will not deter a computer criminal.

Another citation by Herath and Rao [112] used a survey of employees from 77 organizations in a study that included the issue if computer crime is deterred by severity and certainty of punishment. These authors concluded here that certainty of punishment deters computer crime, and, surprisingly, severity of punishment encourages computer crime, perhaps because of the thrill.

So far information security specific studies seem to have offered inconsistent conclusions to the question whether certainty or severity of punishment is the greater deterrent. Most studies in general criminology support that certainty is a greater deterrent than severity of punishment when fear of punishment is present.

4.32 Swiftness Node

4.32.1 Definition

Swiftness, Figure 21, or celerity as often referred to in the literature, is the relative time between the crime’s commission and the offender receiving punishment. Swiftness is the last of the three nodes that describe punishments

4.32.2 Existence and Causal Relationships to Consequences

Swiftness is the least studied of the three nodes that describe punishment: certainty, severity and swiftness. Nagin and Pogarsky, 2001 [113], explain that the general disinterest among researchers of the swiftness factor is due to swiftness being grounded in experimentation of animal behaviors. Experiments have shown animal behaviors can be suppressed with negative reinforcements as long as they occur within six seconds following the targeted behavior. Criminology also assumed that a delay in carrying out the punishment will diminish the effectiveness of the punishment. This is known as “Pavlovian conditioning”. There are a number of problems with the compassion to animal behavior.

- Humans have far more cognitive capacity of the ability to relate punishment to the crime even after a long time.
- Criminal Justice Systems are designed to remind the offender of the crimes that he/she has committed.
- When dealing with general deterrence, a would-be offender contemplates the punishment received by others so the time delay will not have role in decision process of the would-be offender. See Gibbs 1975 [114], pp. 130-131.

Nagin and Pogarsky suggest considering the swiftness effect as the "time value of money". Just as someone will be willing pay extra in order to extend ones payment, similarly the severity of a punishment can be viewed as lesser by extending the time until the punishment occurs. Therefore, even in general deterrence a crime whose punishment takes longer to be implemented will be viewed less severe than a punishment which is applied immediately. See also Paternoster, 2010 [115], for a review of this theory.

This logic is most compelling.

It could then be added that a punishment that takes a long time to be implemented can also be viewed by the decision maker (offender) as not having as much certainty as an immediately applied punishment.

There are few studies that deal with the direct effect of swiftness on deterrence. One such study was conducted by Legge and Park, 1994, [116]. It consisted of a cross-sectional regression model pooled across three years (1980, 1984 and 1987) of single-vehicle nighttime traffic fatalities, which is a proxy measure for alcohol-related fatalities. The data set was derived from 48 states. The study was directed at certainty, severity, and swiftness of punishments for driving under the influence of alcohol. The findings gave the conclusion that “less punitive but more certain and swift punishments have the largest effective impact on alcohol-related crashes”. In this study swiftness showed a deterrent value.

On the other hand another study by Howe and Loftus, 1996 [117], only found minimal effects of celerity, swiftness.

Nagin and Pogarsky specifically tested swiftness using a survey of 252 undergraduate students who responded to a test scenario involving drunk driving. The results showed no deterrence value by having the punishment occur sooner rather than later.

4.32.3 Discussion

While typical crime researchers debate the issue of celerity playing any role in deterrence, the literature does not seem to offer any studies of the relationship of swiftness to deterrence in information security crime, D’Arcy and Herath. This is perhaps because the laws dealing with formal punishment for information security crime are relatively new, have not been fully tested, and the court procedures tend to take a long time.

Paternoster, 2010, offers the following summary of the present status of these three sub-nodes regarding deterrence.

“Finally, while there may be disagreement about the magnitude, there does seem to be a modest inverse relationship between the perceived certainty of punishment and crime, but no real evidence of a deterrent effect for severity, and no real knowledge base about the celerity (swiftness) of punishment.”

4.33 Formal Sanctions Node

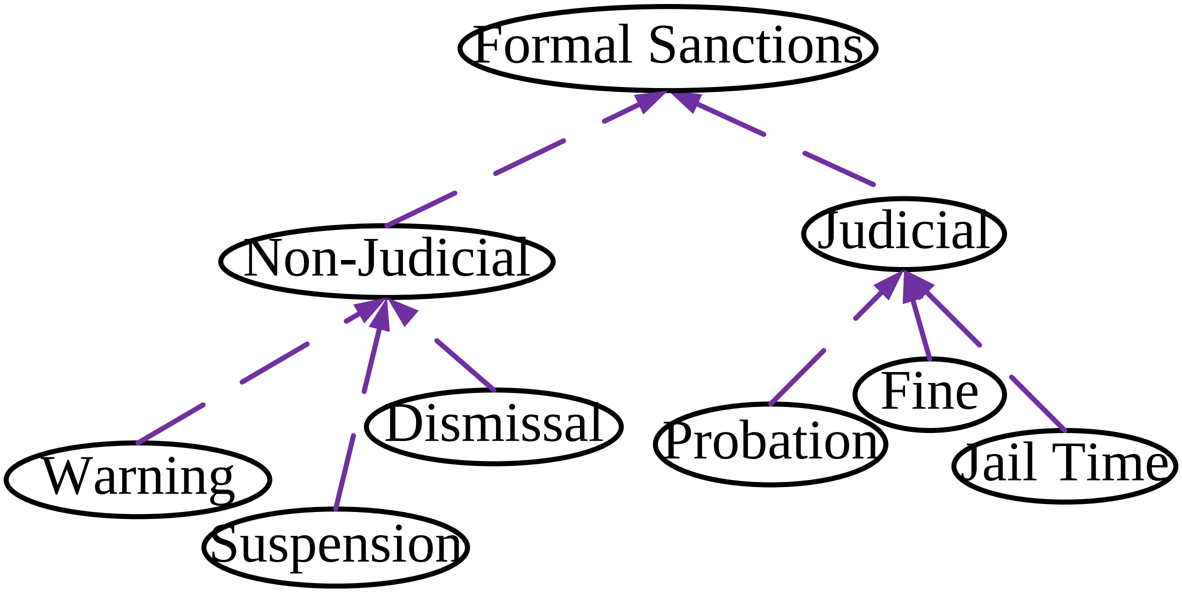


Figure 22: Formal Sanctions and its Sub-Nodes

4.33.1 Definition

Formal sanctions, Figure 22, are specific consequences imposed by an authority, and are based on a law or a rule. The intent of laws and rules, and their consequential sanctions for infraction are to impose norms on society that will be followed; they are a form of social control.

4.33.2 Existence and Causal Relationship to Consequences

There is debate on how effective are formal sanctions as a deterrents. Paternoster, 2010 [115], explains that formal sanctions frequently and effectively influence our actions. One example is that drivers slow down when they spot a patrol car due to the threat of a fine. Burglars generally do not break into occupied homes due to fear of getting caught.

What are not known well are the relative or marginal effects of formal sanctions. Do increasing prison terms and increasing fines decrease crime? There are several reasons for the difficulty in understanding the relationship between formal sanctions and reduction of crime.

- There is difficulty in measuring the deterrence value of a punishment. Often, there are “many things happening before the deterrence can occur”.
- It is possible that the legal system is unable to exploit human rationality effectively to derive the gain from formal punishments.

Studies in early 1960’s showed that states that imposed capital punishment for murder had higher murder rates than those which did not have capital punishment. These results were interpreted to mean that formal sanctions in general did not serve as deterrence. Subsequent studies of more specific crimes cast doubt on these conclusions.

Although researchers do cast some doubt about the effectiveness of formal sanctions, the general public has always viewed formal sanctions as effective deterrence. Examples are “three times and you are out” laws and minimum sentence guidelines.

Regarding imprisonment, a formal sanction, Paternoster, 2010, states that there is a general consensus that observed crime decrease after increasing the length of prison sentences, is due to the prison sentences and their increased length. The debate among the scholars is how much. Spelman, 2000 [118], empirical analysis showed a crime drop between 4% and 21% due to increases in incarceration.

4.33.3 Discussion

The effects formal sanctions can be classified according to their [119]:

- Direct role in the calculus of a would-be attacker's decision to launch an attack, or their
- Indirect role in stimulating and reinforcing social norms that intended criminal behavior is unacceptable.

This indirect role of formal sanctions will influence the nodes that relate to social controls, namely shame, embarrassment and morality, Section 4.37.

In their study, Salem and Bowers found more support for the indirect role of formal sanctions than the direct role.

4.34 Judicial Sanctions Node

4.34.1 Definition

The judicial and non-judicial sanctions sub-nodes of formal sanctions, Figure 22, are distinct factors of formal sanctions.

Judicial sanctions are punishments resulting from formal judicial proceedings. These proceedings are deliberate, based on evidence, and follow pre-determined sets of laws or rules. The burden of proof for criminal cases in the United States is that it must meet the "beyond reasonable doubt" criterion. For civil cases it must have a preponderance of evidence. Successful criminal prosecution is limited because of the beyond a reasonable doubt criterion. Additionally, criminal proceedings tend to be lengthy and therefore judicial sanctions are not swift.

4.34.2 Existence and Causal Relationships to Formal Sanctions

Judicial sanctions are the most visible punishments for criminal behavior. Under the current laws that target specifically computer crime such as the Computer Fraud and Abuse Act of 1984 [120] three punishments are stipulated.

1. Fine – Money paid usually to a superior authority, usually a governmental authority, as punishment for a crime or other offence.
2. Imprisonment - The lawful restraint of a person contrary to her will.
3. Probation - A sentence allowing limited freedom within society, with court imposed supervision (thefreedictionary.com).

4.34.3 Discussion

Its sub-nodes, Figure 22, refer to the above punishments when imposed for only an actual computer crime act, and not for other act associated criminal behavior or effects. It is possible to consider capital punishment associated with a computer crime such as in the case of Bradley E. Manning in connection with alleged Wikileaks disclosures, Section 5.9, where one of the charges was treason which can carry the death penalty.

4.35 Non-Judicial Sanctions Node

4.35.1 Definition

Non-judicial sanctions, Figure 22, are punishments resulting from non-judicial proceedings, such as those presided by school administrators and corporate managers in response rule infractions and misbehavior. For even suspected computer infractions schools and corporations often arbitrarily block user access. They do not have such strict guides as judicial proceedings. See “University of Maryland Policy on the Acceptable

Use of Information Technology Resources" for example [121]. Police act no-judicially when they revoke a driver's license for failing a sobriety test, Legge and Park, 1994 [116]. These processes are more expedient than a legal judicial process as there the burden of proof is more relaxed, and often the prosecutor is also the judge.

4.35.2 Existence and Causal Relationships to Formal Sanctions

The three characteristic nodes of consequences - certainty, severity, and swiftness - distinguish non–judicial sanctions from judicial sanctions.

- Certainty – Due to relaxing of evidence requirements for a non–judicial process there is a greater certainty of punishment than from a similar process under judicial auspices.
- Severity – These sanctions are generally not as severe as for a judicial process. Jail time is not an option.
- Swiftness – These sanctions imposed by a non–judicial process are swifter than those resulting from a judicial process as they do not necessitate "due process".

4.35.3 Discussion

The sub-nodes of the non-judicial node - warning, suspension and dismissal – essentially discuss it and elaborate on it.

- Warning – An official warning is given that the current behavior will not be tolerated. Often a warning becomes part of the student's or employee's record, and can cause problems with future eligibility for promotions or awards.

- Suspension – This is a more severe punishment. Even temporary suspension from a job can be without pay. In an academic environment it could include losing computer privileges and/or course credit, or demotion of a grade.
- Dismissal – This is the most severe sanction a non–judicial process can impose.

4.36 Informal Sanctions Node

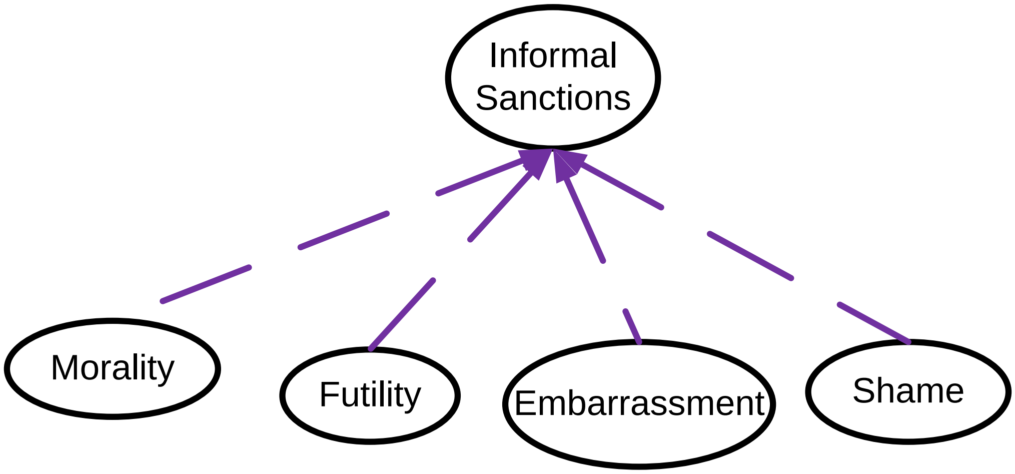


Figure 23: Informal Sanctions and its Sub-Nodes

4.36.1 Definition

Informal sanctions, Figure 23, are punishments for deviant behavior that are imposed by society or custom. They include ridicule and ostracism. They can be a result of formal punishments, for example, someone who served prison time will find it difficult to be accepted socially after being released. Or, informal sanctions can be the only punishment for a crime as in the case of self-inflicted embarrassment resulting from moral failings [106] page 4.

It was mentioned above that consequences can be viewed as social control mechanisms. This is not only true for Formal Sanctions whose formal intent is to force norms on society, but also for informal sanctions which also act as controls in both society and in small social units [122]

4.36.2 Existence and Causal Relationships to Consequences and Formal Sanctions

Anderson et al. [123] found that perceived informal sanctions provide greater deterrence than perceived formal sanctions. This was based on a survey on marijuana use responses of 321 randomly selected students.

Paternoster and Simpson, 1996 [27], found from an analysis of a set of survey data that reliance on corporate crime deterrence was realized where informal sanctions were added to formal sanctions.

French sociology pioneer Émile Durkheim (1858-1917) [124] went so far as to say that the primary function of formal sanctions is to strengthen the "normative climate of the community-to reinforce and mobilize informal social disapproval"; a secondary effect is to directly deter criminal behavior through "Calculus of Utility" [119].

4.36.3 Discussion

Williams and Hawkins, 1986 [125], state that Informal Sanctions can be measured for their ability to deter criminal behavior as "costs".

- Stigma costs are social degradation and loss of respect and reputation due to being caught.

- Commitment costs - Cost of arrest limits attainment of future goals. Examples of these costs are where an arrest will hurt future employment chances, educational opportunities, or marriage prospects.
- Attachment costs - loss of friends and significant others due to being caught. Depending on the relationship, bonds can affect the attachment costs. For example, in many cases family and friends rally around the accused as they view him/her as a victim.

4.37 Shame and Embarrassment Node

4.37.1 Definition

Shame and embarrassment, Figure 23, are described by Gasmick and Bursik, 1990 [126].

- Shame is an individual's perception of violating a norm, as judged by him or by others, Braithwaite and Geis, 1982 [127], and thus shame can be a self-imposed punishment. See Piquero and Tibbetts, 1996 [128], for a discussion whether shame only occurs when there is a social audience. Their conclusions include that most shaming is not preceded by being imposed by others.
- Embarrassment is when friends and relatives might lose respect for an offender if he/she engages in a particular behavior. Thus embarrassment is a socially imposed punishment.

Psychologists differentiate between guilt and shame. Guilt is where an individual has remorse for the committed act. Shame is where the individual blames oneself for the act. With guilt there is a desire to correct the mistake. With shame there is feeling of loneliness and depression. See Gershen Kaufman, 1989 [129]. Shame and guilt may be used interchangeably for the influence model. See Grasmick and Bursik, 1990 [126], footnote 3.

4.37.2 Existence and Causal Relationships to Informal Sanctions

According to Gasmick and Bursik, 1990, the most immediate consequence for both shame and embarrassment is probably a physiological discomfort. Long term consequences for shame include “damaged self-concept, depression, anxiety, etc., which could impede normal functioning in one's social environment”. The long-term consequences of embarrassment “which might include a loss of valued relationships and perhaps a restriction in opportunities to achieve other valued goals over which significant others have some control.” These consequences will include the above noted stigma, commitment, and attachment.

Piquero and Tibbetts, 1996 [128], studied shoplifting and drunk driving in connection with shame. They found that shame negatively affects intentions to commit these crimes. This negative relationship is stronger for shoplifting than for drunk driving. It can be due to less of social stigma being associated with drunk driving than shoplifting.

They also found a relationship between shame and “Perceived Sanctions”, the greater the shame the more aware the offender is of the severity of both formal and informal sanctions. This is due to the increased commitment and attachment costs that a would-be offender would contemplate regarding the severity of these sanctions.

These authors also found a negative relationship between low self-control and shame. Shame is not an important deterrent for offenders who possess the low self-control trait. It was noted above that the amateur computer criminal has low self-control, low self-esteem, and is therefore undeterred by shame.

Higgins, Wilson and Fell [108] found from a self- reporting survey found shame to be "an important self-conscious emotion which may provide a sense of self-disapproval and self-stigma"- stigma costs. Furthermore, family disapproval - commitment costs - is also a strong deterrence to software piracy.

D'Arcy and Hovav, 2009 [130], studied the effects from an IT security perspective of people working remotely, not having physical contact with their superiors and colleagues. They theorized that since these workers are remote they will more likely lack shame and embarrassment in contemplating IS infractions. There is much support for this in typical crime according to deindividuation theory, which deals with the loss of a person's sense of individuality and personal responsibility, such as in the case of mob behavior. This may well happen to one who is not observed or paid attention to, and consequently does not feel scrutinized. This then can result in diminished deterrence to engaging in criminal behavior.

However, D'Arcy and Hovav only found partial support that workers are more likely to be engaged in IS infractions when they work remotely.

4.37.3 Discussion

Shame and embarrassment are powerful deterrence to crime. This applies both when they are in conjunction with a formal sanction as well as with the simple realization of the wrongness of the criminal act. A challenge for information security is to implement social control mechanisms that call forth shame and embarrassment for IS infractions. Presently these factors lack potency because the criminal, attacker, can often remain anonymous and will not be subjected to embarrassment, and there is a lack of clear guidelines on what is acceptable, and what is wrong. It is therefore imperative to raise the awareness of computer crime to the general public and especially to all computer operators, and its ramifications of shame and embarrassment to one's self, family and friends. However, this may not affect computer crime gangs whose "norms" are different from those of the greater society and shame and embarrassment would not be an issue. [131].

4.38 Morality Node

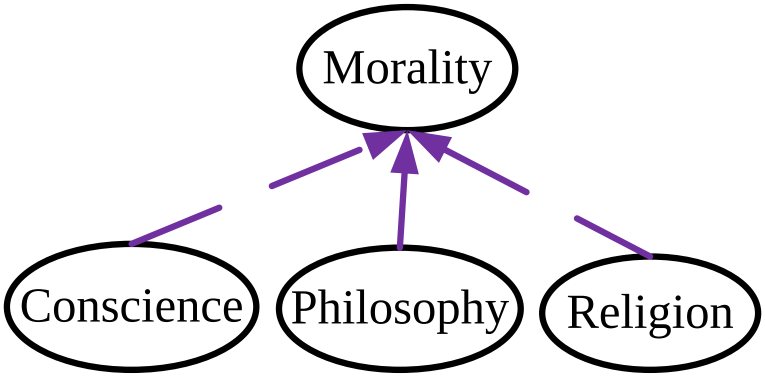


Figure 24: Morality Node and its Sub-nodes

4.38.1 Definition

Morality, Figure 23, and Figure 24, pertains to the differentiation between right and wrong intentions, decisions and actions as related to a preset "norms". Morality is part of social control. It is based both on individual norms and on society-at-large norms. One's morality can come from three sources.

- Conscience – a desire not to cause harm to others has a biological basis, and may even entail pain to the altruistic individual, Broom, 2003 [132]. This altruistic behavior occurs even when it entails pain to not to cause harm to a single individual or a group of individual even when the person must endure some pain. Broom quotes a number of authors that subscribe to such a theory as Moore (1903), Kropotkin (1902), Krummer (1978), de Waal (1996) and Ridley (1996).
- Philosophy – a root of morality variously formulated by classical philosophers.
    - Immanuel Kant 1772-1804 used the concept of "Categorical Imperative" to formulate rational tests for morality "norms". For example such a norm can be evaluated by its universal utility, such as truth telling; if no one will follow it there will be a break down in society.
    - Jeremy Bentham (1748-1832) and John Stuart Mill (1806-1873) developed a moral theory called Utilitarianism which is based on the ability of "norms" to bring pleasure or pain. "Norms" that bring the greatest amount of pleasure for the greatest number of people are considered moral.
    - Among other philosophers, A. J. Ayer," Language, Truth and Logic", Penguin Books, 2001, suggests that moral statements reflect attitudes of individuals, and philosophy is unable to determine right and wrong.
- Religion. Moral determination based on religion is "a system of beliefs and rules which individuals revere and respond to in their lives and which are seen as

emanating directly or indirectly from some intangible power" Broom, 2003 [132]. In fact according to Broom all religions share a system for discouraging harm to others.

4.38.2 Existence and Causal Relationships to Informal Sanctions

Morality can be a powerful deterrent. Morality restrains such conduct that an attacker would find opposed to her moral belief; and this could be independent of a cost-benefit calculus, McPherson [133].

Additionally, Paternoster and Simpson [27], maintain that high morality creates "non-marketable" areas in which no motivation or opportunity will convince a potential attacker to launch an attack.

Morality is often the underlining source of shame for committing a crime. It is also often the source of the embarrassment of the perpetrator of a crime regarding his friends and relatives when his lack of following moral norms is publicly realized. Depending on the strength of the moral conviction of the social group that the offender is a member of, so will be the corresponding stigma, commitment and attachment costs for failure to abide by its norms. See Williams and Hawkins, 1986

The above authors also note that morality also indirectly affects the deterrence due to formal punishment because the perceived threat of punishment intensifies one's condemnation of the act; with such condemnation operates as a moral inhibitor. Gibbs [114] refers to this preventive consequence of legal punishment as "normative validation." This principle originated with Durkheim [124] who stated that “legal punishment can reinforce the condemnation of wrongful acts”.

4.38.3 Discussion

Deterrence due to morality, and shame, may be limited in information security because of the remoteness of the attacker from the victim and lack of clarity of laws. Both of these factors cause potential attackers to be insensitive to moral norms. Companies and schools can counter this by a strong policy and robust training and awareness of the moral and other consequences of computer crime, these being aimed at preventing insider attacks. Since many of the information security infractions are perpetrated by amateur computer criminals who will not consider committing other crimes due to moral considerations, such potential criminals are likely to be affected by moral training and awareness. This would follow the positive experience of corporations that have a strong security policy, robust security training, and awareness of the moral implications of corporate crime.

Paternoster, 2010 [115], quotes Beccaria who argues that “the surest but most difficult way to prevent crimes is by perfecting education”. Paternoster understands this to refer to “moral education or self-restraint education on virtue”.

The effectiveness of widespread moral education is demonstrated by the Mothers Against Drunk Driving (MADD) public campaign, which increases the moral condemnation of drunk driving, and thereby its stigma to the point that it is equal or exceeds that of an arrest [125].

4.39 Contrast Rational Choice and Routine Activity

Earlier, the Rational Choice and Routine Activity theories were discussed in Section 3.2, Typical Crime Theories, to explain cybercrime. Both of these theories can be used to model cybercrime. They both: (1) place far more weight on the situation determinates (opportunity) than most other criminological theories, (2) recognize the distinction between criminal involvement (motivation) of the perpetrator and the criminal event, and (3) provide an organizing perspective i.e. a model, to analyze crime [134].

Routine Activity emphasizes the criminal event's opportunity and deemphasizes the criminal's event's motivation. Routine Activity is oriented to a macro population level. Routine Activity is a causal theory that can link changes in routine activities to changes in crime rates. Finally, Routine Activity only implicitly assumes a rational offender.

Rational Choice is based on cost (deterrence) and benefit (motivation), but also takes the criminal event (opportunity) into account. In this theory motivation, opportunity and deterrence are equal partners. Offenders' decisions to commit the crime are at the micro individual level. Finally, Rational Choice explicitly assumes a rational offender.

At first glance Routine Activity may seem to be a good match for our model because of its emphasis on opportunity which makes up a good part of the model. Also, as a causal theory, Routine Activity will allow for dynamic changes more than the more static nature of the Rational Choice model.

However, Rational Choice equally emphasizes motivation, opportunity and deterrence which are key parts of the general influence model. Furthermore, since the orientation of the model is at the micro level, from the offender's perspective, Rational Choice will allow the model to be easily applied to individual case situations. Finally, because advanced amateur and professional attackers spend great effort in planning successful attacks (benefit) and avoiding detection (cost), Rational Choice theory, which explicitly assumes a rational offender, synchronizes with cybercrime.

It is for above reasons that this work found Rational Choice as the best fit for this model of cybercrime. However, to the extent that causality exists in the model, the Influence Model utilizes aspects of Routine Activity.

4.40 Criminal Theories that Tie into the General Influence Model

Rational Choice is used to explain the top level nodes of motivation (benefit), deterrence (cost), and opportunity (situational perspective).

Low self-control can be used to explain the low level amateur that is lacking in skill, does not have a propensity to crime, is subject to self-centeredness and a preference for risk taking, and has little interest in long term planning.

Desire for control (DC) theory can be used for the advanced amateur and professional cyber-attackers criminal behavior.

It would seem then that low self-control, desire for control and other enduring individual differences that distinguish offenders from non-offenders - which are type of person theories – may be incompatible with situational theories like Rational Choice and Routine Activity. However, Nagin and Paternoster, 1993 argue that there is no fundamental incompatibility between the theories of low self-control and the Rational Choice, Routine Activity theories and those dealing with social control perspectives. They found evidence of support for both “enduring individual differences” and Rational Choice theories to explain drunken driving, theft, and sexual assault. Therefore these individual differences theories can be used in conjunction with Rational Choice theory.

As stated in Section 4.3.1 even the ordinary amateur's cybercrimes can be explained by drawing from Rational Choice theory. This thesis settled on low self-control theory because it addresses the amateur's impulsivity and lack of motivation for skill enhancement.

Deterrence theory is used to explain the relevance of certainty, severity, and swiftness of punishment for their ability to deter cybercrime.

Social control theories, dealing essentially with informal sanctions, are used to explain the role of shame and embarrassment as moral deterrents. Stigma, commitment and attachment costs are collateral informal punishments resulting from formal punishments. They are elements in social control theories.

4.41 References

[1] Z. Mohaghegh-Ahmadabadi. 2007, "On the Theoretical Foundations and Principles of Organizational Safety Risk Analysis," Ph.D. thesis, Department of Mechanical Engineering, University of Maryland.

[2] Felson, M., and Clarke, R., 1998, *Opportunity Makes the Thief: Practical Theory for Crime Prevention,* Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, London.

[3] Felson, M., 1994, *Crime and Everyday Life : Insights and Implications for Society,* Pine Forge Press, Thousand Oaks, CA.

[4] Wikipedia contributors, 2012, "Hacker (Computer Security)," from http://en.wikipedia.org/wiki/Hacker_%28computer_security%29.

[5] Rogers, M., 2010, *Cybercrimes: A Multidisciplinary Analysis*, Springer, Berlin Heidelberg, Chap. "The Psyche of Cybercriminals: A Psycho-Social Perspective".

[6] Stoneburner, G., Goguen, A., and Feringa, A., 2002, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology," SP 800-30, U.S. Dept. of Commerce, National Institute of Standards and Technology, Gaithersburg, MD.

[7] Piquero, L., Lyn, E., and Simpson, S., 2005, "Integrating the Desire-for-Control and Rational Choice in a Corporate Crime Context," Justice Quarterly**, (22) 2**, pp. 252-280.

[8] Sutherland, E., 1949, *White Collar Crime*, Dryden press, New York.

[9] Simon, H.A., 1976, *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*, Free Press, New York.

[10] Maslow, A., 1954, *Motivation and Personality*, Harper, New York, NY.

[11] Verizon RISK Team, 2012, "2012 Data Breach Investigations Report," Verizon, .

[12] Richardson, R., 2011, "CSI Computer Crime and Security Survey 2010/2011," Computer Security institute, from http://gocsi.com/survey.

[13] United States. Dept. of Justice, n.d., "USDOJ: CRM: About the Criminal Division," from http://www.justice.gov/criminal/fraud/websites/idtheft.html.

[14] Franklin, J., Paxson, V., and Perrig, A., 2007, "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants," *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 375-388.

[15] Sutton, M., 2010, "Stolen Goods Market," Problem-Oriented Guides for Police Problem-Specific Guides, Series No. 57, U. S. Department of Justice, Washington, DC.

[16] Sterner, E., 2011, "Retaliatory Deterrence in Cyberspace," Strategic Studies Quarterly**, (5) 1**, pp. 62-80.

[17] Vascellaro, J.,Dean, J., andGorman, S., 2010, "Google Warns of China Exit Over Hacking; Cyber Attack Targeted as Many as 34 Firms, Email of Human-Rights Activists; Investigators Probe Link to Chinese Government," Wall Street Journal.

[18] Sam Gustin, S., January 13, 2013, "Aaron Swartz, Tech Prodigy and Internet Activist, is Dead at 26," Time Magazine, Technology & Media.

[19] Adams, R., July 21, 2011, "Harvard's Aaron Swartz Indicted on MIT Hacking Charges," The Guardian.

[20] O'Neill, B., January 25, 2013, "Only One Person is Responsible for Aaron Swartz's Death, and that is Aaron Swartz," Telegraph.Co.Uk.

[21] Juvonen, J., and Gross, E., 2008, "Extending the School Grounds?-Bullying Experiences in Cyberspace," The Journal of School Health**, (78) 9**, pp. 496-505.

[22] Mishna, F., Cook, C., Gadalla, T., Daciuk, J., and Solomon, S., 2010, "Cyber Bullying Behaviors among Middle and High School Students," American Journal of Orthopsychiatry**, (80) 3**, pp. 362-374.

[23] USLEGAL, 2012, "Cyberextortion Law & Legal Definition," from http://definitions.uslegal.com/c/cyberextortion/.

[24] Kowalski, E., Cappelli, D., and Moore, A., 2008, "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector
," Carnegie Mellon Software Engineering Institute, Pittsburgh, PA.

[25] Addley, E., and Halliday, J., 2010, "The US Embassy Cables War Over WikiLeaks: Cyber War Erupts as WikiLeaks Supporters Join Fray: MasterCard and Other Sites Disrupted on Day of Concerted Online 'Revenge Attacks'," The Guardian (London) - Final Edition, Guardian home pages, p. 4.

[26] Shakespeare, W., and Durband, A., 1986, *Hamlet*, Barron's, Woodbury, NY.

[27] Paternoster, R., and Simpson, S., 1996, "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," Law & Society Review**, (30) 3**, pp. 549.

[28] United States. Federal Bureau of Investigations, 2013, "Hate Crime—Overview," from http://www.fbi.gov/about-us/investigate/civilrights/hate_crimes/overview.

[29] Gottfredson, M., and Hirschi, T., 1990, *A General Theory of Crime,* Stanford University Press, Stanford, CA.

[30] Cornish, D., and Clarke, R., 1987, "Understanding Crime Displacement: An Application of Rational Choice Theory," Criminology**, (25) 4**, pp. 933-948.

[31] *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences,* 2011, The National Academies Press, Washington, DC.

[32] Clarke, R., and Mayhew, P., 1988, "The British Gas Suicide Story and its Criminological Implications," Crime and Justice**, (10)**, pp. 79-116.

[33] Reppetto, T., 1976, "Crime Prevention and the Displacement Phenomenon," Crime & Delinquency**, (22) 2**, pp. 166-177.

[34] Gabor, T., 1981, "The Crime Displacement Hypothesis: An Empirical Examination," Crime & Delinquency**, (27) 3**, pp. 390-404.

[35] Ransbotham, S., and Mitra, S., 2009, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," Information Systems Research**, (20) 1**, pp. 121-139.

[36] *J. Barney Stokes and G. Lee Stokes, Plaintiffs in Error, v. The State Of Florida,* 1907, Supreme Court of Florida, Division B.

[37] United States. Federal Bureau of Investigations, 2012, "Uniform Crime Reports," from http://www.fbi.gov/about-us/cjis/ucr/ucr.

[38] "Internet Security Threat Report, Volume 17," 2012, Symantec Corporation, Mountain View, CA.

[39] Cisco Security, 2011, "Email Attacks: This Time it's Personal," from http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf.

[40] Keizer, G., 2012, "Is Stuxnet the 'Best' Malware Ever?" Computerworld**,** 12/26/2012.

[41] Lemke, T., 2004, "Cyber-Criminals use 'Bot' to Strike Terror," The Washington Times, Business, p. A16.

[42] Rooney, B., 2012, "Advanced Malware Targets Middle East," Wall Street Journal.

[43] Duggal, P., 2002, *Cyberlaw : The Indian Perspective*, Saakshar Law Publications, New Delhi.

[44] Herzog, P., 2010, "OSSTMM 3 – the Open Source Security Testing Methodology Manual," from http://www.isecom.org/mirror/OSSTMM.3.pdf.

[45] Cole, E., 2002, *Hackers Beware*, New Riders, Indianapolis, IN.

[46] Panjwani, S., Tan, S., Cukier, M., and Jarrin, K., 2005, "An Experimental Evaluation to Determine if Port Scans are Precursors to an Attack," *Proceedings, International Conference on Dependable Systems and Networks*, pp. 602-611.

[47] *Verdict in the case Avi Mizrahi v. Israeli Police Department of Prosecution*, 2004.

[48] Moore, D., Shannon, C., and Claffy, K., 2002, "Code-Red: A Case Study on the Spread and Victims of an Internet Worm," *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment*, pp. 273-284.

[49] Ackoff, R., 1989, "From Data to Wisdom," Journal of Applies Systems Analysis**, (16)**, pp. 3-9.

[50] Gordon, L., 2012, "Nmap - Free Security Scanner for Network Exploration & Security Audits," from http://nmap.org/.

[51] "Wireshark 1.8.3 and 1.6.11," 2012, Wireshark News**,** October 2.

[52] Netstumbler, 2012, "Downloads - NetStumbler 0.4.0," from http://www.netstumbler.com/downloads/.

[53] Softpedia, 2012, "Download Nessus 5.0.2 Free - Complete and very Useful Network Vulnerability Scanner," from http://www.softpedia.com/get/Security/Security-Related/Nessus.shtml.

[54] SecurityFocus, 2010, "LC 5 / L0phtCrack," from http://www.securityfocus.com/tools/1005.

[55] Help Net Security, 2011, "Download Cain & Abel," from http://www.net-security.org/software.php?id=110.

[56] Openwall, n.d., "John the Ripper Password Cracker," from http://www.openwall.com/john/.

[57] Aircrack-ng, 2013, "Aircrack-Ng 1.1," from http://www.aircrack-ng.org/.

[58] Giacobbi, G., 2006, "The GNU Netcat -- Official Homepage," from http://netcat.sourceforge.net/.

[59] Sanfilippo, S., 2013, "Hping - Active Network Security Tool," from http://www.hping.org/.

[60] Mitnick, K., and Simon, W., 2002, *Art of Deception : Controlling the Human Element of Security*, John Wiley & Sons, Inc., Indianapolis, ID.

[61] United States Computer Emergency Readiness Team, 2013, "US-CERT - United States Computer Emergency Readiness Team," from http://www.us-cert.gov/.

[62] Berrueta, D., 2003, "A Practical Approach for Defeating Nmap OS-Fingerprinting," from http://nmap.org/misc/defeat-nmap-osdetect.html.

[63] Frei, S., Tellenbach, B., and Plattner, B., 2008, "0-Day Patch - Exposing Vendors (in)Security Performance," *Black Hat 2008 Europe*.

[64] Radianti, J., Sveen, F., and Gonzalez, J., "Assessing Risks of Policies to Patch Software Vulnerabilities," *Proceedings of International System Dynamics Conference*.

[65] Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., Dobson, J., Mcdermid, J., and Gollmann, D., 1993, "Towards Operational Measures of Computer Security," Journal of Computer Security**, (2) 2-3**, pp. 211-226.

[66] Vroom, V., 1964, *Work and Motivation*, Wiley, New York.

[67] Madan, B., Goseva-Popstojanova, K., Vaidyanathan, K., and Trivedi, K., 2004, "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems," Performance Evaluation**, (56) 1-4**, pp. 167-186.

[68] Howard, M., and LeBlanc, D., 2003, *Writing Secure Code*, Microsoft Press, Redmond, WA.

[69] Jones, J., 2005, "An Introduction to Factor Analysis of Information Risk (FAIR)," from http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf.

[70] IEEE Standards Association, 2013, "IEEE SA - POSIX - Austin Joint Working Group," from http://standards.ieee.org/develop/wg/POSIX.html.

[71] Lye, K., and Wing, J.M., 2002, "Game Strategies in Network Security," CMU-CS-02-136, Carnegie Mellon University, Pittsburgh, PA.

[72] Gollmann, D., 2006, *Computer Security*, Wiley, Hoboken, NJ.

[73] Mell, P. and Scarfone, K., 2011, "CVSS v2 Complete Documentation," from http://www.first.org/cvss/cvss-guide.html#n1.

[74] Mell, P., and Scarfone, K., 2010, "The Common Configuration Scoring System," NISTIR 7502, National Institute of Standards and Technology, Gaithersburg, MD.

[75] Van Ruitenbeek, E., and Kent, K., 2009, "The Common Misuse Scoring System (CMSS) Metrics for Software Feature Misuse Vulnerabilities," NISTIR 7517, National Institute of Standards and Technology, Gaithersburg, MD.

[76] King, C., Dalton, C., and Osmanoglu, T., 2001, *Security Architecture : Design, Deployment, and Operations,* Osborne/McGraw-Hill, New York.

[77] Bishop, M., 2003, *Computer Security: Art and Science,* Addison-Wesley, Boston.

[78] Butler, S., 2002, "Security Attribute Evaluation Method: A Cost-Benefit Approach," *Proceedings of the 24th International Conference on Software Engineering. ICSE***, 24**, pp. 232-240.

[79] Stoneburner, G., 2001, "Underlying Technical Models for Information Technology Security Recommendations of the National Institute of Standards and Technology," SP 800-33, National Institute of Standards and Technology, Gaithersburg, MD.

[80] National Institute of Standards and Technology, 1995, "An Introduction to Computer Security: The NIST Handbook Computer Security," NIST Special Publication 800-12, National Institute of Standards and Technology, Gaithersburg, MD.

[81] Schneier, B., 2000, *Secrets and Lies: Digital Security in a Networked World,* John Wiley, New York.

[82] Kraemer, S., and Carayon, P., 2007, "Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists," Applied Ergonomics**, (38) 2**, pp. 143-154.

[83] Reason, J., 1990, *Human Error,* Cambridge University Press, New York, NY.

[84] Blackman, H., Gertman, D., and Boring, R., 2008, "Human Error Quantification using Performance Shaping Factors in the SPAR-H Method," *52nd Human Factors and Ergonomics Society Annual Meeting, HFES 2008***, 3**, pp. 1733-1737.

[85] Great Britain Health and Safety Executive, 2000, *Reducing Error and Influencing Behaviour,* HSE Books, Sudbury.

[86] Peltler, T., 2005, "Social Engineering: Concepts and Solutions," Computer Security Journal.**, (21) 4**, pp. 40-47.

[87] Cialdini, R., 2001, *Influence: Science and Practice,* Allyn and Bacon, Boston, MA.

[88] Samani, R., 2010, "Re-Defining the Human Factor," Infosecurity**, (7) 2**, pp. 30-33.

[89] International Atomic Energy Agency, 2008, *Nuclear Security Culture: Implementing Guide.* International Atomic Energy Agency, Vienna.

[90] Cooper, M., 2000, "Towards a Model of Safety Culture," Safety Science**, (36) 2**, pp. 111-136.

[91] Cox, S., and Cox, T., 1991, "The Structure of Employee Attitudes to Safety: A European Example," Work & Stress Work & Stress**, (5) 2**, pp. 93-106.

[92] Collmann, J., Coleman, J., Sostrom, K., and Wright, W., 2004, "Organizing Safety: Conditions for Successful Information Assurance Programs," Telemedicine Journal and e-Health**, (10) 3**, pp. 311-320.

[93] BSI Group, 2013, "Information Security Management Systems - Guidelines for Information Security Risk Management," BS7799-3 / BS 7799-3, from http://17799.standardsdirect.org/bs7799.htm.

[94] Chia, P., Maynard, S., and Ruighaver, A., 2002, "Exploring Organisational Security Culture: Developing a Comprehensive Research Model," *ISOneWorld Conference*.

[95] Fattah, E., 1992, *Towards a Critical Victimology*, St. Martin's Press, New York.

[96] Nagin, D., and Paternoster, R., 1993, "Enduring Individual Differences and Rational Choice Theories of Crime," Law and Society Review**, (27) 3**, pp. 467-496.

[97] Cochran, J., Aleksa, V., and Sanders, B., 2008, "Are Persons Low in Self-Control Rational and Deterrable?" Deviant Behavior**, (29) 5**, pp. 461-483.

[98] Hirschi, T., and Gottfredson, M., 1995, "Control Theory and the Life-Course Perspective," Studies on Crime and Crime Prevention**, (4) 2**, pp. 131-142.

[99] Wilson, J.Q., and Herrnstein, R., 1985, *Crime and Human Nature*, Simon and Schuster, New York, NY.

[100] Piquero, A., and Pogarsky, G., 2002, "Beyond Stafford and Warr's Reconceptualization of Deterrence: Personal and Vicarious Experiences, Impulsivity, and Offending Behavior," Journal of Research in Crime and Delinquency**, (39) 2**, pp. 153-186.

[101] Wright, B. R. E., Caspi, A., Moffitt, T., and Paternoster, R., 2004, "Does the Perceived Risk of Punishment Deter Criminally Prone Individuals? Rational Choice, Self-Control, and Crime," Journal of Research in Crime and Delinquency**, (41) 2**, pp. 180-213.

[102] Cunniff, M. and Langan, P., 1992, "Bureau of Justice Statistics (BJS) - Recidivism of Felons on Probation, 1986-1989, " from http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=3994.

[103] Gibbs, J., 1968, "Crime, Punishment, and Deterrence," Southwestern Social Science Quarterly**, (48) 4**, pp. 515-30.

[104] Tittle, C., 1969, "Crime Rates and Legal Sanctions," Social Problems**, (16) 4**, pp. 409-23.

[105] Paternoster, R., 1987, "The Deterrent Effect of the Perceived Certainty and Severity of Punishment: A Review of the Evidence and Issues," Justice Quarterly**, (4) 2**, pp. 173-218.

[106] Klepper, S., and Nagin, D., 1989, "The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited," Criminology**, (27) 4**, pp. 721-746.

[107] Pogarsky, G., 2002, "Identifying Deterrable Offenders: Implications for Research on Deterrence," Justice Quarterly**, (19) 3**, pp. 431-452.

[108] Higgins, G., Wilson, A., L., and Fell, B., 2005, "An Application of Deterrence Theory to Software Piracy," Journal of Criminal Justice and Popular Culture**, (12) 3**, pp. 166-184.

[109] D'Arcy, J., and Herath, T., 2011, "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," European Journal of Information Systems**, (20) 6**, pp. 643-658.

[110] Straub, D., 1990, "Effective IS Security: An Empirical Study," Information Systems Research Information Systems Research**, (1) 3**, pp. 255-276.

[111] D'Arcy, J., Hovav, A., and Galletta, D., 2009, "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research**, (20) 1**, pp. 79-98.

[112] Herath, T., and Rao, H., 2009, "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," Decision Support Systems**, (47) 2**, pp. 154-165.

[113] Nagin, D., and Pogarsky, G., 2001, "Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence," Criminology**, (39) 4**, pp. 865-892.

[114] Gibbs, J., 1975, *Crime, Punishment, and Deterrence,* Elsevier, New York.

[115] Paternoster, R., 2010, "How Much do we really Know about Criminal Deterrence?" Journal of Criminal Law and Criminology**, (100) 3**, pp. 765-824.

[116] Legge, J., and Park, J., 1994, "Policies to Reduce Alcohol-Impaired Driving: Evaluating Elements of Deterrence," Social Science Quarterly**, (75) 3**, pp. 594.

[117] Howe, E., and Loftus, T., 1996, "Integration of Certainty, Severity, and Celerity Information in Judged Deterrence Value: Further Evidence and Methodological Equivalence," Journal of Applied Social Psychology**, (26) 3**, pp. 226-242.

[118] Spelman, W., 2000, "What Recent Studies do (and Don't) Tell Us about Imprisonment and Crime," Crime and Justice.**, (27)**, pp. 419-494.

[119] Salem, R., and Bowers, W., 1970, "Severity of Formal Sanctions as a Deterrent to Deviant Behavior," Law & Society Review**, (5) 1**, pp. 21-40.

[120] *18 USC § 1030 - Fraud and Related Activity in Connection with Computers*, 2013.

[121] University of Maryland, 2008, "Policy on the Acceptable use of Information Technology Resources," from http://www.nethics.umd.edu/aup/.

[122] Clark, A., and Gibbs, J., "Social Control: A Reformulation," Social Problems**, (12) 4**, pp. 398-415.

[123] Anderson, L., Chiricos, T., and Waldo, G., 1977, "Formal and Informal Sanctions - A Comparison of Deterrent Effects," Social Problems**, (25) 1**.

[124] Durkheim, E., 1964, *The Rules of Sociological Method*, Free Press of Glencoe, New York.

[125] Williams, K., and Hawkins, R., 1986, "Perceptual Research on General Deterrence: A Critical Review," Law & Society Review**, (20)**, pp. 545-72.

[126] Grasmick, H., and Bursik, R., 1990, "Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model," Law and Society Review**, (24) 3**, pp. 837-861.

[127] Braithwaite, J., and Geis, G., 1982, "On Theory and Action for Corporate Crime Control," Crime and Delinquency**, (28) 2**, pp. 292-314.

[128] Piquero, A., and Tibbetts, S., 1996, "
Specifying the Direct and Indirect Effects of Low Self-Control and Situational Factors in Offenders' Decision Making: Toward a More Complete Model of Rational Offending," Justice Quarterly**, (13) 3**, pp. 481-510.

[129] Kaufman, G., 1989, *The Psychology of Shame: Theory and Treatment of Shame-Based Syndromes*, Springer Pub. Co., New York, NY.

[130] D'Arcy, J., and Hovav, A., 2009, "Does One Size Fit all? Examining the Differential Effects of IS Security Countermeasures," Journal of Business Ethics**, (89)** Supplement, pp. 59-71.

[131] Jordan, T., and Taylor, P., 1998, "A Sociology of Hackers," The Sociological Review**, (46) 4**, pp. 757.

[132] Broom, D., 2003, *The Evolution of Morality and Religion,* Cambridge University Press, Cambridge, UK; New York.

[133] McPherson, M., 1984, "Limits of Self-Seeking: The Role of Morality in Economic Life," Ballinger Publishing Company, Cambridge, Massachusetts.

[134] Clarke, R., and Felson, M., 2004, *Routine Activity and Rational Choice. Vol. 5,* Transaction, New Brunswick, N.J.

5 Case Studies

5.1 Introduction

A validation of the model was made by scrutinizing the facts of eight IS cyber-crime cases by applying 14 questions, Appendix A, Questions, whose answers determined the applicability of specific nodes to specific cases, thereby detailing and mapping applicable nodes for each case. This process established a model for each case that directly reflected its facts, giving credibility to the model and its further applicability to conclusions regarding significant factors of cyber-attacks and their prevention.

The eight cases are the following - perpetrator/cyber-attack: (1) Morris/worm on Internet; (2) Phillips/"brute-force", Texas University website compromised; (3) Barrington/grade and residency status changing; (4) Carlson/spam; (5) Gonzalez/debit and credit card fraud; (6) Shea/ "time-bomb", debit and credit card corruption; (7) Getloaded Co./stealing competitor's proprietary information; (8) Manning/ allegedly passing classified military, diplomatic and political information. They were particularly chosen because they were all except the Manning case tried under the Computer and Abuse Act of 1986 [1] . This law is one of the oldest computer crimes law, and considered by many as the most successful law under which cyber-crimes have been tried.

Six of these cases studies are about crimes whose verdicts were appealed. The advantage of looking at such cases is that the judge in rendering his decision on the merits of an appeal includes a Statement of Facts which can be assumed to be the true nature of the crime.

The Gonzalez case did not have an appeal but it is well documented in both the court proceedings and in the many press reports. It is further supported by an extensive interview with Gonzalez by Time Magazine. It was also quite famous as it compromised more than 180 million credit card records.

Five of the cases are not particularly famous and therefore had scant media coverage.

The Morris worm case is particularly famous as it was considered to be the first worm attack; it disabled about one quarter of the Internet.

The Manning case is included although it is not being tried under the Computer Crime Abuse Act but under the United States Military Code of Justice. This case has not been prosecuted at this writing so the facts as presently understood may change. It is a very good example of where someone using very simple techniques can defeat a large system whose security is very inconsistent.

Each case ends with a “What If”, namely: what simple defense procedure(s) could have stopped an attack or mitigated its effects.

5.2 Morris Worm

On November 2, 1988, Robert T Morris intentionally distributed a “worm” on the Internet that caused massive disruptions of services. A worm is program that replicates through network connections onto other computers, and uses computers and networks as resources of its targets. He was found guilty. The following is a digest the “Statement of Facts” from the proceedings of his appeal [2].

Morris joined Cornell University as a graduate student in the fall of 1988. He was given a computer account. He had considerable knowledge of computers from his previous studies, at Harvard University, and various jobs he held there. At Cornell he discussed computer security with fellow students and his ability to penetrate networks.

He began to work on a worm early on at Cornell, in October 1988. His goal for authoring and later deploying this worm was to "demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered". Morris' plan was to release the worm and let it spread quickly and briefly to university, governmental and military computers throughout the country through Internet.

He designed his worm to be difficult to detect, to limit drawing attention as it spread. Accordingly the worm made very compact, and used few resources. It had encrypted code to make it difficult for a programmer to decompile. Also, its program was designed to kill itself when an infected computer was rebooted.

To further avoid detection, and to limit the worm's impact by single computers crashing due to accumulating multiple copies, the program was designed to assure that any attacked computer ran only one copy of the worm. It asked a targeted computer if it already had a copy of this program, and copied only to a "no" response. To avoid defender immunization activation by a "yes" response, Morris included in the worm logic that every seventh time it received a "yes" response it will copy itself regardless of the response. He underestimated the number of times a computer would be asked this question and as a result many computers ended up running many copies of the worm.

Morris took advantage of vulnerabilities he discovered in the SEND Mail program, finger daemon program, and in the UNIX Trusted hosts feature. Additionally, he implemented automatic password guessing to gain access to targeted computers.

On November 2, 1988 Morris released the worm from a computer at MIT where he also had an account, hoping that it would not draw attention to him at Cornell. He soon found that the worm was replicating itself far faster than he had planned. Since many multiple copies of the program were running on single machines many computers and networks became overloaded and crashed. Morris tried to send anonymous e-mail with instructions to programmers on how to kill the worm and prevent infection. Due to the congestion on the networks his message did not get through to the people who could have stopped the infection.

Morris was found guilty of violating the Computer Fraud and Abuse Act. He was sentence to 400 hours of community service and fined $10,050.00 and court costs.

This case is presented as an adaptation of the general influence model in, Figure 25, which is preceded by discussions of the facts and issues pertaining to its nodes. The relative strengths of some factors – nodes - and their relationships can be understood from the information associated with the various facts.

5.2.1 Nodes and Model

Motivation

Challenge Morris' challenge was given in the Statement of Facts, "The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered." This was defined as the goal challenge.

Amateur (advanced) Based the description of the defendant as a "first-year graduate student in Cornell University's Computer Science PhD program", and the motivation goal of a challenge would classify the defendant as an advanced amateur.

Outsider Morris' worm affected networks to which he had no legal access, and therefor he is classified as an outsider. This classification pertains to Internet as it has grown subsequent to 1988. In 1988 Internet was operated by a close knit group of university and military personnel, and with Morris having access as one of that group he would have then been considered as an insider.

Opportunity

Random Attacks The Morris worm attacked randomly as is stated, **"**Morris designed the program to spread across a national network of computers after being inserted at one computer location connected to the network".

Reconnaissance and Knowledge The reconnaissance Morris used for his attacks was an outgrowth of knowledge he acquired about targets, and discovering ways to achieve his goals. He acquired this knowledge through his education at Harvard and then at Cornell University's Computer Science PhD program. Also, "Morris engaged in various discussions with fellow graduate students about the security of computer networks and his ability to penetrate them”. His knowledge and interest in system security lead him directly to his goal of “demonstrating the inadequacies of current security measures on computer networks”. He used his “knowledge of studying various common protocols and their vulnerabilities” to find weakness in the system that can be exploited as demonstrated by the “four ways in which the worm could break into computers on the network”.

Morris placed great effort in attempting to disguise his attacks and preventing himself from being discovered as the attacker. His attempt to prevent the attack from being discovered was by having the worm occupy little computer operation time, and thus not interfere with normal use of the computers.

Also, Morris wanted to ensure that the worm did not copy itself onto a computer that already had a copy because multiple copies of the worm on a computer would make the worm easier to be detected by bogging down the system, and ultimately cause the computer to crash.

In addition to making the attack difficult to detect Morris made the attack difficult to be stopped from spreading.

Effort The effort both in terms of its intensity and time spent seemed to have been adequate for the success of this attack. As stated in the Statement of Facts Morris began work on the worm in October of 1988 and released the worm on November 2, 1988.

Perhaps, had he spent more time, he would have rechecked his assumptions and avoided the flaw that ultimately caused his worm to replicate far faster and more disruptively than he had envisioned.

Skills Morris did possess great skills to use his knowledge to build and implement this worm. As mentioned in the Statement of Facts, he had made a mistake in calculating the rate of possible reinfection, which ultimately lead to far more infections then he anticipated.

Time Bound The goal of this attacker was to infect as many computers as possible without being detected. This had be done before the computers were rebooted which he estimated as one or two weeks. The reboot would kill the worm.

Means The attacks which disabled large parts of the Internet were denial of service attacks. These attacks did not alter or destroy data.

Security Policy The Statement of Facts does not directly discuss the defenders' security policies, but much can be learned from published reports and the state of the Internet at the time of this attack. At that time the Internet was viewed as an educational tool with a great emphasis on sharing and trust. In this environment of trust, security policies were not particularly strong or well followed. The organizational factors were very ripe for such an attack to take place because it took full advantage in the trust between participants in the Internet. The defenders' capabilities were much stronger in the reactive mode once an attack took place as to what was needed to stop the attack. This can be seen from the effort Morris placed in trying to make the attack difficult to stop by duplicating itself onto every seventh computer regardless if the worm may already have infected the targeted computer. The vulnerabilities that Morris had exploited were in two Unix services, Sendmail and the finger daemon, were well known but not corrected.

Deterrence

Futility Much can be learned from the Statement of Facts about what would have deterred Morris from attacking. He was very concerned with the possibility of futility of the attack, that it might not spread as he wished. He used a mechanism of preventing reinfection of a single target - which would lead to detection - by asking a target if it is infected. If the target answered “yes”, the attack skipped the attacked computer. However, Morris feared that a system administrator would use this feature to prevent the spreading of the attack by having all computers return a “yes” when polled if infected, even computers that are not infected . Therefore, Morris added logic to infect every seventh computer regardless of response.

Consequences Morris also apparently feared the consequences of being caught. It is for this reason that even though he was a student on Cornell University he used an account at MIT to launch the attack in order to make it difficult trace the attack back to him. Also, when he had sent an e-mail describing the attack and a counter measure to prevent the spread of the attack he used an anonymous account on a Harvard computer to protect him from being caught.

It is difficult to assess the impact of an immediate punishment and a punishment after time in this case. In this particular case the charges were from newly enacted laws, and it took nine months for the Department of Justice to decide to prosecute. The final sentencing included a $10,050 fine, three years of probation, and 400 hours of community service.

Morality   Morality played a large role in Morris' attack plans. Morris rationalized that as long as his attacks were not detectable and they did not result in loss, alteration or denial of services, he was morally able to proceed with his attack. When he realized that his attacks had caused denial of service because of the higher than anticipated reinfection rate, he attempted to send anonymous e-mail "instructing programmers how to kill the worm and prevent reinfection".

It is difficult to discern the source of Morris' sense of morality, whether it was religious, philosophical, or conscience. But, it is also possible that his father's very high position as a senior scientist at the National Security Agency, with network security responsibilities, played a role in Robert Morris' morality not to let his father down.

What If   If Morris was made aware of the actual moral implication of his act it is likely that he would not have launched the attack. This seems to be so from Morris efforts to stop the attack once he realized how damaging it was. Also, if the system managers would have been more proactive in installing patches, at least one of the exploits that Morris used would not have been effective, thereby mitigating the spread of the worm.

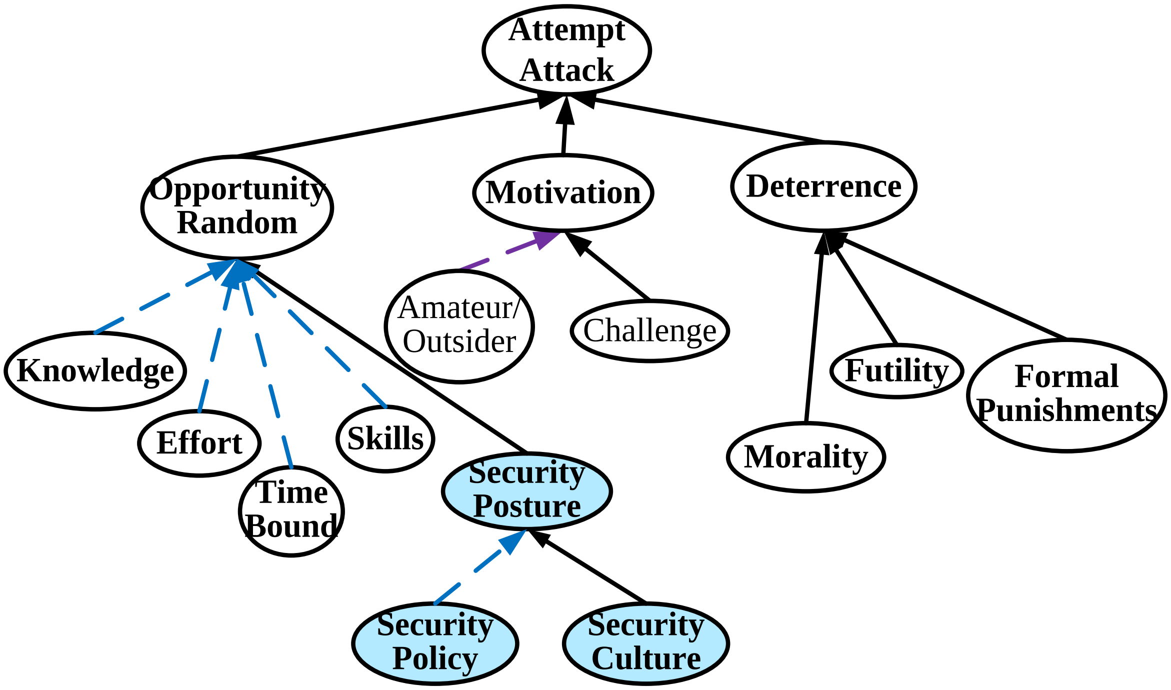


Figure 25: Morris Worm

5.3 Phillips Brute-Force Website Attack

Andrew Phillips by a “brute-force” attack on the University of Texas at Austin (UT) TXClass website compromised 45,000 personal demographics of students, donors and alumni, and caused that website to crash three times [3], [4, 5], [6].

He entered UT Austin in 2001, and was admitted in 2003 into its Department of Computer Science. As all students entering into UT, Phillips signed an “acceptable use” computer policy. Shortly after entering the school in 2001 Phillips began using port scanning programs to scan and later infiltrate hundreds of computers at UT. Theses scans were detected by the University's Information Security Office, and on three separate occasions Phillips was issued a warning.

In early 2002 Phillips designed a computer program to hack into a specific UT website system called "TXClass Learning Central: A Complete Training Resource for UT Faculty and Staff". He had found vulnerability in the login process that he was able to exploit by using a "brute-force attack" program, which automatically transmitted to the website as many as six Social Security numbers per second. The login succeeded when there was a Social Security number match, and Phillips was then able to harvest valuable personal demographics.

Initially, Phillips' program selected ranges of Social Security numbers for all people born in Texas. He later was able to refine his random range to encompass a smaller group of more likely valid Social Security numbers. Over a 14 month period Phillips' program had successfully harvested the personal demographics with corresponding Social Security numbers of 45,000 current and prospective students, donors and alumni of UT.

Phillips attacks hurt the University in several ways. The brute-force attack was essentially a denial of service attack as it caused the UT computer system to crash three times in early 2003 due to overloads of login requests. Also, the 45,000 compromised records caused the University much embarrassment. The University spent $182,000 to access the damage and notify victims that their personal information had been compromised.

After 14 months the University finally discovered the breach and then contacted the US Secret Service. The investigation led to the arrest of Phillips who admitted to designing the brute-force attack program. Phillips maintained that he had no intention to profit from the information that he stole.

Phillips was convicted of violating the Computer Fraud and Abuse Act and sentenced to five years of probation, five hundred hours of community service and restitution of $170,056.00.

The following is the timeline of the Phillips case.

1. Fall 2001: Philips entered University of Texas at Austin.
2. January 30, 2002: Phillips was detected scanning (1st time).
3. February 15, 2002: Phillips was detected scanning (2nd time).
4. April 8, 2002: Phillips was detected scanning (3rd time).
5. October 2002 – November 2002: Phillips downloaded demographic data of people born in Texas.
6. 2003: He was admitted into the Department of Computer Science.
7. January 30, 2003: Phillips created a program to hack into the TXClass Web Site.
8. January 29 – March 30 2003: Phillips used his program to steal 37,000 names and Social Security numbers from the TXClass Web Site.
9. February 26, 2003: TXClass crashed.
10. February 27, 2003: TXClass crashed.
11. February 28, 2003: TXClass crashed.
12. March 2, 2003: The breach discovered (Newsbytes 3/7/2003).
13. February 2002 – March 2003? Over a fourteen-month period, Phillips thus gained access to a mother lode of data on more than 45,000 current and prospective students, donors, and alumni" (US Court of Appeals).

14. March 14, 2003 Phillips was arrested.

15. November 3, 2004 Indictment filled.

This case is presented as an adaptation of the general influence model in Figure 26, which is preceded by discussions of the facts and issues pertaining to its nodes. The relative strengths of some factors – nodes - and their relationships can be understood from the information associated with the various facts.

5.3.1 Nodes and Model

Motivation

Challenge According to Phillips, his only motivation was challenge; he admitted that he only wanted to collect and integrate information. Although the prosecution was unable to prove that he definitely had monetary gain intent, it would have been easy for him to sell to identity thieves merges of the Social Security numbers and demographic information that he downloaded.

Outsider Outsider best describes Phillips, because of his officially very limited access to TXClass website privileges.

Amateur Phillips was essentially an amateur regarding his breaching the University of Texas computer system. He was a student at UT with limited access to its computer system. He did have limited experience with hacking techniques, but most of his hacking was not sophisticated.

Opportunity

Reconnaissance Phillips was caught using scanning techniques on January 30, 2002, February 15, 2002 and April 8, 2002. It is unclear how he used the results from these scans to aid his subsequent attacks.

Random Phillips first attempted logins using random Social Security numbers for the entire State of Texas. Later he improved his algorithm by using only the prefix of the otherwise random Social Security numbers – ones that are specific to three of the most populous counties in Texas - to narrow his searches. These prefixes should have increased the probability of matching with the demographics of UT students, alumni, or benefactors. State universities attract local populations.

The success of his attacks was due to the nature of that "brute- force attack", which "automatically transmitted to the website as many as six Social Security numbers per second, at least some of which would correspond to those of authorized TXClass users". "Phillips's actions hurt the UT computer system. The brute-force attack program proved so invasive - increasing the usual monthly number of unique requests received by TXClass from approximately 20,000 to as many as 1,200,000 - that it caused the UT computer system to crash several times in early 2003." These are quotes are from US Court of Appeals, Fifth Circuit, 2007.

Since all of Phillips' attacks used "brute-force" the nature of his entire attack procedures will be classified as random.

Knowledge and Skills Phillips' initial scanning of the UT system, TXClass, and his attacks by logging in Social Security numbers were rather simple. He did not try to hide his activities, apparently because he did not have the expertise to do so. The program he used for his attacks was simple although effective.

The idea of limiting logging Social Security numbers to those from three of the most populous counties in Texas, based on the prefix of the Social Security number, is only somewhat innovative as the significance of that prefix is well known.

It also took him a long time to locate and merge databases with demographics in order to make his stolen dataset more useful.

The above timeline further indicates that Phillips' skills were at a low level. Despite that Phillips "disavowed that he intended to use or sell the information" he did download a database with demographics of people born in Texas with the apparent intention to build a data base of identity records. It should have been a rather trivial feat for this purpose to fully merge two databases. Phillips after 14 months was still unable to accomplish this.

Furthermore, Phillips was well aware that his brute-force program could crash the TXClass website and thus bring attention to his attacks. As Phillips admitted during cross examination, "TXClass's normal hourly hit volume did not exceed a few hundred requests, but that his brute-force attack created as many as 40,000".

It was also not necessary for him to transmit as many as six Social Security numbers per second to test all the possible matches for the 10 counties he was interested in. Even if each county had a different location prefix, the first three numbers of the Social Security number, all possibilities of the last six digits requires 10 x 1,000,000 or 10 million test matches. This calls for transmitting only four social security numbers per minute.

More importantly, once Phillips realized that he caused the TXClass system to crash he should have throttled back his brute-force attack to prevent further crashes and possibility of discovery.   He did not do this as seen from the fact that the TXClass System crashed on February 26, 27, and on February 28.

Effort   Phillips expended much effort, time and intensity, into his attacks. He was committed to his endeavor from the very time he became a UT student.

Also, he found ways to recover his data even after the server hosting TXClass crashed, due to his attacks.

Time Bound   Phillips needed to complete his discoveries of the Social Security numbers before being detected by the UT system administrator.

His attacks were noisy as they generated much activity on the victim's, UT, computers, and should have been detected.

Human Factors – Attacker Phillips acted alone using relatively simple but slow and effective methods. He was helped by not being detected for a long period of time, although he did not make attempts to conceal activity.

He did share his plans with others, but he did not seek any advice for both gathering Social Security numbers and for exploiting them.

Means The attacks were primarily a disclosure of data attack, as they did not modify data on the UT computer systems. A secondary result of the attacks was denial of service as the attacks overloaded the servers and networks, and caused disruption of hundreds of UT's web application, including library, payroll, and accounting.

Security Posture UT security posture was poor, indeed as admitted by Daniel Updegrove UT VP for Information Security, "We flat out messed up this one," and "Shame on us for leaving the door open" [6]. There is an issue that the only security required for this system was a valid Social Security number. Apparently, the system was either not recording the attack attempts, or the logs were not being monitored. It is incredible that the attacks occurred for fourteen months without being noticed by the IT Department. It also appears that the attacks were not recognized only until after the third time the TXClass System crashed.

Security Policy UT Security Policy was weak for the simple reason that the attacks were not detected for 14 months. This policy weakness was also indicated by the fact that the Security Officer issued early on three warnings to Phillips to stop his unacceptable probes, without further action.

Defender's Tools Defender's tools were weak because failed login attempts were not recorded.

Vulnerabilities The design of the system was essentially vulnerable that it did not require a password, being accessible by only a valid Social Security number.

Deterrence

Certainty of Punishment Phillips was not faced with certainty of punishment. He was warned on three separate occasions not to engage in his probing activities. These warnings were apparently not very strong as they were not followed up with any penalty or punishment. In fact, according to the timeline, he was admitted into the computer science program after he had received the warnings. He was apparently left with a feeling that there is no certainty of punishment. Also, his final punishment was delayed until 2009, six years - involving the appeals process - after being caught.

Morality Phillips did not attach any morality issues to his actions. He declared in his defense that "that an individual's ability to view TXClass's login webpage amounts to a general grant of authorized access to the public-at-large". He was given three warnings against probing, but according to his own testimony they were "a slap on the wrist".

Shame Phillips was removed from his victims, he was caught but continued his activities, so shame was not a fact or. In his eyes as long as he did not intend to use the data he acquired he was not harming his victims. Phillips also seemed unconcerned with the damage he caused UT by the systems crashing three times.

However, he did express remorse at the sentencing phase of his trial, “I’m sorry to my parents, the University of Texas and all these people”, and “It just wasn’t in my mind-set that this kind of thing was going to have this sweeping effect” [7].

What If Had Phillips received a punishment instead of merely warnings for his original scanning, he might have been deterred from committing further attacks. If the TXClass system would have required a user name and a password, this type of attack would not have been possible. Additionally, had the system administrator been more vigilant in monitoring and investigating the source of the system crashes, the attacks would have been discovered much earlier than after the elapse of 14 months that it took to detect them; and their effects could have been mitigated.

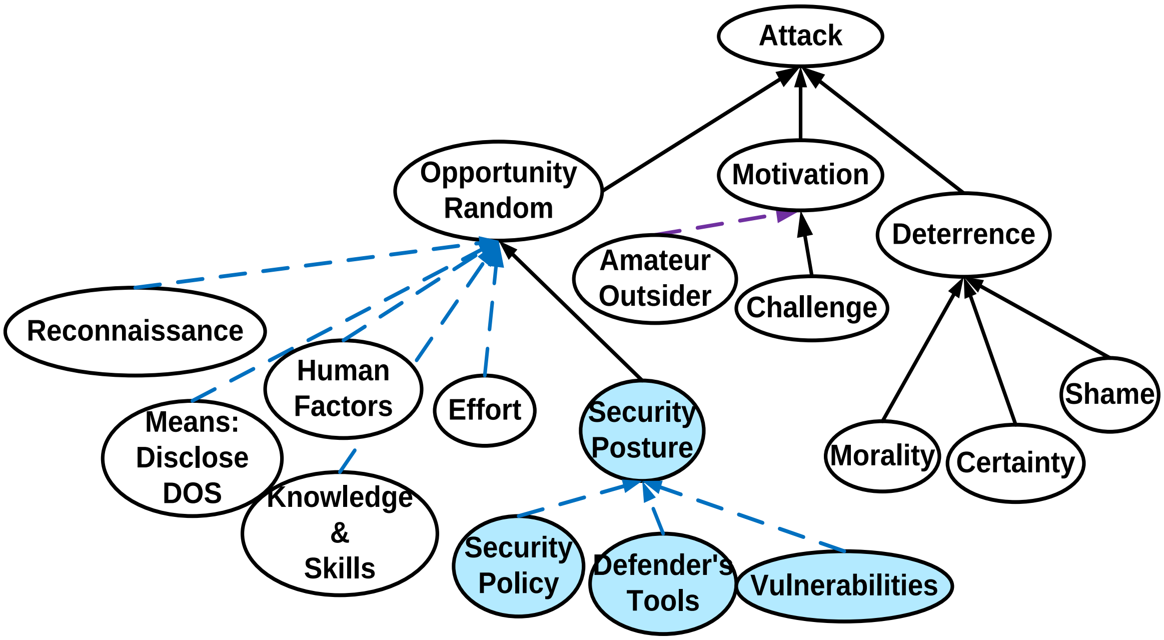


Figure 26: Phillips Brute Force Attack

5.4 Barrington Grade Changing and Residency Status Attacks

Marcus Barrington and two co-defendants, Christopher Jacquette and Lawrence Secrease, all undergraduate students at Florida A&M University, were found guilty of computer fraud for using keyloggers[6] to steal username and passwords of the University Registrar's computers. Their attacks changed 650 grades of at least 90 students and the residency status of out-of-state students to in-state, causing a loss of $137,000 in tuition income. These crimes also damaged to the University's reputation and its grading integrity [8].

[6] A keylogger, also referred to as a keystroke logger, captures every key depression, or keystroke, made on a computer. PCMAG.com.

This case is presented as an adaptation of the general influence model in Figure 27, which is preceded by discussions of the facts and issues pertaining to its nodes. The relative strengths of some factors – nodes - and their relationships can be understood from the information associated with the various facts.

5.4.1 Nodes and Model

Motivation

Non-Monetary Gain Change in final grades to pass courses is classified as non-monetary gain motivation for the attacker.

Monetary Gain The changes in out-of-state student residency status to qualify for reduced in-state tuition would be considered as motivation for monetary gain (for those students). The consequent financial loss to the University was incidental.

Opportunity

Planned Attacks The original attacks targeted to change specific grade and residency records, but when the attackers became aware of the investigation they continued to attack randomly, but as a planned diversion to confuse the investigators.

Reconnaissance The main physical components of the attacks were key loggers, which the attackers installed on the University computers and used them to record key strokes to capture logins and passwords. This is reconnaissance. Special reconnaissance was also used to install and uninstall the keyloggers without detection.

Knowledge Knowledge was employed by the attackers to operate the keyloggers, and to glean from them user names and passwords. Knowledge was also used for the unauthorized operation of the University's system to change grades and residency status without being detected.

Skill Special skills were used to install and conceal the keyloggers without being detected.

Tools The essential tools for the attacks were the keyloggers, for reconnaissance.

Means The means of these attacks was alteration of data, namely changing grades and residencies.

Security Posture The defender's, University's, security culture was obviously weak. From the narrative it is understood that the attackers were able to install the keyloggers numerous times on the sensitive PC's. This was true even after the University became aware that a data breach had taken place. Only when breaches were detected by an alert professor, one month after data changes had already occurred, was an investigation started. These breaches could have been detected and stopped earlier if the University operators had seen the attackers installing keyloggers on their PCs, or if they had noted the extra equipment on their PC's. They also should have questioned that apparently unauthorized logging from unknown sources was entered into their computers using their credentials.

Security Culture The defender's, University's, security culture was obviously weak. Proper training of the University operators to constantly raise awareness of possible security infractions and react quickly was absent; that could have helped to prevent these breaches, or detect them early on.

Security Policy The defender's, University's, security policy was obviously weak. Absent was a computer certificate authentication requirement for access to sensitive applications. This would have prevented these attacks as the attackers would have been unable to access sensitive elements of the University's system.

Defender's Tools Absent were adequate logging tools that detect unusual activity, and, more important, ones that regularly review their output thereby shortening the time between an attack and its detection.

Deterrence

Formal and Informal Sanctions The threat of formal and informal sanctions had little effect on the attackers, as they displayed an unusual amount of resilience in their attacks. Indeed, after they first became aware that they were being investigated and that the grades were restored, they attacked again to change the grades.

Certainty of Consequences The attackers were not very much impressed initially with the certainty of consequences, formal punishment, for their intended crimes. That would have apparently deterred them. When Barrington sensed that the investigation was going to find him, he attempted to conspire with each of his two partners to place the blame on the other one. Instead, his two partners became state witnesses against him in return for a lesser sentence. It appears that once it was clear to the conspirators that they will receive formal punishment, specifically jail time for their crimes, they were willing to go to great lengths to avoid that.

What If Had the defenders' management supported more awareness training it is possible that the staff would of found the keyloggers sooner. Also, had there been a firm policy in place that describes consequences for infractions there would not have been a situation where three warning were issued with no consequences.

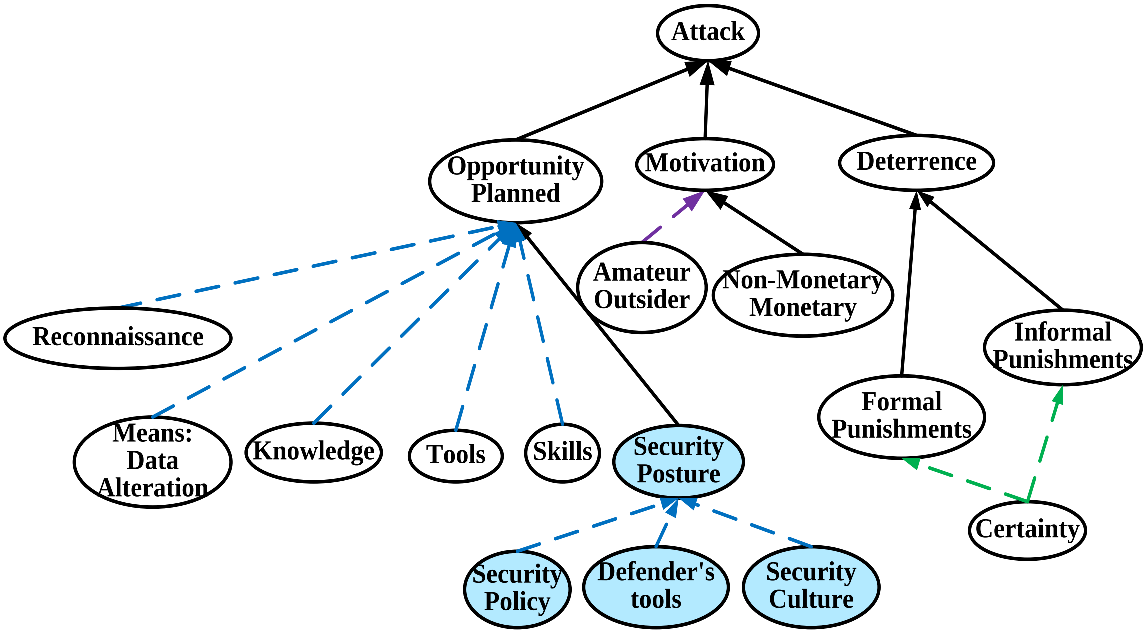


Figure 27: Barrington Grade Changing and Residency Status Attacks

5.5 Carlson E-Mail Spam Attack

Allan Carlson was found guilty on July 14, 2005 for two types of e-mail attacks, and was sentenced to 48 months of imprisonment, and fined $7,900.00. The first kind of attack entailed "direct attack" e-mailing, where he sent 1,000's of e-mails to single e-mail addresses. This spamming caused flooding of the recipients' e-mail accounts. The second kind of attack was an "indirect attack" where he used spoofed addresses as the senders' addresses, and sent 1,000's of e-mails to individual recipients. If the recipients' accounts were non-existent the e-mail was “bounced” back to the spoofed senders addresses. Since many of the recipient’s addresses were non-existent the spoofed senders were flooded with “bounced” e-mail. Both of these attacks are denial of service attacks, and they caused the e-mail users loss of use of their e-mail service. This attacker was a disgruntled Philadelphia Phillies fan who hacked into unsuspecting computers. It was from those computers that Carlson e-mailed these spam messages which contained his complaints about the Phillies management. The targets of his attacks were the Phillies Management and reporters from the local newspapers [9].

This case is presented as an adaptation of the general influence model Figure 28, which is preceded by discussions of the facts and issues pertaining to its nodes. The relative strengths of some factors - nodes - and their relationships can be understood from the information associated with the various facts.

5.5.1 Nodes and Model

Motivation

Amateur While during the appeal process Carlson claimed that he did not know that the result of his sending e-mail to many addresses that are non-existent would result in denial of service to the senders’ e-mail accounts, the court maintained that he did have the expertise to fully understand these results. Although Carlson had a good understanding of the attacks he was launching he will still be classified as amateur as his motivation was non-monetary.

Revenge He was motivated by revenge because he was upset by the policies of his favorite baseball team. According to published reports, he had a history of white supremacy behavior. There is no indication that he had any monetary goal in the attacks.

Opportunity

While the attacks on some of the Philly and newspaper reporter victims appeared planned, many of the attacks appear to be random.

Reconnaissance For his attacks Carlson needed the e-mail address of his victims, who often had very public e-mail addresses. He also obtained his list of e-mail addresses from unsecured networks of high schools and college alumni websites. These lists contained many invalid e-mail addresses as they were often out-of-date which resulted in bounced e-mail when he used them as recipient address.

Knowledge Carlson admitted to having initiated the direct e-mail attacks. But he denied that he intended to execute indirect attacks. He claimed that he did not consider the result of using outdated e-mail lists for recipients of e-mail will result in a massive amount of e-mail being sent to the sender e-mail's address.

Means The means of this attack was denial of service.

Skills **T**he news reports indicate that he sent the e-mails from unsecured computers. This was probably because he used the relay feature of SMTP e-mail to send e-mail from SMTP servers that had no restriction on forwarding e-mail. These kinds of attacks are relatively simple to accomplish

Security Posture - Software Vulnerabilities The ability to attack e-mail in such a fashion is a very well-known vulnerability of e-mail. It is due to the feature that e-mail is accepted from any address and that there is no feature to verify the authenticity of the sender.

Defender's Capabilities - Tools The defenders should have used anti-spam tools to stop unwanted spam. This incident took place in 2001-2002, before these tools were in widespread use. Without these tools susceptibility to such attacks is great as spam e-mail can exceed 90% of e-mail passing through the Internet.

Digitally signing of e-mail will prevent spoofed sender e-mail from being accepted, but it is difficult to implement as it requires corporation of all senders of e-mail.

Deterrence

Formal Sanctions are being attempted to stop these kinds of spam attacks. In this case a 48 month imprisonment, three years of supervised release, restitution of $14,970.63, and a fine of $7,900.00 were imposed. The formal punishments were the prison service and the fine, imposed to deter such attacks.

Futility Futility can be achieved by lowering the amount of spam attacks by increasing the protective mechanism with wide use of anti-spam programs, which stop and mitigate the effects of span attacks, and thereby discourage the attackers from attempting to attack. See [10]**.**

What If Had the defenders used anti-spam software, which at the time of the attack was beginning to be available; the effects of the attacks would have been mitigated. Had the public sources better protected their e-mail lists, which are considered personal information, the attacker would have been prevented from attacking. Both these issues can be addressed by a comprehensive security policy.

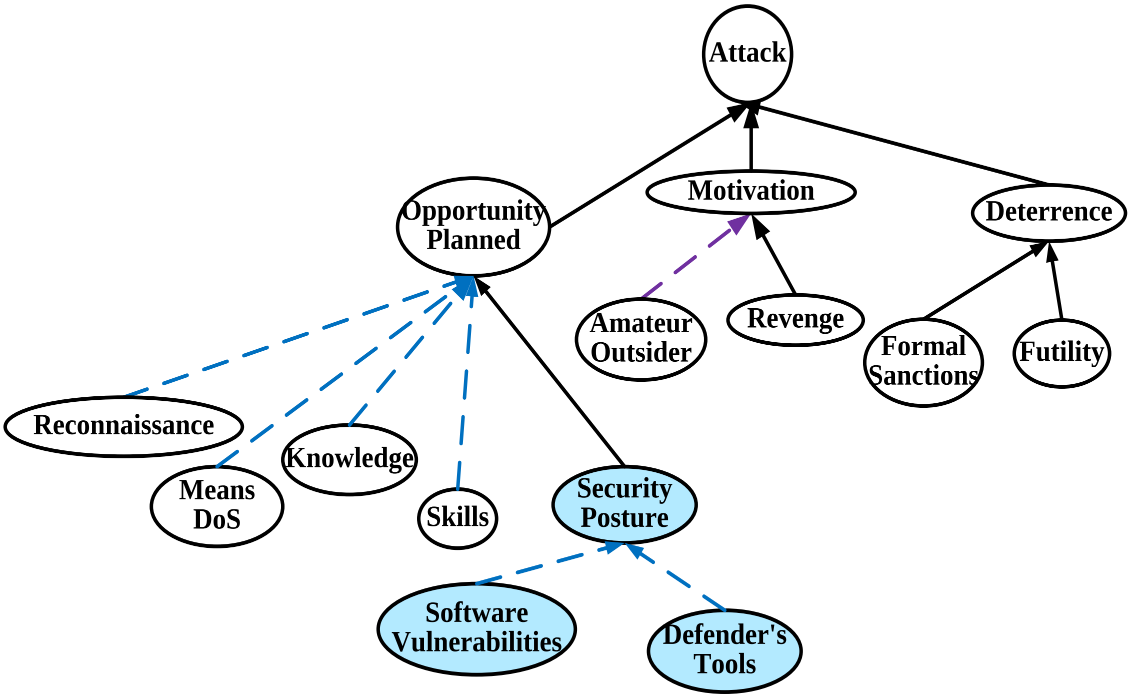


Figure 28: Carlson E-Mail Spam Attacks

5.6 Gonzalez Credit Card Fraud

Albert Gonzales was convicted for major credit card crime thefts, profiting massively from their sale and fraudulent usage. This was a major cyber-crime episode, with extensive court proceedings and media coverage, and warrants the treatment that follows [11], [12, 13].

Summary of Gonzalez' Crimes

Albert Gonzalez' first significant computer crime was his involvement with ShadowCrew message board forum. ShadowCrew was a website and forum that allowed cybercriminals to exchange ideas and information on computer targets and methods to compromise systems. Even more sinister, this forum promoted a market for buying and selling personal data that hackers had obtained about their victims. A prosecutor described the ShadowCrew as "an eBay, Monster.com and MySpace for computer crime". This website operated between 2002 and 2004. It was closed by federal law enforcement, and most of its key figures were arrested. Gonzalez was a major figure in ShadowCrew. He was confronted by the Secret Service in 2003 for his role on that site, and agreed to serve as an informer to avoid arrest.

Gonzalez was one of the best informers the Secret Service ever had for cybercrime. Not only was Gonzalez instrumental in capturing the members of ShadowCrew, but he continued working with the Secret Service to break up numerous other cybercrime rings and to arrest their members.

Nevertheless, while working for the Secret Service Gonzalez explored and exploited vulnerabilities in corporate wireless (Wi-Fi) networks. He used a technique called "wardriving" where he and his cohorts would operate with laptops and high power antennas in the parking lots of large retails stores. He easily was able to gain access to corporate networks because of weak or no security on their Wi-Fi networks. With access to a network they were able to view its credit card transactions. Using these methods Gonzalez was able early on to capture almost a million and half credit card information records.

During the summer of 2003 Gonzalez was able to gain full access to the corporate computers of Marshall's parent company TJMaxx. Using a sniffer program he was able to glean 40 million credit card information records.

In the spring of 2007, about the time that he quit working for the Secret Service, he began planning and executing the largest ever credit card fraud. Using a method called SQL injection he was able to compromise the database servers of Heartland Payment System one of the largest clearing houses for credit card payments. Gonzalez was then able to access 130 million credit card records.

Gonzalez worked closely with “fences” - people who buy and sell stolen goods - in Europe and Asia in order to sell his great horde of credit card records. It was through one of these “fences” that Gonzalez was identified, and arrested on May 7, 2008.

Three separate legal proceedings were brought against Gonzalez. They were combined and he was sentenced to two 20-year jail terms running concurrently. The following are digests of these three legal proceedings.

New Jersey District Court, case number 1:09-cr-00626 [14] **.** According to this indictment, Albert Gonzalez used SQL Injection attacks between October 2006 and May 2008 to gain access to database servers used to process credit and debit cards for Heartland Payment System; HPS is one of the world’s largest credit and debit systems. He gained access to 130 million credit and debit cards. He also, participated in similar attacks against credit and debit cards processing for 7-Eleven, Hanaford Brothers, and two unnamed companies.

Once he and his associates had compromised the servers these hackers would install unique malware to create a backdoor to allow them to access the servers at a later date.

They also installed sniffer programs to capture the credit card information and write it to files and then periodically transmit the information to the hackers. They stored the information and the malware that they used for the attacks on servers throughout the world that they leased under false names. To further hide the existence of the servers used as hacker platforms, they used proxies to disguise their true Internet Protocol addresses. Also, the malware installed on the victims' computers was programmed to erase the computers in order not to leave any evidence.

Eastern District of New York Federal Court, case number 2:08-cr-00160 [15]**.** This indictment, which does not mention Gonzalez by name, is for the alleged crimes committed between May and August of 2007 that Gonzalez and others conspired to steal credit card information from Point of Sale (POS) from Dave & Busters, Inc., a restaurant chain. The hackers used false representation to indicate that they were authorized to gain access to the servers that were located at the restaurants that controlled the POS.

Once they gained access to the servers the hackers installed a sniffer program to capture the credit card information and later send it to the hackers' servers. However, a bug in the sniffer's program required the sniffer to be reactivated when the server was rebooted. This required return of the hacker was one of the identified actions that caused Gonzalez to be caught, and was subsequently arrested.

Massachusetts case number 1:08-cr-10223 [16]**.** According to this indictment, between 2003 and 2008 Gonzalez and others downloaded and stole 40 million credit cards information by exploiting weakness in the wireless networks used by TJ Maxx, Bj's

Wholesales, DSW, OfficeMax and other retailers. As in the other cases the information was sent to servers all over the world and sold to others. In some instances the hackers encoded the credit card information onto cards and used them to withdraw money from ATM machines. As in the other cases the hackers used sniffer programs to capture credit card information from compromised systems.

What made Gonzalez offenses even more grievous was that between August 2002 and October 2004 Gonzalez was accused of participating with a group of hackers for *trafficking* 1.5 million credit and ATM cards numbers. He had cooperated with the Secret Service, in return in return for not being indicted. He used his association with the Secret Service to warn his fellow hackers and to aid his own crimes.

At the end of 2009 the cases in New Jersey and Eastern New York were combined with the case in Massachusetts. Gonzalez pleaded guilty to all counts against him, and showed remorse for embarrassing his family. As noted above, he was given two 20-year sentences that run concurrently.

This case, as the others, is presented as an adaptation of the general influence model in Figure 29, which is preceded by discussions of the facts and issues pertaining to its nodes; they include more details of the indictments. The relative strengths of some factors - nodes - and their relationships can be understood from the information associated with the various facts.

5.6.1 Nodes and Model

Motivation

Professional The prosecution described Gonzalez as a high end criminal, "…elite international carders and hackers, moving seamlessly across international borders, sharing attack tools, helping each other to build the attack, providing each other assistance….".

Outsider Gonzalez was an outsider. Gonzalez' motivation for launching his attacks changed as his crime spree progressed.

Challenge Initially when Gonzalez was a high school student his goal was challenge, as he said in an interview by the online magazine ZDNet that he gave anonymously under his screen name, soupnaz, "Defacing a site to me is showing the admin [and] government … that go to the site that we own them", cited in [12].

After Gonzalez had initially accumulated a huge fortune he still continued his hacking spree. In his own words, "I wanted to quit but I couldn't". He also liked stealing as he also said, "Whatever morality I should have been feeling was trumped by the thrill" [12].

Monetary This was Gonzalez' primary goal. He was highly motivated as is evident from the monetary fortunes he accumulated, his opulent lifestyle, his drug addiction; and he was encouraged by being well versed in computer hacking (all noted in the indictments and sentencing). For example, Gonzalez accumulated great fortunes through his criminal activity that paid for luxuries like cars and a $75,000.00 birthday party, and also for his drug addiction.

Opportunity

Planned His very methodology consisted of well-planned attacks.

Reconnaissance He initially found his targets randomly by using “wardriving”, i.e. driving around with a notebook computer and a wireless adapter looking for unsecure networks.

Skills The judge stated at Gonzalez’ sentencing that he had “technological prowess”, “gifts”, and “skills”, which were all used to perform the above mentioned crime.

Gonzalez’ skills included leadership to secure cooperation of others in executing his attacks. Even in high school, he was “a *troubled* pack leader of computer nerds at South Miami Senior High School in Miami, former teacher said..” [17]. He was cited by the FBI for using the high school’s library to hack into the Indian government’s servers, and left offensive messages [18].

The indictments and sentencing show that he effectively led groups of people located in the US and abroad, successfully achieving “to commit and assist Shadowcrew members (numbering about 4,000)…electronic theft of personal identifying information, credit card and debit card fraud and the production and sale of false identification documents.”

He used his network of friends very efficiently as stated in the New Jersey indictment "…would communicate via instant messaging services while the unauthorized access by them was taking place in order to advise each other as to how to navigate the Corporate Victims' networks and how to locate credit and debit card numbers and corresponding Card Data".

Gonzalez' ability to move money through various countries required the cooperation and organization of many people to accomplish this seamlessly, as mentioned in the Massachusetts indictment, "Moved money through anonymous web currency exchanges and bank accounts in Latvia to conceal the illegal proceeds".

On the other hand it seems as though Gonzalez was a difficult person to work for, as Stephan Watt, who worked for Gonzalez to write code used to steal credit cards, complained that he was not paid for his work ([17].

Effort Gonzalez was essentially solely involved in this activity. He was "…obsessively dealing with the technology…". This is from the sentencing judge.

Time Bound Gonzalez, and associates, could access his targets only within specific time windows, only between reboots of certain victims' servers (and had to reactivate attack sniffers, which led to detection), and only when he gained physical access to certain victims' systems.

T**ools and Knowledge** He had groups of partners who contributed to his capabilities. He was in contact with hackers from all over the world. When he had difficulty decrypting Office Maxx's cards he was able to use his network of friends from outside the country to do so (according to the prosecutor during the sentencing phase).

- He and his associates developed unique tools to use SQL injection to gain control of servers.
- He also developed software known as sniffers which allowed him and his fellow hackers to monitor the compromised servers, and record all their credit card information.
- They also leased servers throughout the world that were known as "hacker's platforms" where they stored the malicious code, and then launch it to affect servers that they had identified. These "hacker's platforms" also received the files which contained the stolen credit card information. Many of these platforms were outside the United States, which made it difficult for US law enforcement to detect and track (New Jersey indictment).

He had physical contact with the other hackers. One of them was his roommate, and the crime took on a more traditional gang crime characteristic. Likewise, he had physical contact with servers that were attacked, e.g. in the case of the D&B restaurant chain intrusion.

In the other crimes, such as noted in the New Jersey indictment (Heartland Payment System), the crime was committed over the Internet.

He used encryption effectively to avoid detection.

Means The attacks were primarily a disclosure of data, as they did not modify any data on the retailers' and credit card clearing houses' databases and communication systems that Gonzalez attacked.

Security Posture

Vulnerabilities The security posture of the retailers' systems that Gonzalez and his fellow hackers attacked was weak. TJ Maxx sent credit card information on wireless networks that were not sufficiently secure. These wireless networks were encrypting the data using the WEP protocol, which has many known deficiencies, vulnerabilities; the much more secure WPA protocol was available, but not used [13].

A routine audit of TJ Maxx security found that in addition to using the unsecure WEP wireless security, the firm was missing software patches and firewalls. The auditors further stated "that it wasn't complying with many of the requirements imposed by Visa and MasterCard"

It was a second audit performed two months after the above routine audit that "another auditor found anomalies in the company's card data. At that point, TJ Maxx hired forensics experts from International Business Machines Corp. and General Dynamics

Corp., and notified the U.S. Secret Service, which spent a month trying to catch the hackers in the act".

"It took the company more than two years to even realize that they were hacked!" [13].

Security Policy Many of the attacks noted in the New Jersey Indictment were made by SQL injection; tighter standards of programming policy and procedures would have made the credit card companies' code much less susceptible to this form of attacks. Additionally, regarding all the attacks that involved compromising a server and loading unique software like sniffers and backdoors could have been mitigated or prevented by using tighter security practices and monitoring, which can detect onslaught of foreign programs on servers.

In the absence of the credit card companies' internal investigation information it is difficult to know their security policies, and then ascertain how well they were implemented, and their relevant security culture. Also it is difficult for large retailers like TJ Maxx, 7-11 and others to enforce policy since they have many stores, and many are franchises. However, there is the Payments Card Industry Security Standards Council (PCI-SSC) [19], which offers standards on how to protect POS systems that greatly improve security from the very weaknesses that Gonzalez exploited.

Deterrence

Morality Gonzalez' participants did not know each other. The prosecutor in the sentencing phase stated that the criminal participants were not worried about "honor among thieves, because what they are using as basis of communication is a nickname that is often nearly untraceable, the cover of the anonymity of the Internet".

Religion and **philosophy** were not factors in his activities and motivation.

Shame He was knowingly removed from the pain he inflicted on victims and therefore lacked shame, his only consideration was to successfully carry out his attacks. From the sentencing judge, "Now I find that people with your gifts sometimes find themselves obsessively dealing with the technology in a way that is asocial and frequently becomes anti-social without adequate consideration to who is being harmed and who can be harmed."

Swiftness, Severity and Certainty When he was first caught (in the criminal investigation of his Shadowcrew scheme) he received what can be termed as a severe social punishment. He agreed to become an informer for the Secret Service to avoid being indicted, ostracizing himself from his friends. This did not deter Gonzalez from continuing criminal activity. While he actually turned on his fellow hackers, he also found "new friends". He may have been aware of an "ultimately severe" punishment - such as 20 years imprisonment that was finally imposed - but that did not deter him.

Formal Punishment Gonzalez was sentenced to a very long prison term, 20 years, which the sentencing judge said "is warehousing, to keep you from doing this crime again". This form of deterrence totally removes the opportunity from committing a crime. The judge stated that through the lengthy prison term "warehousing and also impressing upon you the seriousness of what you have done, and that gets you habituated to the idea you should not do stuff like this". This is based on a more traditional approach to deterrence, to discourage some from a particular behavior. However, the judge did take to heart the feelings of remorse expressed by Gonzalez, the difficulties he experienced while growing up and his relatively young age, and imposed a more lenient punishment than the plea agreement required, giving him a chance to be released by his early 40's.

What If Had the retailers used secure Wifi communication which was available and recommended at the time that these attacks took place, it likely that Gonzalez would have not attacked these targets. Furthermore had Gonzalez been punished swiftly and with certainty for his earlier criminal behavior, according to Gonzalez he would have not continued to commit ever bigger crimes.

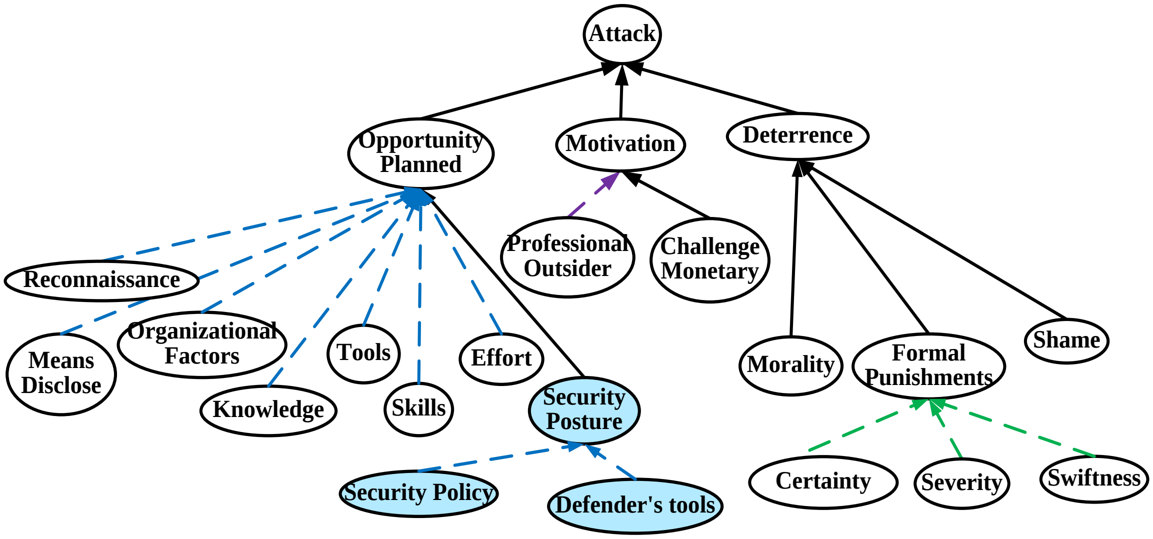


Figure 29: Gonzalez Credit Card Fraud

5.7 Shea Time Bomb Attack

William Carl Shea was found guilty, on circumstantial evidence, of corrupting 50,000 debit and credit records of the database of BACS (Bay Area Credit Services, the name indicates its function) by a "time bomb attack", a program that he designed to attack at a specific time. He had worked as a programmer for this company from August 6, 2001 until January 17, 2003 when he was dismissed. That "time bomb" attack occurred on January 29, 2003, two weeks after he was dismissed. From his unsuccessful appeal nodes for the model were identified as applicable to this case and understood [20].

This case is presented as an adaptation of the general influence model in Figure 30, which is preceded by discussions of the facts and issues pertaining to its nodes. The relative strengths of some factors - nodes - and their relationships can be understood from the information associated with the various facts.

5.7.1 Nodes and Model

Motivation

Insider The identified attacker, William Carl Shea, is classified as an insider because he was a programmer understanding the BACS system, and having full access to it.

Revenge He was motivated by revenge because he was dismissed from his job. He actually stated that people in the company were “out to get him”.

Opportunity

Planned Attack The attack was planned against a specific company and a specific database. The randomness of the attack was only with respect to the records which were corrupted.

Reconnaissance It was not necessary for him to do much or, perhaps, any reconnaissance prior to the attack because of his familiarity with the system.

Knowledge His knowledge of the system was considerable. He was well versed in all of its aspects. He had strengths in all of the programming languages used in the system. The prosecution proved that only he could have written the “time bomb attack” program as it was in in the language called Pick, with which he was familiar, but not the other programmers.

Tools He had sufficient attack tools to complete the program. It did not appear that he used any special reconnaissance tools. The fact that the record of program changes was incomplete could imply that he used some form of stealth to hide the changes he made or to alter the log of the changes.

Means The means of this attack was destruction of information.

Skills He displayed skill in the designing and execution of the "time bomb attack" program. But, that program was flawed as it ran multiple simultaneous sessions which caused it to "hang" when it exhausted the system resources.

Security Posture There were a number of weaknesses in the security posture that are evident from the defender's capabilities security policy.

Defender's Capabilities Security Policy The security policy was weak because the programmers were allowed root access, with the ability to change users without a password. Therefore, there was no real assurance that the user name associated with a security audit was the real user. There was no mention of separation of duties which could be used to prevent this kind of attack.

Security Culture From the above mentioned issue it would follow that the company as a whole did not have a strong security culture

Individual Factors Individual factors inserted here as it, in this case, significantly parallels the defender's human errors node. The identified attacker, Shea, apparently did have some family and health problems.

Defender's Tools There is little mention of defender's tools, but the fact that the logs that were not totally complete would indicate that logging was not well maintained. The backups and recovery seemed to be adequate, although it took two months to fully recover from the corrupted data.

Deterrence

Shea's attack and approach to launching it apparently did not consider any deterrence issues other than the futility factor. It should be noted that the revenge motivation was so powerful in Shea's case that it superseded all other deterrence factors due to the fact that he preplanned his attack before he was dismissed.

Futility He expected his "time bomb" to be entirely successful, fulfilling his revenge goal. He had hoped that his program would systematically corrupt all the records in the database. Instead the program hung after reaching 40,000 records, which he admitted subsequently to that possibility. Furthermore he assumed that the corrupted data will not be repairable. However, the company that designed the database was able to restore all the data without loss, albeit only after a few months.

What If Had the defenders organization had strong separation of duties policy in place, a programmer would not have been given root access. This would have prevented Shea from performing this kind of attack.

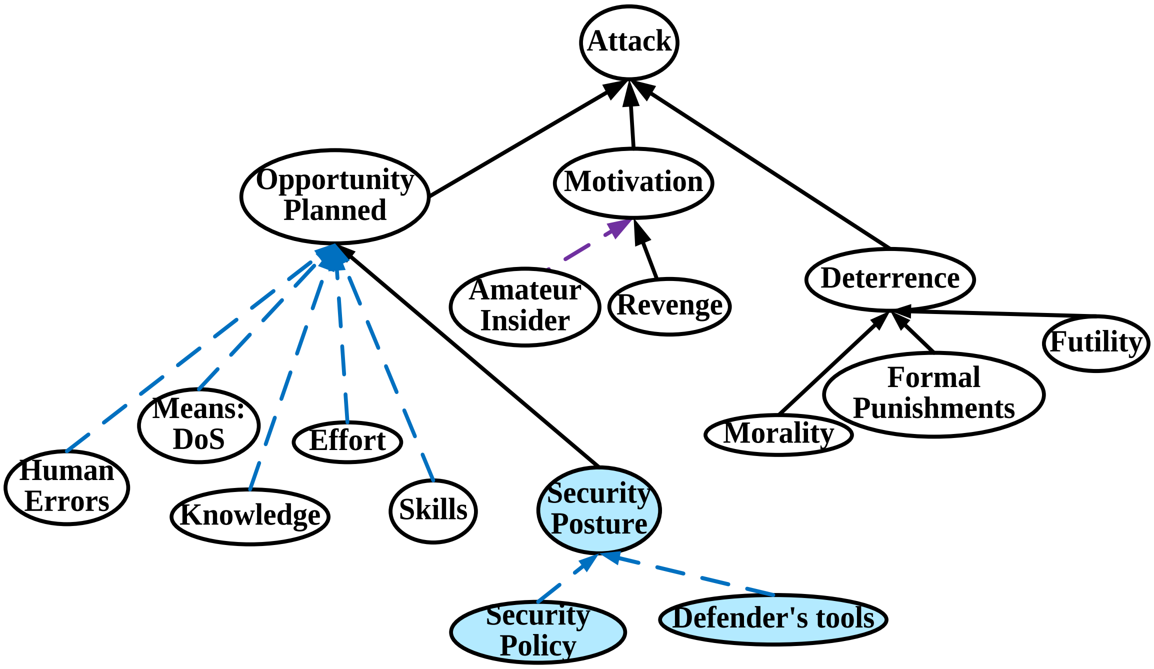


Figure 30: Shea Time Bomb Attack

5.8 Getloaded Website Piracy

Creative Computing (Creative) created a successful Internet site called truckstop.com that matched loads with trucks to help maximize trucker capacity to haul loads and satisfying shippers' needs. Getloaded, competing with Creative, performed the following illegal acts according to their unsuccessful appeal [21]:

1. Getloaded accessed unauthorizedly the trckstop.com site to obtain information about available loads by:
    a. Impersonating legitimate users, and by
    b. Registering a defunct trucking company as a legitimate operating company.
2. Its officers exploited vulnerability in the unpatched Creative's web server for access to the truckstop.com code and its proprietary "radius search" feature, which Getloaded incorporated into their own software.
3. Getloaded engaged a Creative employee to download its customer list.

Creative sued, and received a temporary restraining order against Getloaded. Subsequently, Getloaded violated the terms of the injunction. The Court expressed its finding as: "Getloaded acted in bad faith as its senior management -- and others under its supervision and with its knowledge -- lied under oath and violated the Court's injunction".

A jury found Getloaded guilty of violating the Federal Computer Fraud Abuse Act. Creative was awarded $510,000 in damages, and an additional $120,000 in exemplary damages due to Getloaded's "willful and malicious conduct".

This case is presented as an adaptation of the general influence model in Figure 31, which is preceded by discussions of the facts and issues pertaining to its nodes. The relative strengths of some factors – nodes - and their relationships can be understood from the information associated with the various facts.

5.8.1 Nodes and Model

Motivation

Financial Gain The motivation for this attack was financial gain in Getloaded's competing dishonestly with Creative Computing. In the words of the Appeals Judge, "Getloaded decided to compete, but not honestly …..it wanted to get a bigger piece of Creative's market".

Outsider and Insider The overall unauthorized usage of the truckstop.com site was by outsiders, Getloaded employees; the actual hacking into the truckstop.com website was by Getloaded officers. The downloading of the Creative customer list was by an insider, a Creative employee. This employee did join Getloaded, but Creative "found evidence that he improperly accessed customer information before his departure".

Amateur The various attacks were by amateurs. The unauthorized usage attacks and exploit of vulnerability were by computer unsophisticated Getloaded personnel, without resorting to professional criminal hackers. Also, the gathering of the customer list by the former Creative employee was sloppy, as the Statement of Facts declares: "found evidence that he (former Creative employee) improperly accessed customer information before his departure". A professional attacker would not have left behind such evidence.

Opportunity

Planned Attacks The attacks were planned attacks against a specific target.

Reconnaissance and **Tools** There is no information on reconnaissance or special tools used to perform the attacks.

Knowledge and Skills The attackers appeared to possess sufficient knowledge and skills to successfully carry out their attacks. It took a number of years until the defender/ victim, Creative, realized that they were being attacked.

They displayed teamwork. The officers of Getloaded encouraged perpetrating the crime, leading by example, as they were the ones who hacked Creative's servers.

Time Bound The attacks took several years to be discovered. This was only after Getloaded released a version of their software that was very similar to that of Creative Computing.

Means The attacks were data disclosure attacks to gain access to code and customer lists of the defender.

Defender's Security Policy The defender should have installed the available patch from Microsoft that would have prevented Getloaded from hacking into their system. In fact Getloaded claimed in their appeal that Creative was at fault for their attack because they did not practice due diligence. The judge rejected their argument.

Deterrence

Futility However, an element of futility by the attacker is detected, as Getloaded apparently did not use the stolen code in their own product. For this reason Creative Computing could not prevail over Getloaded in a copyright infringement lawsuit.

Consequences Because of the fear of consequences it is likely that Getloaded did not use the stolen code in their own product. Additionally, after being subjected to a court ordered injunction Getloaded removed or destroyed evidence of: (a) how they had, copied and used truckstop.com's source code, (b) how they stole Creative's customer list, and (c) how they accessed the truckstop.com site.

Although it was obvious that Getloaded had committed malicious crime, prosecution prevailed only according to the Federal statute, the Computer Fraud and Abuse Act. A limitation to consequences consideration is indicated because a case could not be proved under copyright infringement laws, namely the Lanham Act, and Idaho Trade Secrets Act.

Morality Getloaded displayed a great lack of morality throughout the entire episode. They brazenly stole trade secrets and a customer list, and later ignored a Court ordered injunction. Officers of that company assumed a leadership in committing the crimes. Moreover, customers did not display moral concern about Getloaded, but continue to use that site.

What If If the defender would have had a security policy that required prompt installation of recommended security patches, Getloaded would have not been able to obtain the code from Creative. Also, if Creative had a formal separation from employment policy in place, it is likely that the former worker would have been prevented from taking the customer list with him.

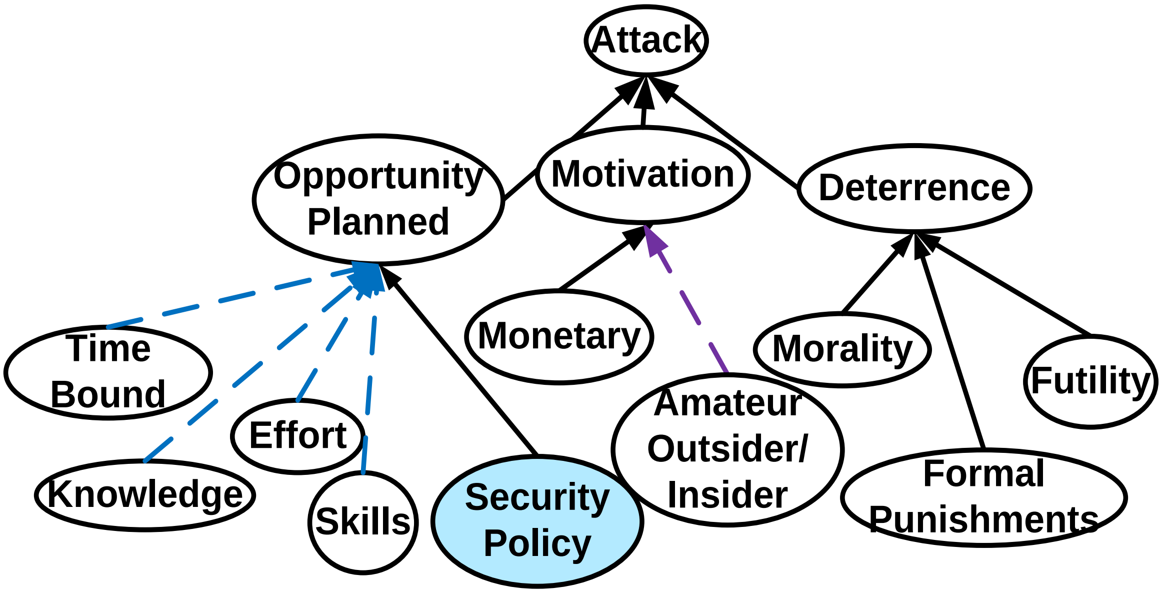


Figure 31: Getloaded Website Piracy

5.9 Manning - WikiLeaks

US Army Private First Class Bradley E. Manning is alleged to passing almost 500,000 classified documents with political, diplomatic and military content to WikiLeaks' founder Julian Assange during the six month period between November 19, 2009 and May 27, 2010. These came from Iraq where he served as an intelligence analyst. He was arraigned on February 23, 2012, and will be tried under the Uniformed Code of Military

Justice (USMJ). As opposed to all the other cases presented here there is no legal "statement of fact", as this case has not yet been prosecuted. Also, since that case is to be prosecuted under USMJ there will be less transparency than what is typical under civilian prosecutions. Information presented here about Manning, his person and alleged actions, and surrounding circumstances are essentially from press reports as of the second half of 2012 [22, 23], [24], [25].

Manning was granted a high security level clearance although he was known to suffer from a number of psychological problems. He should have lost his clearance in May 2009 for overturning a table, and for trying to grab a gun in December 2009. In the May 2010 he assaulted a fellow intelligence analyst.

There is more regarding the victim/US Army, i.e. security, shortcomings. It was quite easy for him to copy sensitive information because the computer security at the facility was very lax. The passwords to secure computers were left on Post-it notes stuck on terminals. There was no system in place for checking for the removal of classified information from the building. It was a common practice for analysts to store music and movies on secure intelligence computers. An officer stated at a preliminary hearing that she was not even aware that it was wrong to store such personal files on secure computers.

Manning spelled out his motivations for committing this crime in a letter that accompanied some of the data he sent to WikiLeaks. It included: "This is possibly one of the more significant documents of our time, removing the fog of war and revealing the true nature of 21st century asymmetric warfare."

He was “politically” motivated, and his goals were in his mind more important than his duty. He apparently had no moral problem with his actions, and was not afraid of Formal Sanctions. He bragged in a letter to a mathematician named Eric Schmiedl, "I was the source of the 12 Jul 07 video from the Apache Weapons Team which killed two journalists and injured two kids".

This case is presented as an adaptation of the general influence model in Figure 32, which is preceded by discussions of the facts and issues pertaining to its nodes. The relative strengths of some factors - nodes - and their relationships can be understood from the information associated with the various facts.

5.9.1 Nodes and Model

Motivation

Non-Monetary As noted above, Manning’s alleged motivation was non-monetary, political. Available information indicates that his motivation did not include financial gain. Wired Magazine, July 13, 2011, published logs of chats between Manning and Adrian Lamo, which included a Manning’s explanation for disclosing that data, “..because it is public data, it belongs in the public domain information and should be free..”. Lamo was a former hacker with whom Manning conversed starting May 21, 2009, and who subsequently reported Manning.

Insider Manning was an insider who was able to use his secure computer accessibility to allegedly disclose some 500,000 documents.

Amateur Manning does not appear to have had any special training in computer hacking. He took only a few precautions to encrypt his communications to cover his tracks. The investigation found an SD card with unencrypted files from Afghan and Iraq war logs, together with a message to WikiLeaks. He did claim that he deleted the hard drive from his computer, but he actually never completed that process, and its files were recovered [26].

Opportunity

Random Attacks Manning's attacks were random. Even his first scoop, which was the 2007 video of a helicopter attack, was discovered by accident.

Tools Manning used few special tools for his attacks. He copied files to an SD card to avoid detection because of its smallness. He used secure communication (SSH and STP) when communicating with WikiLeaks founder Julian Assange. He used Wget, a free software program to download entire classified web sites [26]. Manning attempted to use a program to securely delete his hard drive by overwriting the data with zeros. He chose the least reliable option, of only overwriting the data only once, and therefore the investigators were able to recover the data. Here, was included a chat session Manning had with Wikileaks founder Assange where Manning asked for help in cracking NT LAN passwords using a "rainbow table" to crack the main password on a classified computer.

Knowledge and Skills Manning had the knowledge required for his job related computer systems and their security. He did not seem to be particularly careful in in attempting to cover his tracks. He was inconsistent in using encryption in his attacks, and always used the same password. The actual downloading that large amount of data did not require any special skills, having had such access, as he had bragged during a chat session. However, from the chat sessions with WikiLeaks' Assange, Manning seems to have worked well with Assange, who contributed advice to gathering and posting the data on WikiLeaks.

Effort and Time Manning put great effort into committing this attack during a 10-day period when he spent his entire 14 hour shifts gathering and downloading documents.

Time Bound Manning's available time for his attacks was limited to the six month period he served in Iraq, at the end of which he would lose his lose his security clearance. Therefore he devoted himself very intensely to his attacks, noting that he was completely preoccupied with his downloading during the entire 14 hour shifts over a period of ten days.

Means The attacks were disclosure of data attacks. They did not alter data nor affected the availability of computer services.

Security Posture As noted above, the US Army's cyber security in Iraq where Manning was located was inadequate. There were few controls, personnel placing passwords in open view. There were many security infractions that were prohibited by stated security policy, but personnel were even unaware of that policy. Manning in a chat session with Lamo wrote, "weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis ... a perfect storm".

In fact, the Army did log Manning's activity. These logs showed that Manning accessed the State Department's servers 794,000 times, downloading more than 250,000 diplomatic cables. Additionally, there was a minute-to-minute record of Manning's search of the Pentagon's classified intranet SIPRNet.

In addition to the disregard of security policy there were human errors contributing to that security failure. The staff in Manning's unit was working 14 hours day, seven days a week, in Manning's words: "people stopped caring after three weeks".

It should be reiterated that Manning was granted a high level of security clearance despite his known psychological problems.

Futility Futility did not seem to be a factor in this case as Manning proceeded with great ease to access confidential data, and to copy and send it to WikiLeaks.

Deterrence

Consequences and Morality Manning had psychological problems that might have made it difficult for him to understand the consequences of his actions. He did believe that he had destroyed the evidence of his downloading, and therefore would not be caught.

He also had deep convictions that his actions were correct. In the deterrence section Professors Paternoster and Simpson, Section 4.38.2 state that an essentially a high morality stance assumed by an attacker counteracts any deterrence/consequences considerations by the attacker. In fact, such "high morality" encourages the commission of the crime.

What If Had the U. S. Army enforced its own security policy these attacks would likely not have taken place. In fact, an officer at Manning's unit was unaware of the security policy. The failure of the enforcement of the security policy was partially due to a weak security culture, especially among units in the field.

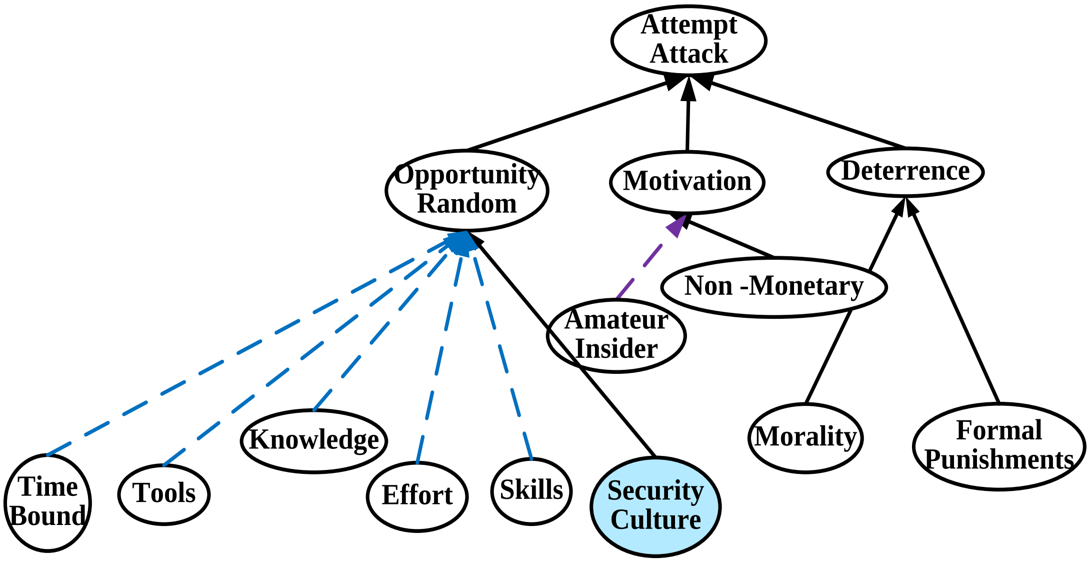


Figure 32: Manning-Wikileaks

5.10 Eight Cases, Bias Issue

The eight cases were particularly chosen because they were all except the Manning case tried under the Computer and Abuse Act of 1986. This law is one of the oldest computer crimes laws, and is considered by many as the most successful law under which cybercrimes have been tried, and therefore these cases represent real cybercriminal acts.

The following specific factors were noted in the Introduction to these eight cases studies that underscore their applicability to cybercrime in general.

- Case proceedings with a guilty verdict are a reliable information resource of the nature and circumstances of a crime, with a judge's opinion and understanding of a particular motivation based the "statement of facts".
- The findings in six of the eight cases were further reinforced by unsuccessful appeals.
- Three cases are of celebrity status, and therefore have extensive media coverage to augment the legal opinions.

The US Government has two primary annual crime measure reports. The Uniform Crime Reports from the Federal Bureau of Investigation (FBI) which is based on statistics from crimes reported to law enforcement agencies throughout the country. The other crime measure report is the National Crime Victimization Report from the Bureau of Justice Statistics which surveys crime victims and includes statistics from both reported and unreported crimes. Researchers have compared the statistics of both these reports and found bias between reported and non-reported crimes. (Zedlewski, 1982)[27], [28], [29].

Is there bias in these eight cases that their combined analyses and conclusions may not have wide applicability to cybercrime? The following paragraphs indicate the possibility of bias, considering the results of various surveys.

According to the Verizon Report, the CSI survey and the CSO Report most cyber-attacks are not reported. Often a victim is unaware that an attack has taken place, or a victim chooses to handle the attack internally; the latter may often be because negative press can impact customer trust. In fact, CSO reports that 72% of insider incidents are handled internally.

Some cyber-attacks that are reported to law enforcement are often not prosecuted because of the particular difficulty to prove culpability, or lack of sufficient evidence of damage to the victim.

All eight cases that are presented here were reported and prosecuted, seven successfully and one case is pending. All of the attacks were detected, and therefore the attacker was unsuccessful in concealing the attack. This can be due to lack of skills and knowledge, as opposed to many attackers who have not been caught. Furthermore, the victim(s) in all eight cases reported the attack to the authorities and did not attempt to handle the incident internally. The successful prosecutions demonstrate a strong willingness of both the legal authorities and the victims to pursue these particular cases. This may introduce biases regarding unique reasons for prosecuting these cases with respect to the many cases that were and are not prosecuted.

The following are some other possible bias issues.

- The motivations in five of the eight cases were for non-monetary goals, while according to the various surveys the majority of cyber-attacks are for monetary reasons.
- The eight cases ranged in degree of expertise of the attacker, from Gonzalez who had superb expertise to Carlson’s email spam attack that involved very little expertise.
- The primary victims of the attacks in four of the cases were for-profit corporations; the other four were non-profit organizations, three Universities and the US Government.

- All of the offenders in the eight cases were men. In five cases the offender's age was 25 or bellow.

These cited possible biases do not appear to play a role in the conclusions that cyber-attacks are generally simple, and that simple protections are generally effective. These findings are essentially the same as those of Verizon, where their ninety case studies included both reported and unreported attacks. The attacks were primarily for profit. The victims were from large, medium and small organizations.

5.11 Case Studies Conclusions

It is apparent that the facts of the eight cyber-crimes are directly translated to the nodes and sub-nodes of the general influence model, allowing a creditable model to be mapped for each case.

Addressing these models, it can be seen that they represent a very diverse group of attackers and targets. Table 1 highlights some of the most significant nodes with respect to the eight cases. Six of the cases dealt essentially with simple attacks where had the victims used standard security practices their systems would have been either fully protected, or the effects of the attacks would have been greatly mitigated according to the What Ifs. Even the Morris attack, which can be considered a sophisticated attack, against the Internet, could have been mitigated had the system administrators applied an available patch. While Gonzalez' credit card attacks were sophisticated, he did choose targets that were not practicing easily available security thereby amplifying his "success".

The issue is raised about simple attacks in cyber-crime, and consequential simple means of protection.

Table 1: Brief Summary of Eight Case Studies

Case	Attacker	Insider/ Outsider	Goal	Knowledge	Planned/ Random	Means
Morris	Amateur	Outsider	Challenge	High	Random	Denial of Service
Barrington	Amateur	Outsider	Monetary [7]	Medium	Planned	Alter Data
Phillips	Amateur	Outsider	Challenge	Low	Random	Disclosure of Data
Getloaded	Amateur	Insider[8]	Monetary	Med/High	Planned	Disclosure of Data
Shea	Amateur	Insider	Revenge	High	Planned	Destructio n of Data
Carlson	Amateur	Outsider	Revenge	Medium	Planned	Denial of Service
Manning	Amateur	Insider	Political	Medium	Random	Disclosure of Data
Gonzalez	Professional	Outsider	Monetary[9]	High	Planned	Disclosure of Data

[7] Monetary and Non-monetary
[8] Insider and Outsider
[9] Monetary and Challenge

5.12 References

[1] *18 USC § 1030 - Fraud and Related Activity in Connection with Computers*, 2013.

[2] *United States of America, Appellee, v. Robert Tappan Morris, Defendant-Appellant*, 1991, No. 90-1336, United States Court of Appeals, Second Circuit.

[3] *Christopher Andrew Phillips, Petitioner, v. United States of America*, 2007, No. 06-1602., Supreme Court of the United States.

[4] Contreras, G., September 7, 2005, "Ex-Student Sentenced in UT Computer Hacking," San Antonio Express-News, Metro and State News, p. 2B.

[5] Haurwitz, R., April 6, 2003, "Audits Turn Up Shortcomings in Computer Security at UT," Austin American-Statesman (Texas), Metro/State, p. B1.

[6] Brock, R., March 21, 2003, "Hackers Steal Data from U. of Texas Database," The Chronicle of Higher Education, Information Technology, p. 35.

[7] Kreytak, S., June 11, 2005, "Mixed Verdict for UT Hacker; Ex-Student Acquitted of Gravest Charges, Convicted of Taking Data from Network," Austin American-Statesman (Texas), METRO/STATE, p. B1.

[8] *United States of America, Plaintiff-Appellee, v. Marcus Barrington, Defendant-Appellant*, 2011, No. 09-15295, United States Court of Appeals for the Eleventh Circuit.

[9] *United States of America, Appellee, v. Allan Carlson, Appellant*, 2006, No. 05-3562, United States Court of Appeals for the Third Circuit.

[10] Cisco Security, 2011, "Email Attacks: This Time it's Personal," from http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf.

[11] *United States of America v. Albert Gonzalez*, 2010, No. 1:09-cr-10382-DPW-1, United States District Court, District of Massachusetts.

[12] Verini, J., Nov 14, 2010, "The Hacker Who Went into the Cold," New York Times Magazine, pp. 44.

[13] Pereira, J., May 4, 2007, "Breaking the Code: How Credit-Card Data Went Out Wireless Door; in Biggest Known Theft, Retailer's Weak Security Lost Millions of Number," The Wall Street Journal, p. A1.

[14] *United States of America V. Albert Gonzalez, Hacker 1, and Hacker 2*, 2009, 1:09-cr-00626, United States District Court, District of New Jersey.

[15] *United States of America V. Maksym Yastremskiy, Aleksandr Suvorov, Defendents,* 2008, 2:08-cr-00160, United States District Court, Eastern District of New York.

[16] *United States v. Gonzalez,* 2009, No. 08-10223-PBS, United States District Court for the District of Massachusetts.

[17] Gordon Meek, J., and Siemaszko, C., August 19, 2009, "Soupnazi Hacker Went from Nerdy Past to Life of Sex, Guns," Daily News, News, p. 18.

[18] "Mega-Hack Accused 'Nerd' Lived Large," August 21, 2009, The New Zealand Herald, Technology.

[19] 2013, "Official PCI Security Standards Council Site," from https://www.pcisecuritystandards.org/.

[20] *United States of America, Plaintiff-Appellee, v. William Carl Shea, Defendant-Appellant,* 2007, No. 06-10450, United States Court of Appeals, Ninth Circuit.

[21] *Creative Computing, dba Internet Truckstop.com, Plaintiff-Appellee, v. Getloaded.com LLC, and/or Codified Corporation, Defendant-Appellant, and Jack C. Martin, Defendant,* 2004, No. 02-35856, United States Court of Appeals, Ninth Circuit.

[22] "(Unofficial) Transcript of Bradley Manning's Arraignment at Fort Meade, MD ," February 23, 2012, WL Central.

[23] Dishneau, D., December 20, 2011, "Alleged Leaker Case More Tech than Military," The Associated Press.

[24] Dishneau, D., and Jelinek , P., December 19, 2011, "Witness: Manning Said Leak would Lift 'Fog of War'," Associated Press.

[25] Zetter, K., December 19, 2011, "
Jolt in WikiLeaks Case: Feds found Manning-Assange Chat Logs on Laptop," Wired.Com.

[26] Zetter, K., December 22, 2011, "Army Piles on Evidence in Final Arguments in WikiLeaks Hearing," Wired.Com.

[27] Zedlewski, E. W., 1983, "Deterrence Findings and Data Sources: A Comparison of the Uniform Crime Reports and the National Crime Surveys," Journal of Research in Crime and Delinquency**, (20) 2**, pp. 262-276.

[28] Kingsnorth, R. F., MacIntosh, R. C., and Wentworth, J., 1999, "Sexual Assault: The Role of Prior Relationship and Victim Characteristics in Case Processing," Justice Quarterly: JQ**, (16) 2**, pp. 275-302.

[29] Sheley, J.F., 1991, *Criminology: A Contemporary Handbook,* Wadsworth Pub. Co., Belmont, Calif.

6 Applications of the Model

6.1 Introduction

The model as presented in Chapter 4 will be used to further understand cyber-attacks and their nature as shown in the case studies, Chapter 5, and apply it to suggest effective means to protect specific systems. Protection entails preventing attacks, or, or mitigating their effects. So modeling a system and anticipated attacks based on its value to potential cybercriminals can point to weak attack paths or nodes that require strengthening.

However, it has been understood that most cyber-attacks are simple, and simple and easily available procedures may well offer protection. Simple protection may even help countering sophisticated attacks. These issues are dealt with in the following discussions. The importance of simple means of protection is first presented. Then, recognizing the parallelism of cyber-crime and white collar crime, the significance and implementation of moral deterrence will be discussed.

A high value and sophisticated system will obviously require special consideration; the issue of risk is an issue for high value systems protection implementation, and even for simple systems, and is discussed briefly at the end of the following chapter.

6.2 Simple Attacks and Simple Protection

Are information security attacks usually simple attacks that will not require elaborate protection defenses? Or, are the attacks usually sophisticated and require elaborate defenses. Or, can simple protection be also effective against sophisticated attacks?

The following discussion on crime, and specifically white collar crime, points to cyber-attacks generally being simple, not requiring elaborate protection. This issue is restricted to individual criminals acting on their own behalf, although corporate crime will be cited.

Simple cyber-attacks are usually random in nature, do not involve much planning, and are usually successful against systems whose operators do not follow best practices. Simple protection is often effective against sophisticated attacks. This was indicated in the above case studies, and cyber-attack surveys presented below.

6.2.1 White Collar Crime

Another way to look at the comparison of cyber-crime with typical crime is through the similarities of white collar crime to cyber-crime, 3.2.6 . Both occur with the attacker being remote from the victim, and for both the laws governing their legality are unclear. A difference between the two is that white collar crime, at least at the corporate level, is on behalf of a larger group, for the benefit of that group. Cyber-crime tends to occur for the individual criminal's benefit, although there exceptions such as politically motivated attacks. The individual attacker is the focus of this issue.

Gottfredson and Hirschi, 1990 [1], present a general theory of crime that is based on a low self-control trait that a general a criminal possesses, and that:

- Crimes usually "require little preparation", and
- "Skills required to complete the general run of crime are minimal".

They apply this theory to white collar crime, as surveys show that such criminals also have little self-control and desire quick and easy results.

One study that partially supports this approach to white collar crime is by Benson and Moore [2], 1992:256-57, who concluded from a study of over 2,400 convicted white collar criminals about 2,000 crime offenders that the evidence is mixed regarding the Low Self-Control theory of white collar crime, see 3.2.6. The white collar criminals lived quite conventionally and individually committed few crimes, unlike the other group. However, chronic offenders of both groups seemed similar.   White collar crime here entailed fraud, embezzlement and bribery; crime included narcotics, forgery and bank robbery.   Accordingly, Benson and Moore support applying the Low Self-Control accounting of white collar crime when it is chronically committed.

However, the Gottfredson and Hirschi [1] extension of this theory overall to white collar crime is challenged by a number of researchers. Geis and Salinger, 1995:101 [3], and Yeager and Reed [4], propose that corporate crime, essentially white collar crime, is better explained by organizational theory. The commission of corporate crime is directly related to the culture and aims of the corporation. They propose that white collar crime is unlike crime, that its motivation in a corporate setting is more linked to the environment of the corporation, to achieve corporate goals. Included in this theory is that corporate crime is a well thought out.

Simpson and Piquero in “Low Self-Control, Organizational Theory, and Corporate Crime”, 2002, question Benson and Moore that the crimes they studied do not meet the originally defined white collar crime by Edwin Sutherland [5] as "a crime committed by a person of respectability and high social status in the course of his occupation". Likewise, fraud and embezzlement often committed by unsophisticated and desperate individuals do not meet that criterion.

Using a restrictive definition of corporate crime, Braithwaite and Geis, p. 6 [6], define corporate crime as: "the conduct of a corporation or of employees acting on behalf of a company, which is proscribed and punishable by law".

Simpson and Piquero [7], portray the corporate criminal as a rational calculator, motivated for both his and the corporation's gain, but aware of the risks; unlike one who is impulsive, risk taking and short-sighted, according to Gottfredson and Hirschi [1]. This was based on a vignette survey of executive MBA students who were given realistic scenarios, and were asked about their likelihood to commit the given corporate crime. These students were sophisticated, had high self-control and some were in responsible positions.

With the above as background, cyber-crime committed by individuals on behalf of individuals would be characterized by originating from ones with low self-control, to those who are sophisticated and having a large degree of self-control, as in the case of corporate crime. Gottfredson and Hirschi claim simple attacks as consequential to low self-control. However, even cybercriminals who are well educated, very patient, and exhibit considerable self-control - similar to white collar/corporate criminals, Geis and Salinger, and Yeager and Reed - many of them will opt to use simple and random attacks. A cyber attacker has on hand the power to replicate a random and simple attack many times until a weakly defended target is found. This is especially true where the attacker's goal is monetary and therefore has many targets to choose from, as noted above regarding typical crime.

6.2.2 Case Studies: Eight Attacks

The case studies, with their "What Ifs", presented above, and experience learned from cyber security surveys, presented below, show that much cyber-attack damage could have been averted by use of very simple protection means.

Table 2 classifies the eight attacks according to their nature-random or targeted- and attacker and attack sophistication.

Table 2: Eight Case Studies - Attackers and Attacks

Case Study	Attacker	Knowledge	Targeted/ Random	Sophistication of Attack
Morris-Worm	Amateur	High	Random	High
Barrington – Grade Changing	Amateur	Medium	Targeted	Low
Phillips-Social Security Numbers	Amateur	Low	Random	Med
Getloaded- Website Piracy	Amateur	Med/High	Targeted	Low/Med
Shea- Time Bomb	Amateur	High	Targeted	Med
Carlson- E-mail Spam	Amateur	Medium	Targeted	Low
Manning- Wikileaks	Amateur	Medium	Random	Low
Gonzalez-Credit Card Fraud	Professional	High	Targeted	High

Five of these attacks were targeted and three are classified as random attacks. Of the eight attackers seven are classified as amateur and one is a professional. The knowledge level of the attacker does not necessarily correlate with the sophistication of the attack.

The only highly sophisticated attacks were the Morris worm, which at the time was considered to be the first computer worm, and the Gonzalez SQL injection attacks. In the case of the Morris worm lax security allowed Morris access to the networks against which he launched his attacks. In the case of Gonzalez the weak Wi-Fi security allowed easy access to the database servers that Gonzalez was then able to attack using SQL injection attacks.

Each of the Case Studies – eight attacks - concludes with a “What If” citing one or more “best practice” measures that could have stopped or mitigated the damaging effects of the particular attack. These protective measures include the following. These measures - and there are other protective measures - are essentially simple. They may be difficult to implement, but the sensitivity of the information they are to protect dictates their need.

- Security Procedures
    - Regularly applying security patches
    - Using secure code
    - Regularly monitoring system for security issues
    - Awareness training for all users of the system
- Effective Security Policies
    - Enforcement of acceptable computer Usage policy
    - Non-disclosure policy of sensitive information
    - Separation of duties policy
    - Separation from employment policy

Table 3 and Table 4 summarize these “What Ifs” and their expected effectiveness against each of the eight attacks

Table 3: Protective Measures for the Eight Attacks

Case Study Information Security Attack What If→	**Patches Applied**	**Awareness Training**	**Secure Code**	**System Monitor**	**Effective Security Policy, next Table**	**Stop/ Mitigate**
Morris - Worm	✓					**Mitigate**
Barrington - Grade Changing		✓			✓	**Stop**
Phillips - Social Security Numbers			✓	✓	✓	**Stop**
Getloaded- - Website Piracy	✓				✓	**Mitigate**
Shea – Time Bomb					✓	**Stop**
Carlson - Email Spam					✓	**Mitigate**
Manning - Wikileaks		✓		✓	✓	**Stop**
Gonzalez - Credit Card Fraud	✓		✓			**Mitigate**

Table 4: Security Policies for the Eight Attacks

Case Study Information Security Attack/ What If→	Acceptable Computer Usage	Non-Disclosure of Personal Information	Separation of Duties	Separation from Employment
Barrington - Grade Changing	✓			
Phillips - Social Security Numbers	✓			
Getloaded - Website Piracy				✓
Shea – Time Bomb			✓	
Carlson - E-mail Spam		✓		
Manning - Wikileaks	✓			

An effective security policy would never have allowed Barrington, Phillips and Manning to have accessed the sensitive data and information to which they were respectively not entitled. If Shea's company had a security policy with defined separation of duties, Shea could not have had the means and access to develop and implement his "time bomb".

Application of patches would have prevented some of the Morris worm attack paths from propagating. One of Getloaded's attacks would have been prevented had the targeted software been patched. Many of Gonzalez' attacks exploited the lack of security of sites using inadequate Wifi security. Various e-mail lists should have been better protected from access by Carlson because of their required privacy. While some elements of these four attacks would have occurred, their overall effects would have been mitigated.

6.2.3 Relevant Computer Crime and Security Surveys

CSI Survey

“2010/2011 Computer Crime and Security Survey” [8]

This is the final of the longest annual security survey by CSI.

This CSI Report identifies three levels of sophistication of attacks

1. Basic attacks – are such as phishing port scans and brute-force attacks. They cause much damage. Every organization is exposed to them, but a properly protected organization can protect itself from their effects. Basic attacks can be considered to be simple attacks, lacking planning.
2. Malware attacks - are a more sophisticated form of the basic attacks that require the defenders to very actively update their systems in order to stay ahead of the attackers. Insider attackers would often launch such attacks. These attacks are random attacks, and can also be classified as somewhat sophisticated.
3. Attacks 2.0, often called Advanced Persistent Threats, are highly sophisticated, against highly targeted systems, and entail a high degree of planning. They incorporate several zero day vulnerabilities. It is very difficult to defend against them, but conversely they entail considerable cost and effort for the attacker.

The report assumes that the roughly half of the respondents who did not report any cyber-attacks were subjected to some kind of basic attack.

The report did not provide a breakdown of attacks according to their level of sophistication.

One important survey query and its responses are addressed here.

“Did any of your security incidents experienced involve targeted attacks? The survey question was understood to refer to “a malware attack aimed exclusively at your organization or at organizations”.

The respective percentages of those responding positively to this question for the years 2007 to 2010 were:

- **Targeted malware attacks:**
    - **32% for 2007 - 27% for 2008 - 24.6 for 2009 – 21.6% for 2010**.

These average approximately 25% of reported attacks being targeted, and therefor **12.5%** targeted attacks for all respondents.

However, targeted attacks must be less than 12.5% of the total number of attacks, because individual attack responses referred to numerous actual attacks.

Also, the report notes that target attacks were often, but not always precursors to highly sophisticated attacks, Attacks 2.0, Advanced Persistent Threat.

This report stresses that targeted and highly sophisticate attacks are a growing concern. Although they are relatively few they are very damaging. The majority of attacks are still untargeted and unsophisticated which a properly protected organization can protect itself from their effects.

Verizon Reports

The Verizon yearly reports on computer security are derived from a dataset based on external forensic investigations and on data from partners' investigations [9].

- They interviewed administrators of networks for their experience with security measures and breaches, and
- They analyzed reported attacks against surveyed corporations to determine the following.
    - Were the attacks targeted or random?
    - Were the attacks simple or sophisticated?
    - Will standard security measures protect against simple attacks?
    - Are the losses due to targeted/sophisticated attacks greater than those of random/simple attacks?

Table 5 gives significant findings of the Verizon 2008 to 2011 reports, regarding sophisticated and targeted attacks, record losses, and Verizon determined avoidable breaches.

Table 5: Verizon 2008-2011 Annual Reports

Year →	**2008**	**2009**	**2010**	**2011**
Attacks↓	**Attacks/Losses, % of Total**	**Attacks/Losses, % of Total**	**Attacks/Losses, % of Total**	**Attacks/Losses, % of Total**
Highly Sophisticated	17/95	15/87	8/18	4/61
Targeted	28/90	27/89	17/21	16/63
Verizon Conclusion: Avoidable Breaches, % of Total	87	96	97	98

The following are some details of these findings.

- The highly sophisticated attacks often included use of specialized customized malware in order for the attacker to attack undetected and be often unstoppable.
- Percentage of loss of records due to highly sophisticated attacks was based on estimated the number of records compromised by highly difficult attacks. All lost records were treated similarly regardless of the value of a record.
- Targeted attacks were those that appeared that the victim was specifically chosen as a target. Note that it is possible that an attack was identified as both targeted and highly sophisticated.
- Percent of loss of records from targeted attacks was calculated by estimating the number of records that were compromised by targeted attacks, and these could

also include losses due to highly sophisticated attacks. Therefore, the sums of losses due to highly sophisticated attacks and to targeted attacks could exceed 100% as for 2008, 2009, and 2011.

- Avoidable breaches were considered such that could be stopped by simple or intermediate security procedures.

The 98% figure for avoidable breaches in 2011 correlates well with the percentage of attacks that were not highly sophisticated, i.e. 96% (100% - 4%). In fact, some of the 4% sophisticated attacks may have been stopped simple or intermediate means, as 98% includes sophisticated attacks.

The survey shows consistently that, over the span of four years, attacks were mostly not sophisticated. Likewise, most attacks were random, not targeted.

However, it was reported that highly difficult and targeted attacks, although infrequent, imposed most losses in terms of record value.

Verizon Reports Continued: Initial-Subsequent Attack Series

Starting in 2011 Verizon began identifying series of initial and subsequent attacks. Jay Jacobs, one the authors of the Verizon Report, shared part of the underlying data set analyzing some eighty-six, 86, such attack series. Table 6 breaks down these as percentages in levels of sophistication-very low to high-and as random and targeted.

Table 6: Verizon Analysis of 86 Initial/Subsequent Attacks

Type of Attacks	Very Low %, Initial/Sub-sequent	Low %, Initial/Sub-sequent	Moderate %, Initial/Sub-sequent	High %, Initial/Sub-sequent	Total, %, Initial/Sub-sequent
Random	3.5/2.4	68.6/53.6	17.4/29.8	0.0/0.0	89.5/85.8
Targeted	0.0/0.0	3.5/2.4	7.0/8.3	0.0/3.6	10.5/14.3
Total, %	3.5/2.4	72.1/56	24.4/38.1	0.0/3.6	100/100

Very Low: No special skills or resources required **Low**: Basic methods were used, no customization, and/or low resources required, used automated tools and scripts. **Moderate**: Skilled techniques were used, some customization, and/or significant resources required. **High**: Advanced skills were used, significant customizations, and/or extensive resources required.

All initial attacks were determined as not "highly difficult attacks". The Verizon researchers noted that even a sophisticated attacker will first try simple attacks in order to find weakness before deciding to use more sophisticated attacks on the target.

Table 7 shows that losses due to subsequent attacks, which were the more sophisticated, were a significant source of loss.

Table 7: Verizon: 82 Initial/Subsequent Series, Breaches and Losses

Attacks→ and their Effects↓	Very Low %, Initial/ Subsequent	Low %, Initial/ Subsequent	Moderate %, Initial/ Subsequent	High %, Initial/ Subsequent	Unknown %, Initial/ Subsequent
Percent of Breaches	2/2	65/49	24/39	0/4	8/6
Percent of Records Lost	0/0	37/6	16/37	0/61	47/0

Unknown: Cases where logs were sparse and the exact techniques utilized simply were not clear enough to assess their difficulty.

While the vast majority of the attacks were simple and easy to prevent the few difficult attacks caused, as noted, the most damage.

This 2011 data shows that by virtue of preventing or stopping initial attacks in these 82 cases no subsequent attacks would have occurred.   This finding has to be followed up regarding overall cyber-attacks.

Symantec Survey

Symantec Internet Security Report 2012 [10]

The Symantec Internet Security Report is based on:

- Symantec Global Intelligence Network, which is made up of more than 64.6 million attack sensors;
- Vulnerability databases, consisting of more than 47,662 recorded vulnerabilities;
- Symantec Probe Network, a system of more than 5 million decoy accounts; and
- Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

This report also determined the most frequently attacked vulnerabilities in 2011for which patches had been available, Table 8.

Table 8: Symantec Survey of Vulnerabilities Attacked in 2011

Vulnerability	Date of Patch	Number of Detected Attacks
MS Server RPC Handing Remote Code Execution Bid 31874 CVE-2008-4250	10/2008	61.2 million
MS Windows RPCSS DCON Interface DOS Bid 8234 CVE-2003-0605	8/2003	12.9 million
MS Windows LSASS buffer overflow Bid 10108	6/2004	4.3 million
MS Windows Server Remote buffer Overflow Bid 19409 CVE-2006-3439	8/2006	1.3 million
Adobe Acrobat, Reader and Flash Player remote code execution Bid 35759	9/2009	1.2 million

These vulnerabilities were at least two years old. The Symantec report lists several reasons why so many attacks were, and do occur, against old vulnerabilities that have well known patches.

- Exploits using newer vulnerabilities are more expensive for the attackers.
- Older vulnerabilities have more established malware and therefore they involve less effort for the attacker.
- Since there is always a part of the user community which did not apply security patches, there is ample opportunity for exploits based on old vulnerabilities.

The report investigated malicious E-mail attacks. One in 238.8 E-mails was identified as malicious; and of the malicious E-mails one in 8,300 were "highly targeted". The chance that an E-mail is a highly targeted malicious attack is 1 in 2 million. As highly targeted attacks, these targeted E-mail attacks were often precursors to Advanced Persistent Threats, according to Symantec.

Comments

- From the three Survey Reports sophisticated attacks are a small fraction of the incidence of cyber-attacks.
- However, they do account for a disproportionate amount of cyber-attack losses and damage.
- Nevertheless, according to the Verizon Report for 2011, Table 7 they may be preceded by low and moderate level initial attacks; but the relatively small sampling, and that was only the first year that categorization was done, calls for follow-up .
    - Accordingly, low and moderate levels of protection, may significantly stop or mitigate cyber-attack losses.

6.2.4 Low Probability/High Loss Risk Tolerance

While widespread low and moderate level protection will decrease overall cyber-attacks and their damage, consideration has to be given to risk tolerance in considering implementing sophisticated protection against catastrophic loss. There is always a low probability that a system will be subjected to a highly sophisticated attack, with considerable loss. It is also understood that protecting a system against a highly sophisticated attack could be very costly. A cost/benefit analysis should be constructed and should include input of the willingness of the system's owners to tolerate risk.

Risk tolerance level is often divided into three groups: risk-adverse, risk-neutral, and risk-seeking. Therefore the impetus and feasibility of investing in an expensive risk reduction technique will be greater for a risk-adverse system owner than for a risk-seeker system owner. It is often not cost effective to achieve a near zero risk through exorbitant cost using sophisticated technologies; indeed near zero risk can entail limited performance of a system and its user accessibility [11], [12].

At issue here is also risk perception, which pertains to the subjective judgment that people make about the characteristics and severity of a risk. A newly discovered risk tends to be overrated. More emphasis is often placed on Advanced Persistent Threats, CSI Survey, than on old Windows vulnerabilities, Table 8.

6.2.5 Summary of Evidence for Simple Attacks, and Simple Protection

1. The above cited Benson and Moore [2], 1992:256-57, study is relevant to the relationship between white collar crime and cybercrime. This study of over 2,400 convicted white collar criminals, and about 2,000 typical crime offenders concluded that the evidence supports applying the low self-control accounting of white collar crime when it is chronically committed. Criminals with low self-control tend to desire quick and easy results.

2. Six of the eight case studies attacks are classified as of low or medium sophistication. All of the attacks could have been stopped or mitigated by simple protections.
3. The CSI annual reports, 2007-2010, which are based on survey responses found that of approximately half of the respondents who reported cyber-attacks, only about 25% of the attacks were targeted attacks. This information was derived from 500 information security and information technology professionals in United States corporations, government agencies, financial, educational and medical institutions, and other organizations.
4. The Verizon Reports which are based on “first-hand” evidence collected from paid external forensic investigations conducted by Verizon from 2004 to 2011 support the prevalence of simple attacks and efficacy of simple protections. The 2011 caseload is the primary analytical focus of the report, but the entire range of data is referenced extensively throughout. Though the RISK team worked a variety of engagements, over 250 in 2011, only those involving confirmed data compromise are represented in this report. Ninety of these were completed and showed that 11% of attacks can be classified as highly sophisticated and 95% of all attacks can be avoided using simple or intermediate controls.
5. The Symantec Internet Security Report which is based on: (1) Symantec Global Intelligence Network, which is made up of more than 64.6 million attack sensors; (2) Symantec Probe Network, a system of more than 5 million decoy accounts; and (3) gathering phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

> The collected information showed that the most common attacks were exploiting three to four year old vulnerabilities for which patches were available. The report does not deal with tracking the number of successful attacks against these vulnerabilities, and their impact. It did show that targeted email attacks were only a very small percent of malicious email.

6.3 Increased Moral Deterrence

The cited literature in the on deterrence, specifically Sections 4.36, 4.37 and 4.38, on informal sanctions, shame and embarrassment and morality showed that these sanctions are generally more effective in decreasing typical crime than formal sanctions. Often it is argued that the greatest deterrence of formal punishments is the added repulsiveness to committing the crime more than the fear of actually receiving the formal punishment.

This is especially true of corporate offenders as Chambliss, 1967 [13] states that because they are as a rule are not committed to criminal lifestyle they are more deterrable because of sanctions. Furthermore Braithwaite and Geis, 1982 [6] and Scott, 1989 [14] argue that corporate criminals due to their social status will be responsive to embarrassment that often accompanies formal legal sanctions.

The shame and embarrassment, moral, deterrent of potential corporate criminals is extended further by Paternoster and Simpson, 1996 [15] with the suggestion that “moral appeals may be especially powerful source of corporate social control”. This deterrent should be implemented by two steps.

- Strengthen business ethics of corporate managers through moral education.

- Instill awareness of and enforce business laws and regulations.

The reason that moral appeals alone may not be sufficient is that their studies showed that not everyone is deterred by morality. Therefore when the morality factor fails to deter, compliance can be secured through legal threats. Also, the awareness of legal sanctions can strengthen moral repulsion of the behavior. Greater legal punishment makes the behavior more shameful in the eyes of the offender.

The strong parallelism between corporate/white collar crime and cyber-crime, 6.2.1 above, indicates that at least the advanced amateur attackers who are most similar to white collar criminals would be deterred by "appealing to their morality". The methods to increase awareness of the moral implications for cybercrime are:

- Actively logging and monitoring;
- Aggressively confronting attackers, and attacks; and
- Awareness training which would be mostly effective for insider threats.

Using active monitoring and then aggressively confronting attackers will increase the embarrassment of would-be attackers even if legal sanctions are not pursued. Awareness training will be very effective against potential inside attackers who approximate 50% of cyber-attacks. There is some awareness "training" that can be done even for would-be outsiders in the form of warnings placed on systems that appeal to one's morality.

The effectiveness of monitoring and awareness training as a deterrent to computer misuse, as opposed to attack, is documented in a study by D'Arcy et al. [16]. Although information systems misuse may well not constitute an attack, it is almost always confined to insider action, it is considered similar to information security attacks. These authors found that perceived certainty of punishment was a greater deterrent to prevent computer misuse than perceived severity of punishment by attackers who have high levels of moral commitment. On the other hand, attackers, whose level of moral commitment is low, perceived severity of punishment as the greater deterrent. This can be explained by equating the amateur attacker, who is not committed to a criminal life, to a corporate criminal who will be much deterred by embarrassment which is very sensitive to the certainty of being discovered. On the other hand the professional cybercriminal who has great criminal propensity, if he is deterred it will be due to the severity of the punishment more than the embarrassment of being caught.

6.3.1 Summary of Evidence for Increased Moral Deterrence

1. The study by Paternoster and Simpson, 1996 on corporate crime is relevant to cybercrime that morality plays a role in deterring corporate crime. Here, 96 respondents, 84 students and 12 executives, completed the research instrument. About 50% of these respondents were male, 84% were white, and the average age was nearly 29. Actually, the total sample size was 384, because each respondent read and responded to four different scenarios describing the commission of corporate crime (96 x 4 = 384). This study is described in Section 3.2.4.
2. Moral consideration played a role in six of the eight case studies. Statements of regret due to moral consideration by the offender during the sentencing phase may not indicate that moral consideration would have deterred the offender at the time of commission of the crime.

3. The D’Arcy, Hovav and Gelletta, 2009 study provided documentation for the effectiveness of monitoring and awareness training by 269 usable responders to an online survey. Email invitations were sent to 805 employed professionals to complete the survey; 304 responded for an initial 38% response rate. Incomplete or otherwise unusable entries were discarded from the dataset leaving 269 usable responses (33%). It is unclear where the original pool of 805 employed professionals came from. These 269 computer users were from eight different companies. This survey also showed that users with high levels of moral commitment are deterred by certainty of punishment.

6.4 References

[1] Gottfredson, M., and Hirschi, T., 1990, *A General Theory of Crime,* Stanford University Press, Stanford, CA.

[2] Benson, M., and Moore, E., 1992, "Are White-Collar and Common Offenders the Same? an Empirical and Theoretical Critique of a Recently Proposed General Theory of Crime " Journal of Research in Crime and Delinquency**, (29) 3**, pp. 251-272.

[3] Geis, G., Meier, R.,F., and Salinger, L., M., 1995, *White-Collar Crime: Classic and Contemporary Views,* Free Press : Distributed by Simon & Schuster Inc., New York, NY.

[4] Reed, G., and Yeager, P. C., 1996, "Organizational Offending and Neoclassical Criminology: Challenging the Reach of a General Theory of Crime," Criminology**, (34) 3**, pp. 357-382.

[5] Sutherland, E., 1949, *White Collar Crime,* Dryden press, New York.

[6] Braithwaite, J., and Geis, G., 1982, "On Theory and Action for Corporate Crime Control," Crime and Delinquency**, (28) 2**, pp. 292-314.

[7] Simpson, S., and Piquero, L., 2002, "Low Self-Control, Organizational Theory, and Corporate Crime," Law and Society Review**, (36) 3**, pp. 509-548.

[8] Richardson, R., 2011, "CSI Computer Crime and Security Survey 2010/2011," Computer Security institute, from http://gocsi.com/survey.

[9] Verizon RISK Team, 2012, "2012 Data Breach Investigations Report," Verizon, .

[10] "Internet Security Threat Report, Volume 17," 2012, Symantec Corporation, Mountain View, CA.

[11] Bernstein, P., 1996, *Against the Gods : The Remarkable Story of Risk,* John Wiley & Sons, New York.

[12] Modarres, M., 2006, *Risk Analysis in Engineering : Techniques, Tools, and Trends,* Taylor & Francis, Boca Raton.

[13] Chambliss, W., 1967, "Types of Deviance and the Effectiveness of Legal Sanctions," Wis. L. Rev, pp. 703-719.

[14] Scott, D., 1989, "Policing Corporate Collusion," Criminology**, (27) 3**, pp. 559-587.

[15] Paternoster, R., and Simpson, S., 1996, "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," Law & Society Review**, (30) 3**, pp. 549.

[16] D'Arcy, J., Hovav, A., and Galletta, D., 2009, "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research**, (20) 1**, pp. 79-98.

7 Conclusions

7.1 Summary of Work

An influence model for cyber-attacks, information security attacks, was developed using criminology, law and information security literature mainly by drawing the parallelism between cyber-crime and typical criminal behavior. The applicability of well-established typical crime theories to cyber-crime is not deterred by the uniqueness of cyber-crime, namely the remoteness and particular power of the attacker, and the uncertainty of cyber laws. The crime theories of Rational Choice, Low Self-Control, and Situational Crime Prevention were applied to cyber-crime. Accordingly, that literature was used to develop and define the nodes of the influence model to represent the factors that have to be considered for launching a cyber-attack. The links between the nodes show the path and strength of the various factors, and influence they have on each other. This influence model essentially reflects the perspective of the attacker. The likelihood that a specific attack would be launched is determined by three root nodes, motivation of the attacker, her opportunity, and deterrence.

The main purpose of the model is to explain how and why a cybercrime will or did occur, and how it can be prevented or stopped, or how its effects can be mitigated when attacks do occur.

This thesis attempts to dovetail each type of cyber attacker with the theory most appropriate to the description of her particular crime. Future directions of this research would also include applying Rational Choice theory to all cyber attackers, including the ordinary amateur.

This work adds face validity to the depth of the credibility of cyber-security measures, and to the understanding of the factors affecting cybercrime. In addition the work broadens the approach to cyber-security from a solely a technology centric perspective to the inclusion of a behavior based perspective. The incorporation of a behavior based approach may enable the highlighting of deficiencies in security measures that would not otherwise appear obvious from a purely technological view.

While, much of the model can be adapted to deal with non-cybercrimes, for example terrorism and white-collar crime, many of its nodes are specifically cybercrime oriented, such as the means and vulnerability sub-nodes. More important is the degree of influence of the links connecting nodes which is based on cybercrime surveys, experience and literature.

The correctness of this model is validated by how well it accommodated crime and cybercrime concepts, and their underlying findings. Included in this validation are major annual information security surveys whose conclusions can be understood through this model.

The proposed model was successfully mapped onto eight case studies that were analyzed from related court prosecution/decision documents, press accounts and specific public reports.

.

7.2 Major Contributions

1. The core hypothesis of this research was that general criminology theories are applicable to cybercrime. This hypothesis was evaluated and addressed through analyses of similarities and contrasts between criminology and information security literature, cybercrime case studies, and information security surveys. The following are examples of such similarities and contrasts.
    - Rational Choice Theory as applied to typical crime indicates that a cybercriminal also does a cost/benefit analysis before attempting to attack. Cyber-attacks have shown to be generally similar to white collar crime attacks, typically committed

by people who are well-educated, very patient, and exhibit considerable self-control.

- An outgrowth of the Rational Choice theory is that removing crime opportunities is usually effective in reducing overall crime and does not result in a simple displacement of that offence to other times, places or crimes, with no net reduction in crime. Cybercrime is similar, and when a popular path of attack is removed there is usually an overall reduction in attacks. A would-be attacker will not necessarily seek another path of attack [1].
- The Situational Crime Prevention Techniques to reduce crime, can also be adapted specifically for cybercrime. Increased visibility (lighting, patrol) in public and sensitive areas and continuous electronic monitoring (closed circuit TV) improves crime detectability and reduces criminal opportunity. Likewise, requiring id for website access, and increased and announced access logging achieve the same [3], [4].
- Knowledge and theories such as the Low Self-Control and Desire for Control used to understand the causes of white collar crime can also be directly applied to cybercrime. This is very useful in understanding the role of moral deterrence in cybercrime.
- Moral deterrence is especially applicable to the advanced amateur cybercriminal who is much like the white collar criminal. The professional cybercriminal has a highly self-perceived criminality and will be less deterred by moral considerations.

2. Using crime theories and their implications a new **General Influence Model** was developed that integrates *known factors and sub-factors*, and their *relationships* regarding attempted *cyber-attacks*, emphasizing the attacker's perspective. These factors and strength relationships between them make the model "greater than the sum of its parts". This model is uniquely useful to *understand and highlights* cyber-attacks, and to *generate countermeasures*. The correctness and completeness of the model is further justified by information security literature, as well as criminal justice, social science and logic literature used to develop the factors and relationships known to influence a cyber-attacker

3. Application of the Model

   The following are specific considerations to be dealt with in establishing cyber security, or mitigating consequences of attacks.

   - Using the model in conjunction with criminology and information security literature, case studies, and information security surveys it was shown that most cyber-attacks are simple in nature, and that well known readily available protective means will be most effective in protecting systems in most circumstances. This can be useful in determining resource allocation for information security.
   - The most prevalent vulnerability in a system is due to human factors, e.g. negligence and social engineering enticement; this should be accordingly addressed.
   - As in typical crime, monetary gain is the dominant motivator for cybercrime.

- It is presently debatable whether certainty of punishment or its severity is the greater cyber-crime deterrent; certainty of punishment is the greater typical crime deterrent [2].
- Moral deterrence, namely shame and embarrassment, was shown to be a significant factor in discouraging many forms of cybercrime. This deterrence may be more effective than the traditional formal punishments, which often lack in certainty and swiftness.
- Cyber-attack awareness training, emphasizing this moral deterrence, should impact insider attacks, which account for about one half of cybercrime events. Likewise, the threat of shame and embarrassment will be generally apparent by publicized monitoring, which will increase the certainty that an attacker will be detected and confronted.
- To defend against different types of cyber-attackers, i.e. amateur, professional, etc., the defender determines her system's value as perceived by potential attackers and, commensurately, which type of attacker would be motivated to launch an attack. The defender would then determine the resources needed to protect her system against the expected attacker.
- The model can be used in the Design/Implementation, Operation, and Recovery phases of a system.
    - For the **Design/Implementation phase** of a system emphasis should be applied in ***reducing security attack attempts*** by: *decreasing opportunities*, *increasing deterrence*, and *diminishing* an attacker's *internal motivation*.

- During the **Operation phase** of a system the model can be used likewise to proactively stop attacks, or to mitigate their progression.
- For the **Recovery** phase the model can be used likewise to ***retroactively analyze attacks***, to better understand ***"why"*** they affected ***particular targets***, and to be able to answer ***"what if"***.

7.3 Future Work

7.3.1 Apply Bayesian Belief Network, BBN

The influence model offers a qualitative assessment of a cyber-attack. Since it is based on literature and on limited studies, it yields a sense of which of its nodes and the strength of relationships between nodes are stronger, given a cybercrime environment. Continued effort on this model should be directed to build formal quantitative assessments of at least some of these relationships. This would be backed by empirical evidence where it is available. Then, with enough such evidence a Bayesian Belief Network, BBN, can be constructed, and a more precise semi-quantitative assessment can be performed. As such evidence is increased the model will improve. Questions like what would happen if effort is made to remove hardware vulnerabilities, essentially setting that node to zero. How would this affect the overall probability of a cyber-attack taking place?

7.3.2 Apply Game Theory to the Model

There are game theories that deal essentially with how intelligent individuals interact with one another in their efforts to achieve their own goals.

Game theory has been applied to economics, foreign affairs, and biology. It has also been used in information security for building attack graphs, see CMU [5]. Surprisingly, very little work has been done applying game theory to criminology. Application of game theory can be considered for this model in a number of cyber-attack approaches and scenarios.

- An attacker can be viewed as one player, and deterrence or punishment that the attacker will receive for committing the attack as the second player. Deterrence can take the form of formal punishment such as jail time and fines. These formal punishments are dependent on certainty, severity and swiftness of their execution. Other forms of punishments are informal punishments like shame and embarrassment. These, although they are generally less severe than formal punishments, have much greater certainty attached to them. Game theory would then evaluate the effectiveness of these various deterrents for given situations. Similarly game theory could then be applied to evaluate the various opportunity factors.
- Computer attacks that take place because of a “revenge” motivation can be constructed as the “Prisoner’s Dilemma” game repeated multiple times to form a “tit-for-tat response”. This would be similar to games constructed for modeling arms control agreements.
- There is a need to look at security as a game between different defenders. What one defender does for defense has an effect on other defenders. Some defensive strategies shift the crime onto other defenders so they too have to invest in this aspect of security. An example is installing visible alarms will shift the crime

target to other defenders who now have to invest against attacks that they did not anticipate. This can cause an overinvestment in security viewing society in general. Other defensive actions such as installing antivirus which reduces the spread of a virus from one computer, and thus has a positive effect of protecting neighboring computers. This may create underinvestment in defensive strategies of these other operators who may be relying on “free rides”.

7.3.3 Human Reliability Analysis

Section 4.26 Human Errors Node of this dissertation deals with the human failures that lead to cyber-attacks, particularly those generated by social engineering. That human vulnerability warrants comprehensive study and analysis. Human reliability models such as the Systematic Human Reliability Procedure (SHARP) developed by Hannaman and Spurgin, 1984 [6], [7], could also be used to quantitatively evaluate this node. The SHARP assessment has seven steps.

1. **Definition** of all human errors that can facilitate social engineering cyber-attacks.
2. **Screening** Select significant human errors that will be further analyzed.
3. **Qualitative analysis** is performed to further understand these human errors; what caused and what contributed to the error performance shaping factors (PSF).
4. **Representation** Build a representation of how the errors lead to failure, e.g. build an event tree.
5. **Impact assessment** Explore the impact of human errors identified in the preceding steps
6. **Quantification** Using the above results build a likelihood index for various human errors

7. **Documentation** produce a traceable description of the process used to develop the assessment.

7.4 Appendix A: Structured Case Study Questions

1. What was the (Motivation) Goal of the attack?
   - Monetary Gain
   - Non-Monetary Gain
   - Blackmail
   - Hate/ Revenge
   - Challenge
2. What was the relationship between the attacker and intended target?
   - Insider
   - Outsider
3. What best describes the attacker's propensity to commit the crime?
   - Amateur
   - Professional
   - Government agent / Terrorist
4. What was the target selection?
   - Random
   - Planned
     - Specific firm
       - Random target or record in firm
       - Specific target or record in firm
5. Did the attacker use Reconnaissance before the attack?
   - Yes

   - No

6. Did the attacker use tools to perform the attack?
      - Yes
      - No
7. What was the attacker's knowledge and skills level?
   - This information can be gleamed from mistakes the attacker made, or from the sophistication of the attack?
8. Did the attacker work with a team or as an individual?

- If worked in a team what was his/her relationship with other team members?
   - Human factors

9. Time Bound?
      - Measured how long the attack continued until it was discovered?
      - Estimate how long that attack should have continued had the defender practiced due diligence.

10. What was the defender's Security Posture?
       - Security Policy and adherence?
       - Security Culture?
          - Insider attacks provide much information about a firm's Security Culture.
          - Examining the path of an attack with respect to the Security Policy can yield insights to Security Culture.

11. Futility: Had the attack been less successful than anticipated would that have deterred the attacker?
    - Did the attacker continue attacking even after getting disappointing results?
    - Did the attacker express remorse that the attacks were not as successful as anticipated?
12. Consequences: Did fear of punishments play a role in the decision to attack?
    - Was the attacker warned, but continued the attacks?
    - Was it a crime of passion i.e. Revenge or Hate?
    - Did the offender go to great lengths to avoid capture or punishment?
13. Morality: Did morality have a role in decision to attack?
    - Did the attacker express remorse for his/her actions?
    - Did the attacker's lifestyle before and after the commission of the crime reflect one of high morality?

7.5 References

[1] Felson, M., 1994, *Crime and Everyday Life : Insights and Implications for Society*, Pine Forge Press, Thousand Oaks, CA.

[2] D'Arcy, J., Hovav, A., and Galletta, D., 2009, "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research**, (20) 1**, pp. 79-98.

[3] Clarke, R., 1980, "Situational Crime Prevention: Theory and Practice," British Journal of Criminology**, (20) 2**, pp. 136-147.

[4] Willison, R., and Siponen, M., 2009, "Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention," Communications of the ACM**, (52) 9**, pp. 133-137.

[5] Sheyner, O., Haines, J., Jha, S., Lippmann, R., and Wing, J. M., 2002, "Automated Generation and Analysis of Attack Graphs," *2002 IEEE Symposium on Security and Privacy*, pp. 273-284.

[6] Hannaman, G., and Spurgin, A., 1984, "Systematic Human Action Reliability Procedure (SHARP)," NP-3583, Electric Power Research Institute, Palo Alto, CA.

[7] Modarres, M., 2006, *Risk Analysis in Engineering : Techniques, Tools, and Trends*, Taylor & Francis, Boca Raton.