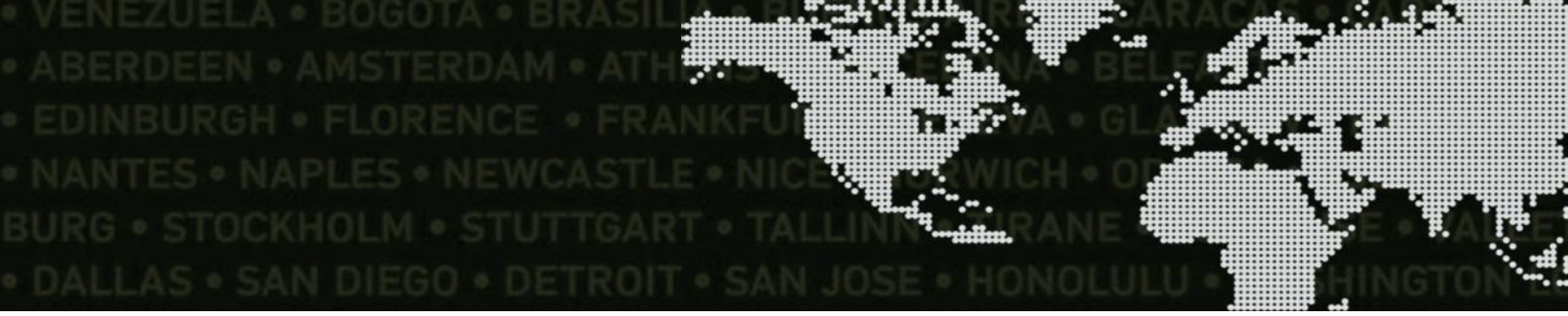


"A Failed State of Security"

A Rational Analysis of Deterrence Theory and The Effect on CyberCrime

Chris Mark, *CISSP, CIPP*

www.MarkConsultingGroup.com

www.GlobalRiskInfo.com

435-513-0484

chris@markconsultinggroup.com

Table of Contents

Abstract

In reviewing the literature on criminology and information security it appears that, while they share many common themes, there is a disconnect between the criminological theory and its application in information security. Information security, as a field, is focused on the protection of information assets. Criminology is focused on the prevention of criminal behavior. As most information security practitioners will likely attest, there is little overlap between the two fields and there has been little research or focus on the use of crime theories on the prevention of cybercrimes. This paper attempts to bridge the gap between the fields and highlight the deficiencies in the current approach of compelling victims to prevent cybercrime as opposed to deterring the criminals from committing cybercrimes.

Introduction

In keeping with the recurring theme for the last several years, 2011 presented some of the largest, and most publicized data breaches in history. In addition to security vendors such as RSA disclosing a breach of their vaunted SecureID system, and Sony was repeatedly hacked, resulting in the breach of consumer data. Additionally, 2011 also saw hacktivism begin to take center stage, with groups breaching the International Monetary Fund (IMF), Stratfor, and various government agencies. The dawn of 2012 has seen a growing threat of state sponsored cyberespionage and intellectual property theft. Since 2000, the US Government, as well as 46 state governments, numerous foreign governments, and a variety of industry bodies have increasingly focused on protecting personal data. Within the US alone has different 46 state breach notification laws at this time, numerous payment card industry standards, and various state data protection laws in place.

The concepts of *deterrence* and *compellence* are familiar to parents, law enforcement personnel, political scientists, sociologists, and military strategists, to name but a few. Affecting a person's decision making and subsequently modifying behavior to either deter an unwanted action or compel a desired action are common tactics. If one were to ask why people pay taxes, many would likely answer that they don't want the IRS to penalize them for not filing. This is an example of compellence. Additionally, if asked why people don't exceed the posted speed limit, the majority of respondents will likely respond they "don't want to get a ticket". This is an example of deterrence. Military strategists, political scientists, economists, and criminologists have long recognized the value of compelling an adversary to act in a particular manner or deterring unwanted actions. These two concepts are so inextricably

entwined with criminology it is not even possible to speak of "crime prevention" without considering how to deter deviant behavior and compel lawfulness. Unfortunately, for companies facing increasingly frequent attacks against their systems, and data by increasingly sophisticated criminals, there is little, if any effort to deter the crimes. To make matters worse, the victims are made to proactively deter future crimes. Data theft is a crime. Hacktivism is a crime. Cyberespionage is a crime.

At its most basic level, crime prevention relies upon two basic principles; appropriate protective security controls, and crime prevention through deterrence and/or compellence of behavior. Unfortunately, the laws, strategies, and other mechanisms enacted to protect data have not kept pace with the cybercriminals. This has left companies fending for themselves in a veritable 'Wild West' of hackers, data thieves, and hacktivists in which the criminals can act with near impunity. Unfortunately for the companies being victimized, there is neither a sheriff nor a deputy to stop the acts. Even if there was, there are few, if any, effective laws to which the criminals can truly be held accountable. If a person robs a bank, the bank is not eviscerated in the press or held responsible for the robbery. If a bank has financial data stolen by a cybercriminal the bank is required to wear a scarlet letter displaying their inability to not be victimized.

This paper will discuss the state of cybercrime today and discuss the concepts of deterrence and crime prevention. Finally, it will discuss why the current environment of regulation and penalizing the victims in order to protect data is a failing strategy.

CyberCrime Today

Much like reports their previous reports, the 2011 Verizon Data Breach Report showed a sharp increase in the number of identified data compromises from 2009-2010. In 2009, Verizon reported 141 data breaches compared to 761 in 2010. 2010 saw a decrease in large companies being compromised but there was, according to Verizon, an "explosion of breaches involving smaller organizations."[1] Additionally, companies are increasingly being targeted by criminal organizations and not 'lone' cyberthieves. In 2011 organizations such as Sony, Epsilon, HBGary, Wordpress.com, TripAdvisor/Expedia, and RSA have all fallen victim to data compromises. This seems to counter Verizon's suggestion that in 2010 the cybercriminals were beginning to target small organizations that represented a 'lower risk.'

[1] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

At RSA's annual security convention, the head of the Federal Bureau of Investigation, Mr. Robert Mueller stated, on February 28th, 2012, ominously: *"There are only two types of companies. Those that have been hacked and those that will be."*[2] At the same event, the CEO of RSA, told the audience: *"Our networks will be penetrated. We should no longer be surprised by this."* He further stated*: "The reality today is that we are in an arms race with our adversaries, and right now, more often than not, they are winning."*[3] The comments, while accurate, are late in coming. RSA, one of the worlds' largest security vendors, was breached in 2011. The breach was more than a simple theft of customer data. The breach was a theft of intellectual property that compromised the infrastructure of RSA's 2-factor authentication system known as SecureID. This potentially exposed thousands (if not more) of companies to a bypass of their own access control mechanism.

RSA's CEO then continued:

> *"Online security has traditionally been about building the biggest, fiercest defenses possible to keep attackers out. That's not enough. Now, you have to assume you've been compromised, and invest just as heavily in* ***detection****."* He continues: "*We need to tap more military experience and military intelligence experience," Coviello said. "The new breed of analysts I'm talking about need to be* ***offensive in their mindset****." (emphasis added)*[4]

As any student of foreign affair or military strategy can attest, adopting a more military type experience and offensive mindset is not possible without adopting one of the primary tools of the military and US defense strategy; deterrence.

Unfortunately for companies on the receiving end of an attack, it is neither legal nor ethical for businesses to adopt an offensive deterrence strategy against cyber criminals. This leaves companies without one of the primary tools of crime prevention, and defense. The lack of a deterrent threat can be seen as a major reason that cybercrimes continue to increase seemingly unabated.

[2] Sengupta, S., and Perloth, N. (March 5, 2012) "The Bright Side of Being Hacked"; New York Times online. http://www.nytimes.com/2012/03/05/technology/the-bright-side-of-being-hacked.html?_r=2&pagewanted=all
[3] Cowley, Stacy. (Feb 28, 2012) "New Cybersecurity Reality: Attackers are winning." http://money.cnn.com/2012/02/28/technology/rsa_cybersecurity_attacks/index.htm
[4] Cowley; 2012

A Primer on Security

The definition of security, as a concept, is often debated. Security by itself represents only one element of crime prevention. For this reason, it is not possible to discuss crime prevention without a working understanding of the concept security. While a number of definitions exist, for the purposes of this paper we will use a rather simplistic definition of security. Security can be defined as the *"implementation of controls to address vulnerabilities with the objective or providing protection for assets."* It is important to understand that security cannot be 'assured ' and security can never be considered to completely address all potential threats as there are always vulnerabilities that can be exploited. Vulnerabilities may not have been identified yet, but they do exist. Given enough time, effort, and the right tools, any security control can be circumvented. Security can be measured as a *function of the time and resources needed to circumvent the controls in place to protect the assets*. Security should be commensurate with the risk to the assets that the controls are intended to protect. For example, a house may be considered to have 'appropriate security' if the standard door and window locks are installed and the house does not possess any assets of great value. The same house's security, if used to store the Hope Diamond, would be considered grossly inadequate since the risk has increased with the addition of the diamond. Security then can only be evaluated in the context of risk.

Second, it is important to understand that the concepts of exploits and vulnerabilities are inextricably entwined and are mutually dependent. A vulnerability can be described as a susceptibility that would allow a single (or combination of) technique, tactic, or technology (exploits) to circumvent, bypass, or defeat the protection offered by the technique, tactic, or technology in place as protection (the control). In short, vulnerability *is a susceptibility to an exploit.*

Conversely, an exploit can be described as a technique, tactic, or technology which can be used to circumvent, bypass, or defeat a given technique, tactic or technology used as a protective control. In short, an *exploit is something that can be used to take advantage of a susceptibility in a control* (a vulnerability).

The concepts have been written in an intentionally circular manner to reinforce their relationship. As stated previously, exploits and vulnerabilities are inextricably entwined and are not mutually independent. In fact, one can only exist in theory without explicit knowledge of the other. Since this position is likely controversial an example will help illustrate the point.

Consider a modern bank vault with 3 foot thick, reinforced concrete walls covered with hardened steel and a Class 3 bank vault door made of 12 inch thick reinforced concrete, hardened steel locks, and all of the accompanying features. A Class 3 vault door is rated to withstand 120 minutes with "torch and tools"[5]. This means that a person with a cutting torch and tools (prybars, etc.) can circumvent the door's security in 2 hours. This is all the manufacturer can guarantee and the safe is rated and certified under the Underwriters Laboratory. In the description of a Class 3 vault door provides insight into at least one vulnerability that has been identified that will allow a person to defeat the control in over 2 hours with the proper exploit. Quite simply, the vulnerability is the melting temperature of the steal used to construct the door and the exploit is the focused heat of a torch and tools.

To reinforce the concept of exploits and vulnerabilities as discussed above, an example will used. Now consider the same vault being transported back 3 thousand years to the time of the Egyptian empire and the Bronze Age. If you were able to ask a person during the Bronze Age whether the vault was "vulnerable" to any known tools or techniques the answer would likely be a resounding 'No'. During the Bronze Age, iron had not yet been discovered and steel was at least 1,000 years away from being invented. There was no mechanism to create enough focused heat to even test the metal. In short, there were no KNOWN exploits and no KNOWN vulnerabilities. This is a very important concept. It should be noted that whether or not the exploits and vulnerabilities had been identified does not change the fact that they still existed. Someone could have likely said: *"In theory, if we can get a flame hot enough and focused enough we can burn through the door."* As stated, without the vulnerability being explicitly known the exploit existed in theory only. In the same way, without explicit knowledge, the vulnerability existed in theory only. As stated, the implementation of protective controls is only one component of cybercrime prevention. The second component applies to the 'human element' of crime.

An Overview of Deterrence Theory

Deterrence theory has applications in a variety of fields including military, and maritime security settings, foreign affairs, and in criminology, to name a few. While seemingly unrelated, when looked at closely, the similarities are apparent. Each these fields involve human decisions and humans that have the ability to behave and act in a manner contrary to the wishes of the other party. It is the 'human element' that is being modified by deterrent strategies.

[5] SafeandVault.com http://safeandvault.com/index.php/vaults-a-doors/class-3-doors

History of Deterrence Theory

The concept of deterrence is relatively easy to understand and likely extends to the earliest human activities in which one early human dissuaded another from stealing food by employing the threat of violence against the interloper. Written examples of deterrence can be attributed as far back as the Peloponnesian War, when Thucydides wrote that there were many conflicts in which one army maneuvered in a manner that convinced the opponent that beginning or escalating a war would not be worth the risk.[6] In the 4th Century BC, Sun Tzu wrote: *"When opponents are unwilling to fight with you, it is because they think it is contrary to their interests, or because you have misled them in to thinking so."*[7] While most people seem to instinctively understand the concept at the individual level, contemporary deterrence theory was brought to the forefront of political and military affairs during the Second World War with the deployment of nuclear weapons against Nagasaki and Hiroshima.[8]

The application of deterrence during WWII was the beginning of understanding that an internal value calculus drives human behavior and that behavior could be formally modeled and predicted with some degree of accuracy. By the mid-1940s and through the 1950's John Van Neuman and, later Nobel Prize recipient John Nash (a Beautiful Mind), developed the mathematical models of Game Theory, which addresses human rationality and decision making. Game theory and the concepts that underlay game theory are inextricably entwined with deterrence. Game theory is defined as: *"the study of mathematical models of conflict and cooperation between intelligent, rational decision makers."*[9] By 1962 game theory and its underlying principle of the Rational Actor Model (RAM) was put to real world use during the Cuban Missile Crisis. In this instance the Nash Equilibrium[10] was employed to predict that the Soviet Union would not escalate the crisis by attempting a run of the US Naval Blockade. The clearest evidence of the value of deterrence can be seen in Nikita Krushchev's own words when he warned colleagues that they were: *"face to face with the danger of war and of nuclear catastrophe, with the possible result of destroying the human race."* He went on to say: *"In order to save the world, we must retreat."*[11]

---

[6] Alexander L. George, Richard Smoke (1974). *Deterrence in American Foreign Policy: Theory and Practice*. Columbia University Press. P 84
[7] Greene, Robert. (2006) *The 33 Strategies of War.* Viking Penguin. P 135
[8] Taquechel, Eric F. (Feb 17, 2012). *Validation of Rational Deterrence Theory: Analysis of U.S. Government and Adversary Risk Propensity and Relative Emphasis on Gain or Loss.* Kindle Edition. (Kindle Locations 561-563)
[9] http://en.wikipedia.org/wiki/Game_theory
[10] http://en.wikipedia.org/wiki/Nash_equilibrium
[11] Allison, Graham (1971). *Essence of Decision*: Explaining the Cuban Missile Crisis, 1ed. Little Brown. P 362

The concept of deterrence is synergistic with the concepts of the rational actor model and game theory. Today, rational deterrence theory has application to, and is frequently employed in, national defense, tactical military operations, counterinsurgency, counterterror, law enforcement, security, and numerous other areas where the predictable understanding of human behavior plays a crucial role.

Key Concepts of Deterrence Theory

USAF General Kevin Chilton (2009) accurately describes deterrence theory when he says:

> *"deterrence is ultimately about decisively influencing decision making. Achieving such decisive influence requires altering or reinforcing decision makers' perceptions of key factors they must weigh in deciding whether to act counter to (our interests) or to exercise restraint."*[12]

This single sentence encompasses the two underpinnings of deterrence; rational choice and risk management.

Rational Actor Model (RAM)

Deterrence and game theory rely upon the premise that people are rational actors. The Rational Actor Model is based on the rational choice theory which posits that humans are rational and will take actions that are in their own best interests. Each decision a person makes is based upon an internal value calculus that weighs the cost and the benefits of an action. By altering the cost-to-benefit ratios of the decisions, decisions, and therefore behavior can be changed accordingly. While the concept is simple in theory, it can be somewhat more complex in practice. It should be noted at this point that 'rationality' relies upon a personal calculus of costs and benefits. When speaking about the rational actor model or deterrence, it is critical to understand that 'rational' behavior is that which advances the individual's interests and, as such, behavior may vary among people, groups and situations. For this reason, it is impossible to prevent all crime through deterrence. Some people will simply weigh the pros and cons of committing a crime and determine it is 'worth the risk' based upon their personal value calculus.

While some criminologists dispute RAM in favor of other models, anecdotally it is difficult to argue with the value of the model. In *The Management of Savagery* by Al Qaeda strategist Abu Baker Naji, he

[12]Chilton, Kevin. (2009) "Waging Deterrence in the Twenty First Century"; *Strategic Studies Quarterly*

directs planners to weigh the "benefit and harm" of differing actions.[13] This clearly indicates a rational model where a cost benefit calculus is being applied to the operations of a terrorist organization. George Habash of the Popular Front for the Liberation of Palestine was quoted as saying: "*The main point is to select targets where success is 100% assured."*[14] This, again, echoes the model of risk management and a rational model of decision making. While the previous quotes are attributed to terrorist organizations or those associated with terrorist originations, the concept repeats in all areas of behavior, including cybercrime.

In his seminal work *More Guns Less Crime*, economist John Lott discusses burglary rates in Canada, the United Kingdom, and the United States. In Canada and the UK, where gun control laws are strict, almost half of all burglaries are classified as "hot," meaning someone was in the house when the burglars committed the crime. In the US, where gun ownership is more prevalent, "hot" burglaries only account for about 13% of all burglaries. As Lott explains: *"criminals are not behaving differently by accident."* Surveys of convicted felons indicate that the felons are much more worried about armed victims in the homes then they are about the police. In interviews about why they did not break into a house when someone was home, the recurring them among criminals was: *"that's the way to get shot."*[15] While these examples demonstrate that people do weigh costs and benefits to criminal decisions, it is obvious that the challenge lies with understanding the internal, personal value system of the criminal, which varies from individual to individual. The RAM provides a very good theoretical model from which to work, but is not sufficient to address all known variables.

When considering crime, studies indicate that deterrence does play a role. As stated by Lott:

> *"Overall, my conclusion is that criminals as a group tend to behave rationally when crime becomes more difficult, less crime is committed. Higher arrest and conviction rates dramatically reduce crime."*[16]

This is consistent with research that shows that, in general, non-violent criminals and those seeking monetary rewards are more likely to qualify as rational actors. It is then logical that cybercriminals,

---

[13] Naji, Abu Bakr. *The Management of Savagery, the Most Critical Stage Through Which The Umma Will Pass.* Translated by William McCants, http://www.wcfia.harvard.edu/olin/images/Management%20of%20Savagery%20-%2005-23-2006.pdf P 106

[14] Jackson, Brian A.; Morral, Andrew R. (Dec 7, 2009) *Understanding the Role of Deterrence in Counterterrorism Security.* RAND Corporation. Kindle Edition. (Kindle Locations 111-117).

[15] John R. Lott Jr. *More Guns, Less Crime: Understanding Crime and Gun Control Laws, Third Edition* (Studies in Law and Economics) University of Chicago Press. Kindle Edition. (Kindle Locations 135-138).

[16] Lott, 2011

generally drawn by monetary greed, may be classified as rational actors. For this reason, it is suggested that the use of deterrent strategies would have a predictable impact on cybercrime.[17]

3 Components of Deterrence

For any form of deterrence to be effective, it must be based upon the three principles of certainty, celerity, and severity. Certainty applies to the criminal's **belief** in the likelihood of the threat (whether arrest, punishment or retribution) being carried out. Studies suggest that a certain, consistent level of certainty must be achieved to produce desired consequences. In short, if a law is all bark and no bite, the threat of a bite will have no impact on the cost benefit analysis. Logically, if a criminal perceived a certainty of retribution, the criminal would calculate the risk of the crime differently than if they felt it was unlikely the threat would be carried out. The result is a greater deterrent effect.

Celerity applies to the promptness of the threat being carried out. If there is the threat of immediate action as opposed to the threat of action at some point in the distant future, the deterrent will have greater effect. Even if the likelihood of the punishment is 100%, if there is no immediate threat of retribution, there will be a decreased level of deterrence. This can be seen in the statements of the criminals interviewed about "hot" burglaries where they indicated a fear of immediate retribution in the form of an running into angry, armed homeowner during the course of the burglary more than they feared eventual arrest and punishment.

Finally, the severity of punishment is critical to any deterrent. Most are probably familiar with the statement: *"the punishment must fit the crime".* The increase in severity has a correlation to the effectiveness of the deterrent. In short, the greater the severity of the action, the less likely the prospective criminal is to perpetrate the act. An easy way to show the correlation is through the traditional model of risk analysis.[18]

Categories of Deterrence

Deterrence theory relies upon the rationality of actors to be effective. Criminal justice proposes two broad types of deterrence; general deterrence and specific deterrence. Both types of deterrence have application for cybercrime.

---

[17] Turrini, Elliot (2010) "Increasing Attack Costs & Risks and Reducing Attack Motivations," *Cybercrimes: A Multidisciplinary Analysis.* Ghosh and Turrini, eds. Springer-Verlag. Pp365-375

[18] http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=27596

General Deterrence

General deterrence is proactive and attempts to target potential crimes *before* they are committed. Examples of general deterrence may include "no trespassing" signs warning that trespassing is a crime and stating the particular law and penalty. It is likely that most readers are familiar with the posted signs in post offices that warn of the *"…minimum of 15 years in federal prison for robbing a post office."* For those who have travelled to Singapore, a form of general deterrence to drug trafficking is the very obvious sign that warns people entering the country that trafficking in drugs is punishable by death. Additionally, the passing of laws with increasingly stiff penalties for data theft would be an example of general deterrence. If general deterrence was entirely effective data theft would be trending downward instead of increasingly sharply year after year. Clearly, general deterrence has its limitations in cybercrime.

Specific Deterrence

Specific deterrence, on the other hand, is reactive and is focused upon punishing those that perpetrate crimes. Arrest and conviction provide specific deterrence to crimes. The concept of "The punishment should fit the crime" is an example of specific deterrence in action. Another example of specific deterrence is the use of armed guards on ships traversing pirate infested waters of the Gulf of Aden. Not only do the armed guards provide protective value the pirates must consider the immediate consequences of being wounded or killed if they attempt a hijacking. Evidence of the value of the deterrent effect of armed guards can be seen in the fact that not a single armed vessel has been hijacked. Clark proposed that: *"offender's calculus is mostly based on that which is most evident and immediate, while neglecting the more remote costs and benefits of crime or its avoidance*[19]*."*

The US National Academy of Sciences established a panel in 1978 to study the various academic studies of deterrence. It found that:

> *"Taken as a whole, the evidence consistently finds a negative association between crime rates and the risk of apprehension, conviction, or imprisonment…the evidence certainly favors a proposition supporting deterrence more than it favors one asserting that deterrence is absent."*[20]

[19] V. Clarke, "Situational Crime Prevention: Its Theoretical Basis and Practical Scope," *Crime and Justice* Vol. 4 (1983): Issue 1. Pp 225-256.
[20] Lott Jr. 2011 Kindle Edition. (Kindle Locations 135-138).

To be effective as a specific deterrent, the criminal must believe that he or she will be caught, be prosecuted, and be sentenced to a term that increases the risk to a point that criminal behavior changes. Certainty, celerity, and severity are critical when discussing specific deterrence.

Risk Analysis & Expected Utility

To understand and apply the concept of deterrence, it is first necessary to analyze the "rational" behavior of a person or group who acts in a manner that most law abiding citizens considers 'irrational' It is also necessary to have a working understanding of the concept of risk since people, criminals included, employ an internal decision calculus based upon risk & reward to influence their decision making.

Experience demonstrates that risk is a topic that is frequently discussed but often not well understood or properly applied with respect to information security. While often this analysis may not be a conscious or intentional, it is applied when making decisions. From deciding whether to walk down a dark alley to deciding upon a particular financial investment, people deal with risk on a daily basis and analyze risk numerous times per day. However, applying risk management to information security often proves complex. To better understand its application in the realm of information security and understanding of general risk management is helpful.

Basic Risk Modeling

Risk is commonly described as the probability or likelihood of a known loss. Risk can be quantified or qualified. For the purposes of this paper, it is useful to quantify risk simply to demonstrate the value of deterrence. This paper will define Risk as a function of the following:

The likelihood of an *Event* occurring and the resulting *Impact* should the event occur.

A simple method of quantifying risk is to multiply the likelihood of an event occurring in a given time frame (expressed as a probability) by the expected impact should the event be realized.[21] The calculation for an annualized loss can thus be expressed as:

(% of Event A occurring) X ($ Impact should Event A be realized) = Annualized Loss Expectancy (ALE)

[21] The general Annualized Loss Expectancy (ALE) model has been modified for the purposes of the paper.

Assume there is a 5% probability that an event (a home fire) will occur in a given year and the estimated damage will be $10,000. In this scenario the Annualized Loss Expectancy (ALE) is calculated at $500 per year (5% x $10,000). A person would be well served to consider insurance or other risk management controls that did not exceed $500 per year. These types of models are often used by insurance underwriters to calculate premiums and coverage. Obviously, this type of model is too simple to analyze decisions where the losses and probabilities are subjective.

Advanced Risk Modeling

The US Department of Homeland Security expands on the basic risk model by defining risk as the function of threat, vulnerability, and consequence (R = T x V x C) where risk is the expected loss, threat is the probability an adversary will attack, vulnerability is the probability an attack will succeed, and the consequence is the outcome or the loss.[22]. As with the basic model, the DHS model is deficient to define risk where human rationality subjectively defines the inputs.

The Subjective Expected Utility (SEU) is a risk model that has come to the forefront of Rational Deterrence Theory. The SEU is also a variation of the basic risk model but enables the analyst to view risk from the perspective of the criminal and accounts for the subjectivity of perceived probability and outcome or utility of a decision. First, the SEU ascribes a value to the actor of the consequences of a course of action, which is then modified by a *subjective expected probability* of that outcome occurring.[23] SEU= p(u), where p= subjective probability, u=subjective utility. If one replaces "consequence" with subjective utility in the DHS model, it is easy to see that the study of "utility" is similar to that of risk. Consider two adversaries. One adversary is predicting the risk that the other will take some adverse action and is evaluating controls to mitigate the risk. The other party is predicting the utility of their action against the adversary in light of the controls that the person believes are in place. A more relevant example can be seen in the case of a bank robber and a bank. The bank is analyzing the risk of being robbed by a bank robber and is considering controls to put in place to mitigate the risk. The bank robber, on the other hand, is considering the controls in place, the consequences of getting caught, the possibility of being shot by an armed guard, and is evaluating the *utility* of robbing the bank. If the bank robber estimates that the personal utility is high enough (greater reward than risk) then the robber may embark on the crime.

[22] Department of Homeland Security. (2008). "DHS risk lexicon." Retrieved from www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf
[23] Taquechel, (2012) Kindle Edition. (Kindle Locations 561-563).

As described previously, the theory of rational choice assumes that an actor (in this case a criminal) will attempt to maximize the expected utility, which is subjective. For this reason, the SEU will vary depending upon actor's risk tolerance and emphasis on loss or gain.[24] Preferences among the courses of action are determined by two separate factors: 2) strength of preference for the consequences under certainty, and 3) attitude toward risk.[25]

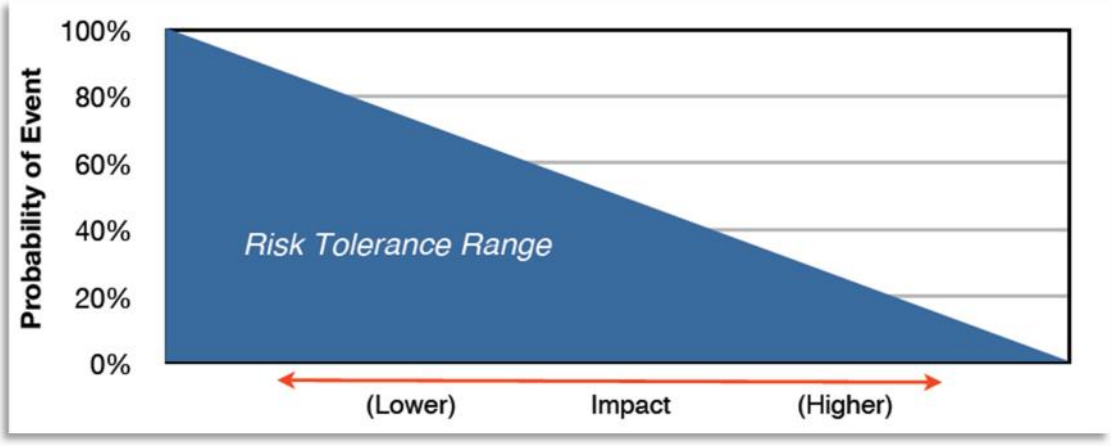
Understanding Risk Tolerance

Risk tolerance describes the threshold of risk that a person is willing to tolerate given the potential 'payoff' or utility if the act is successful. In short, it is the risk the criminal will accept in light of the utility of their choice. Going back to a previous statement, there is no single value calculus for all people. That being said, it becomes a bit easier to divine motives when discussing criminal behavior. It is worth repeating a statement from a previous section. Research shows that, in general, non-violent criminals and those seeking monetary rewards are more likely to qualify as rational actors. It is then logical that cybercriminals, generally drawn by monetary greed, may be classified as rational actors.[26]

While criminal behavior motivated by monetary terms may be easier to predict, behavior that is driven by ideology (terrorism, insurgency, and activism) is much more difficult to analyze as it relies upon a personal perception of value.

When discussing crime that is driven by money, in general it can be assumed that if there is a high potential payoff and there is a high likelihood of an event occurring but there is little impact (consequence), the willingness to tolerate the event is high. Similarly if there is a high potential payoff and a low likelihood of an event occurring, yet a greater impact, the willingness to tolerate the impact is also high. If the likelihood increases relative to the impact or the impact increases relative to the probability, then the tolerance decreases. The tolerance to risk increases with the potential payoff. The old adage: "high risk, high reward" is very relevant when considering risk tolerance and deterrence.

[24] Lebow, R., & Stein, J. (1989). "Rational Deterrence Theory: I think, therefore I deter," *World Politics, 41*, Pp 208–224.
[25] Shoemaker, P. (1982) "The Expected Utility Model; Its variance, purposes and limitations," *Journal of Economic Literature*, 20 Pp 529-563
[26] Stanely, Richard (2006) "Information Security," *Cybercrimes; A Multidisciplinary Analysis* .Ghosh and Turrini, eds. Springer-Verlag. P 201



Crime & Criminal Behavior

Criminal science, as one can imagine, often proposes theories related to criminal behavior. While there is debate on the socioeconomic causes, mental predisposition, and other aspects of crime, evidence still supports the theory that 1) criminals act rationally and in their own self-interest and 2) an opportunity for crime must be present. The various theories of criminology are not mutually independent and often overlap.

Individual Behavior

Understanding deterrence and rational choice is about understanding human behavior. People do not behave consistently in all environments and at all times. Certainly, moral and ethical relativism play a role in individual behavior. People that state unequivocally that they would never steal, have likely never been in a situation in which their child was starving. While an extreme example, it highlights the variability of individual behavior. Individual behavior can be described as a function of the person and their environment. This is commonly known as Lewin's equation and can be expressed as Behavior= function (person, environment) or B= f(P,E).[27] While a heuristic and not a mathematical model, it is intuitive to the user. The person, as described in the model, includes all aspects of the person that relate to their ethics, morals, and beliefs, to name but a few characteristics. Some people will be naturally more inclined toward violence if presented with the right situation. It should be noted that there is a distinct difference between a person that **is** violent and a person that **has the capability for** violence under specific circumstances. In much the same way, each person has a threshold for various

[27] Gibbs, Stephen (February 2012) "Applying the Theory and Techniques of Situational Criminology to Counterinsurgency Operations: Reducing Insurgency Through Situational Prevention" Kindle Edition (Kindle Locations 100-105).

crimes that is part of each individual's moral and ethical compass. Few people (this author included) would not consider stealing food to keep their own child from starving to death. Some people are naturally more inclined toward stealing and have a lower threshold under which they would resort to theft. In short, personal behavior is a function of the person's own ethical and moral beliefs within a specific environment.[28] It is this understanding of behavior coupled with rationality that allows for the predication of behavior and crime. In a simpler sense, crime can be explained as the *interaction between disposition and situation*.[29] Disposition refers to the natural inclination to commit crimes under certain circumstances and situation refers to the environment and opportunity that is presented to the person. If there is a disposition toward crime given a certain situation and that situation is presented, then criminal activity can be expected.

Situational Crime Prevention

Situational crime prevention is a theory that encompasses three approaches to crime prevention and is well suited to discussing cybercrime. Routine Activity Theory, Crime Pattern Theory, and Rational Choice Perspective are each considered opportunity theories. The specific goal of Situational Crime Prevention is to address specific crimes by managing, designing, and manipulating the environment in a manner that seeks to increase the risk to the offender, while reducing the offenders reward for committing the act.[30] Building on the concepts presented to this point, situation crime prevention attempts to deter the criminal behavior by reducing the utility of the act or modify the opportunity which in turn reduces the utility to the potential criminal and deters the act.

Rational Choice Theory

As can be seen in this paper, rationality, and rational decision making is a recurring theme of deterrence and crime prevention. Rational choice theory simply applies the rational choice model to criminal behavior. As stated previously, rational choice assumes that a person (or criminal in this case) will act in a rational manner to maximize their benefit. Clarke theorized that the *"offender's calculus is mostly based on that which is most evident and immediate, while neglecting the more remote costs and benefits*

[28] Gibbs; 2012
[29] Gibbs; 2012
[30] Gibbs; 2012

of crime or its avoidance[31]*."* In short, criminals will calculate the immediate reward against the immediate risk when calculating when to commit a crime. This is consistent with Lott's assertion that, when asked why they did not break into houses when people were home, burglars in the US stated: *"that's the way to get shot."*[32] It is interesting that the burglars did not state that if caught, they might face a longer prison sentence. It was the immediate threat that impacted their decision making. This is also consistent with deterrence concept of celerity. People weigh future costs differently than immediate costs and, as such, immediate costs impact the decision calculus to a greater degree than future costs.

Crime Pattern Theory

Crime pattern theory suggests that criminals look for and find criminal opportunities during the course of their daily lives. As stated in Gibbs: *"Crime pattern theory argues that opportunities for (Crime) does not always occur randomly; (criminals) often search for an create these opportunities."*[33] Crime pattern theory also provides insight into how criminals evaluate the opportunities and choose to act upon them. Crime pattern theory would appear less applicable to cybercrime because it relies upon physical proximity in order to estimate criminal activity. In today's interconnected world, a criminal in Kazakhstan is as dangerous to a company trying to protect their data as a criminal next door. In short, opportunity for criminal behavior abounds on the Internet. This creates a number of issues related to deterrence.

Routine Activity Theory

Routine activity theory states that for crime to occur, three things must be present. 1)a likely offender, 2)a suitable target, 3)the absence of a capable guardian. The routine activity theory is commonly shown as a triangle.

[31] Clarke; 1983
[32] Lott; 2011
[33] Gibbs: 2012

Since all three elements must be present for a crime to occur, then removing one element will prevent or reduce crime. While this is described in three components, it is easy to fit it into the previous description *of crime = disposition + situation*. In this case the likely offender refers to the person with the disposition and the situation refers to the target and absence of a suitable guardian. Regardless of how you view crime prevention it comes down to two components, people and opportunity. With an understanding of basic crime prevention, it is not possible to put all of the pieces together with an eye toward understanding the challenges of preventing cybercrime.

Putting it all Together

At the risk of oversimplifying the work of criminologists, most relevant crime prevention theories can be distilled into two basic concepts. The first concept applies to controlling or modifying the environment to reduce opportunities for crime and the second concept is the influencing of human behavior to make a criminal act less attractive to a would be offender. This can be further distilled into the basic ideas of ***crime prevention = protection + deterrence***. Protection refers to the security controls that are applied to increase the difficulty of committing a crime. This, in turn, reduces the utility of the act to the criminal and changes the risk/reward calculation. Security is often described as 'hardening' of targets by implementing controls that increase the level of difficulty of perpetrating a crime. This has the effect of increasing the cost to the criminal by requiring more resources (time, skills, money, etc.). When used with a deterrent such as an alarm that would notify policy, it could also be perceived as increase the risk associated with the effort. By applying protective measures the utility to the criminal is reduced and it has a deterrent effect as the payoff may not justify the investment of time and effort required to circumvent the controls. A vault is a good example of a protective measure. While no vault is completely impenetrable, vaults do provide significant protective value. Firewalls, encryption and other

controls are considered 'protective measures'. While protective security measures are critical, they are only one prong of the solution. As stated in the Transportation Security Administration's report:

"The impracticality of eliminating all transportation vulnerabilities means the efforts to deter must be a key part of transportation security strategies"[34]

As discussed at length in this document, deterrence is critical to preventing criminal. Without deterrence, people and companies are at the mercy of the criminals. Time and effort have no real meaning without deterrence. Imagine a bank robber that knew that the police would not come to the bank after the alarm was tripped. Instead of focusing on robbing the bank and getting out within 2 minutes, the bank robbers could simply sit the bank casually taking their time to collect as much money as possible. A major component of a bank's risk management strategy is the belief that the police will come if an alarm is tripped. If the deterrence of the police were removed, the bank would be in the position of building, to quote the CEO of RSA; "*…the biggest, fiercest defenses possible to keep attackers out."*[35] Companies operating today face the same sort of dilemma. The value of their data is great enough that criminals are willing to invest the time and effort in circumventing the security controls. As RSA demonstrated even companies with world class expertise and large security budgets will be compromised if the criminals invest enough time and resources.

The Failure of CyberCrime Prevention

A review of the Verizon data, as well as numerous other resources show that the number of network intrusions and data thefts have increased sharply year over year. Research shows that, in spite of increased controls, companies continued to be victimized at alarming rates. Cybercriminals are attacking companies with apparent impunity. While some argue that the fault lies with the companies being hacked, this is a dangerous position to support. Blaming the victim of a violent crime for being victimized is deplorable. Why should companies be treated any differently?

[34] Jackson, Brian A.; Morral, Andrew R. (2009-12-07). "Understanding the Role of Deterrence in Counterterrorism Security," RAND Corporation. Kindle Edition (Kindle Locations 111-117).

[35] Cowley; 2012

Laws, Regulations & Enforcement

International cybercrime presents an interesting challenge for law enforcement. Laws in the US have not kept pace with the crimes being committed only and, more challenging, US laws have little, if any jurisdiction outside of the US.

Jurisdictional Issues

Compounding the problem is the debate over which law enforcement agency in which country even has jurisdiction over a crime committed in the US, by a Ukrainian using an IP in Thailand? Another example is that of a country without cybercrime laws. The purpose of this paper is not to debate the legal jurisdiction over cybercrimes rather to illustrate the challenges with enforcing laws over the Internet.

Law Enforcement

Numerous research studies have demonstrated the value of a police presence in crime prevention. Even the theories underpinning Situational Crime Prevention discuss the need for a 'capable guardian'. A police presence reduces crime in high crime neighborhoods as the perceived likelihood of arrest increases relative to the proximity and number of law enforcement officers. " As stated by Davis: "*When comparing nearby neighborhoods with similar characteristics, crime is lower where arrest rates are higher…"* The point is further confirmed by Florida State University Law Professor and Economist Jonathan Click in his study on policing and crime:

> *"We found that the additional police had a pretty big effect on crime," Klick said. "Our local and federal governments spend tons of money on policing, and it looks like we may be justified in spending much more."*[36]

Unfortunately, even if effective law existed and no jurisdictional issues existed, the simple fact remains that there is no way to 'police' the internet and gain the benefits of a 'police presence'. While a bank robber is limited to banks that he or she can physically rob, the virtual nature of the Internet allows a cybercriminal to attack a company anywhere in the world. This means that while police can patrol "high crime" physical neighborhoods, they cannot patrol the Internet.

[36] Elish, Jill. (June 24, 2005) "More cops on beat reduce crime on street, FSU study shows"; online http://www.fsu.edu/news/2005/06/24/more.cops/

Compellence & Blaming the Victim

Challenges with law enforcement over the Internet have created a situation in which regulators, industry personnel, and others have turned to compelling companies operating online to adhere to increasingly strict controls in an attempt to keep the criminals at bay. A review of the 46 state breach notification laws, as well as the penalties for non-compliance with HIPAA/HITECH, the PCI DSS, Minnesota Plastic Card Security Act and other regulations demonstrate that the trend is toward compellence of the victim to prevent crime and not deterrence of the criminal from committing crime. Regulators and others appear to have thrown up their hands and resigned themselves to the fact that they cannot deter the criminal behavior so, instead, they will compel companies to adhere to increasingly strict data security requirements. Certainly, there is some value in this position as the laws apply to companies that are handling PII but the sole focus on the companies while ignoring the criminal is a dangerous trend.

An unfortunate result of the increasing regulation is the trend toward blaming the victims of cybercrimes. Quick review of the opinions and comments put forth by various experts demonstrate that when a company is victimized by criminals, the reaction is to blame the company for not being 'adequately secure'. Companies that have been targeted by organized crime groups, state sponsored hackers and sophisticated hacktivists can attest that one a company is targeted, it is simply a matter of time before the criminals successfully penetrate the network and access the information they after.

Expanding upon the bank example used in this document; if a bank is robbed the bank is not blamed for the robbery. If the same bank has their network breached and customer data stolen it is blamed for the penetration and inability to keep the hackers at bay.

The "Substitution Effect"

The lack of effective criminal deterrence is a problem for all companies operating online. An individual level, any company can be targeted and, if the pay-off merits the dedication of sufficient effort and resources, will eventually be hacked and their data compromised. Another phenomenon that needs to be considered is that of the substitution effect. The substitution effect is the move from one crime to another or one neighborhood to another when the desired crime or desired opportunity is no longer a

viable alternative. This effect was astutely recognized by the Verizon forensic investigators when they wrote:

> *"Criminals may be making a classic risk vs. reward decision and opting to "play it safe" in light of recent arrests and prosecutions following large- scale intrusions into Financial Services firms. Numerous smaller strikes on hotels, restaurants, and retailers represent a lower-risk alternative, and cybercriminals may be taking greater advantage of that option."*[37]

The unfortunate result is that even if some form of deterrence is enacted, criminals will simply shift targets and attack those that present a greater opportunity and reduced risk.

Summary

Cybercrime is a growing threat for all companies operating online. Since 2000, cybertheives have targeted financial data, intellectual property, and personal data. While the news will identify the odd criminal that is brought to justify for a major data breach, the percentage of criminals that are caught and prosecuted is alarmingly low. In an effort to stave off the onslaught of cybercriminals, regulators, industry bodies, and others have taken the approach of placing the burden of not being victimized squarely onto the shoulders of the companies that are being targeted with little, if any effective effort at deterring the criminals perpetrating the crimes The end result is an environment where penalties are applied to compel compliance with increasingly stringent data security rules while little is being done to bring the criminals to justice or otherwise deter their behavior. The unfortunate result is that cybercrime will continue to increase for the foreseeable future while the very companies being targeted will continue to be blamed for their lack of security. This is the failing state of information security today.

[37] Verizon (2011) "2011 Data Breach Investigations Report: A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit." http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cts=1330986211332&ved=0CEEQFjAA&url=http%3A%2F%2Fwww.verizonbusiness.com%2Fresources%2Freports%2Frp_data-breach-investigations-report-2011_en_xg.pdf&ei=ND5VT77QCujZiQL54-m0Bg&usg=AFQjCNGOtUxthsm_nlzOK8lLCJYy6Fvbkw&sig2=e3jgQMFFl8HpdqK_iEGtEQ

About The Authors & Mark Consulting Group

Chris Mark is the founder and principal consulting of The Mark Consulting Group, Inc. He is a recognized payment security expert and risk management professional. He is the former founder and CEO of the two data security companies, experienced executive, and has worked for both MasterCard and Visa on their respective data security programs. Chris has conducted payment security and risk management training globally on behalf of Visa and the PCI SSC and trained over 10,000 people globally. He is the founder of the Society of Payment Security Professionals (SPSP) and led the development of the Certified Payment-Card Industry Security Manager (CPISM) and Certified Payment Card-Industry Security Auditor (CPISA) certifications. He is Certified Information Systems Security Professional (CISSP), Certified Information Privacy Professional (CIPP), has various technical certifications and also holds MBA and BA degrees. Chris has published numerous articles on risk, risk management, regulatory compliance, PCI DSS, and information security and is a frequent speaker on the topics of payment card security and risk management. Chris publishes a risk management blog at: www.GlobalRiskInfo.com

Chris is a former enlisted US Marine and US Navy Officer. He is a qualified Marine Infantryman (0311), Scout/Sniper (8541) and Reconnaissance Marine (airborne/scuba qualified) (8654) and a former Reconnaissance Instructor. Chris is a combat veteran of Operation Continue Hope and has attended numerous military training courses.

About Mark Consulting Group

The Mark Consulting Group was founded to provide expert, professional consulting, information services, and training to clients of all sizes. Mark Consulting has deep experience as business owners, executives, consultants, and researchers. Some of the services Mark Consulting Group can provide include:

- Content Development (Whitepapers, datasheets, blog posts, website content, and more)
- Market and/or competitive research
- Product Development & Support
- Information Assurance & Privacy Consulting (PCI DSS, GLBA, SB1386, etc.)
- Marketing & Branding Support
- Professional Speaking

- In House Training

Mark Consulting can provide expert, outsourced information services as well as strategic consulting to your company. If you have a need to demonstrate expertise through the publication of articles, whitepapers, blogs, public speaking, training, or other media, Mark Consulting can help. Numerous companies today take advantage of our "ghostwriting" content development services.

Email: chris@markconsultinggroup.com

Phone: 435-513-0484

www.markconsultinggroup.com

www.globalriskinfo.com