Digital Investigation (2005) **2**, 261—267

ELSEVIER

Digital Investigation

www.elsevier.com/locate/diin

Criminal profiling and insider cyber crime

Nick Nykodym*, **Robert Taylor**, **Julia Vilela**

Management Department, College of Business Administration, University of Toledo, OH, USA

KEYWORDS
Legislative compatibility;
Profiling;
Cyber crime

Abstract On a global scale, cyber crime has skyrocketed with the advancement of the electronic medium. While progress is being made in combating cyber crime (particularly with the Council of Europe's Convention on Cyber Crime), a large gap continues to exist in legislative compatibility across international borders. Often overlooked in regard to profiling is cyber crime. The idea that an individual committing crime in cyberspace can fit a certain outline (a profile) may seem far-fetched, but evidence suggests that certain distinguishing characteristics do regularly exist in cyber criminals. This can be particularly useful for companies (the most often hindered victims of cyber crime) attempting to do away with cyber criminals inside their own walls (the most common type of cyber criminals). Whether they are simply breaking company policy by browsing the Internet while on the clock or embezzling thousands of dollars through the company's network, insiders are a very real problem that companies spend millions of dollars annually to prevent. An accurate profile of an inside cyber criminal may help in identification both prospectively and retrospectively.

History of profiling

The profiling of criminals dates back to the 15th century. The investigative technique's path through history has been, at times, poorly documented and marred with occasional inaccurate findings and prejudices. As many adversaries as the method seems to have, however, there exists strong instances throughout history in which the process has produced incredible results that demand attention and consideration. Today, profiling takes a very different form than it did in the 1400s. Since the 1970s the United States Federal Bureau of Investigation has recognized criminal profiling as an official field and has advocated its use in retrospective analysis. While opinions differ on the most effective profiling process, real world instances have proven that criminal profiling can be helpful and can lead to accurate arrests. Alone however, profiling is completely useless and potentially dangerous: it must be combined with detailed case analysis, accurate information and demographics, precise crime scene investigation, and reliable records and statistics to provide its true worth.

* Corresponding author.
E-mail address: nick.nykodym@utoledo.edu (N. Nykodym).

1742-2876/$ - see front matter © 2005 Nick Nykodym, Robert Taylor, Julia Vilela, University of Toledo, Ohio. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2005.11.004

The acknowledged account of profiling can be traced back to the 1400s,[1] when the fear of witches and a strong demand for a system of identifying them, led to the publication of *Malleus Maleficarum*, which came to serve as an outline for recognizing witches.[2] Through the ages the field of profiling and identifying criminals based upon distinguishable characteristics has taken many forms and has evolved greatly. From the 18th century studies of Franz Gall[3] and the eventual development of the field of cranioscopy (Phrenology): the belief and study that a person's psychological aspects (including criminal inclinations) could be assessed by examining the bumps and depressions on the skull, and the fingerprint identification system influenced by Galton in the late 1800s,[4] to the release of the *Criminal Man* in 1876 great study has gone into what makes criminals different from the law abiding men and women.

Modern criminal identification systems can be traced to the notorious case of Jack the Ripper. Dr. Thomas Bond investigated the case and applying psychology to profile the perpetrator and assess the scene, exceeded the limits of profiling during this era.[5] His intuitive skills were so precise that he had even pinpointed physical characteristics (neatly dressed, middle-aged, harmless looking, etc.) of the perpetrator, and accurately reconstructed his personal environment (reserved, eccentric, living in respectable surroundings, etc.). In the late 1950s, psychiatrist James Brussel took a psychoanalytical approach to profile the ''Mad Bomber''. After reviewing the evidence and other facts, Dr. Brussel provided authorities with a profile to work with: the bomber is an educated eastern European male between 40 and 50 years old. He is an unmarried, paranoid personality type probably living with a female relative. His physique is neat, clean-shaven, with a muscular build. Because he is a detail-oriented person, he resents criticism and feels he is superior to others. Brussel concluded, ''When you catch him, he'll be wearing a double-breasted suit — buttoned''.[6] Surprisingly, this was one of the first and last times that this psychoanalytical approach was employed.

By the end of the 1970s, the Federal Bureau of Investigation had officially recognized 'criminal profiling' as an official field and had introduced Applied Criminology as a permanent course at the FBI Academy.[7,8] Between 1979 and 1983, correction facilities were visited on the account of interviewing incarcerated felons.[9] Questions were asked about the crimes committed, the victims, background information (both the criminal and the victim), the meditation behind the crimes, etc. They also studied court transcripts, police reports, criminal records, and psychiatric reports of the perpetrators' behavior.

Today's profiling process takes two approaches: Prospective and Retrospective. Prospective profiling attempts to create a ''template'' of a specific type of offender (for example: a terrorist, a child molester, or a serial murderer) based on the characteristics of previous offenders. These Prospective profiles are then held over a specific population in order to attempt to narrow down and predict who will commit these specific types of offenses. This type of profiling often receives tough criticism because it is often overly inclusive and may lead to suspicions against innocent people. The antithesis of Prospective profiling and the type of profiling used most often by the FBI is Retrospective profiling. This approach is after the fact and case specific. It attempts to use the clues left behind by a specific criminal to develop a specific description of that person. The idea is to link a specific person or persons to a specific crime (or series of crimes) that have already occurred based on personality and behavioral characteristics that have been identified through analysis of the crime scene and the facts of the case.[10]

In the 1990s, profiler Brent Turvey met with and interviewed an incarcerated serial killer after extensively reviewing crime reports, court transcripts, and court records. After the interview, Turvey compared his verbal interview with evidence from the records. Nothing matched! Turvey couldn't comprehend how the prisoner's

[1] Woodworth M, Porter S. ''Historical foundations and current applications of criminal profiling in violent crime investigations''. *Expert Advice* 1999;*7*:241—64.

[2] Kramer H, Sprenger J. *Malleus Malificarum*. New York: B. Blom; 1970.

[3] Wickepedia. ''Franz Joseph Gall''. Jan. 05. Online Posting. Wickepedia.org. Accessed: January 21, 2005, <http://en.wikipedia.org/wiki/Franz_Joseph_Gall>.

[4] Gall S, Beins B, Feldman A. *The Gale Encyclopedia of Psychology*. Detroit: Gale; 1996.

[5] North Carolina Wesleyan College. ''History of Profiling''. December 19, 2003. North Carolina Wesleyan College. Accessed January 24, 2005, <http://faculty.ncwc.edu/toconnor/428/428lect01.htm>.

[6] Pinizzotto A. ''Forensic psychology: criminal personality profiling''. *Journal of Police Science and Administration* 1984; 12:32—40.

[7] Op cit note 1.

[8] Petherick W. ''Criminal Profiling''. *Crime Library* 1999; 15 May 2001.

[9] Op cit note 8.

[10] McCrary Gregg. The unknown darkness: profiling the predators among us. New York: Morrow; 2003.

statements could be so contradictory to the information in the crime reports until he realized that the perpetrator was purposely misconstruing the facts to redirect the responsibility of the crime. Turvey's approach, called Behavioral Evidence Analysis (BEA), relies more on an intuition than past approaches.

Behavioral Evidence Analysis consists of four steps within two phases (Turvey, 1997 as cited in Petherick, 1999).[11] Step one is called the *Equivocal Forensic Analysis*. This step involves evaluating the evidence. Although the significance of the evidence is most likely ambiguous, the examiner must interpret the most probable meaning of the data. This step employs an unlimited number of sources from which to collect data.

Step two, *Victimology*, is assessing the victim. Profiling the victim could be the primary source of information that could lead you straight to the perpetrator.[12] If the victim was killed during the attack, this step will be used to create an accurate make-up of the victim. By determining characteristics of the victim, a profiler can use this information to determine characteristics of the offender. For instance, if the abduction of the victim doesn't show a struggle, perhaps the victim knew or trusted the offender.

Step three is known as *Crime Scene Characteristics*, and is quoted as ''the distinguishing features of a crime scene as evidenced by an offender's behavioral decisions regarding the victim and the offense location, and their subsequent meaning to the offender''.[13] This step encompasses the perpetrator's approach to the victim, the location of the crime scene, many other elements of the crime venue, and where the crime took place in comparison to other crimes. There may be a strong possibility that the majority of the crime took place at a site that had some sort of significance to the offender.

The final step is known as *Offender Characteristics*. This step consists of assumptions of the offender's personality and behavioral characteristics based on the following collected information. Characteristics defined in this stage include: physical build, offender sex, work ethic, mode of transportation, criminal history, skill level, race, marital status, passiveness/aggressiveness, medical history, and offender residence in relation to the crime.[14] Collectively, these data could reduce or increase the number of suspects.

The assumptions from these four steps can be applied in the two phases of the BEA, known as *The Investigative Phase* and *The Trial Phase*. Turvey explains the objectives of the Investigative Phase, aka the 'unknown offender for the known crime' phase, as:

- Reducing the suspect pool in a criminal investigation.
- Assisting in the linkage of potentially related crimes by identifying unique crime scene indicators and behavioral patterns.
- Assisting in the assessment of the potential for escalation of nuisance criminal behavior to more serious or more violent crimes.
- Helping keep the overall investigation on track and undistracted.
- The Trial Phase is also known as the 'known offender for the known crime.' The objectives of this phase are listed below.
- To assist in the process of evaluating the nature and value of forensic evidence to a particular case.
- To assist in the process of developing interview or interrogative strategy.
- To help develop and gain insight in offender fantasy and motivations.
- To help gain insight into offender state of mind before, during, and after the commission of a crime.
- To help suggest a crime scene linkage by virtue of modus operandi (those things the perpetrator had to do to commit the crime) and the signature behavior (those things the perpetrator did not have to do to commit the crime, which usually fulfill a physical or psychological need).[15]

The BEA is not reliant upon statistics.[16] This method is the circumspect analysis of the event, the victim, the perpetrator, the scene, and the psychological make-up of all persons involved. This method is extremely time-consuming and is based on intuition and acquired skills attained through thorough training.

Although criminal profiling seems to be a specific term, there are many methods of profiling. Many successful profilers have their own methods to solve crimes, but no two methods are exactly the same. Profiling has come a long way and has evolved to encompass all aspects of a crime. While the term 'profiling' has come under heavy scrutiny recently, particularly since the 2001 attacks

[11] Op cit note 8.

[12] Op cit note 8.

[13] Op cit note 8.

[14] Op cit note 8.

[15] Op cit note 8.

[16] Op cit note 8.

against the United States, work in its field continues to evolve and is still employed today.

Cyber crimes against business

Cyber crime is a hot topic of the 20th century. The world stands at a crossroads for developing defense mechanisms against it. Cyber crime by its most general definition can be any crime committed over a computer network.[17] These crimes have been occurring since the creation of the Internet. If there is information to be shared, there is information to be sabotaged. The challenge is faced by every online individual, company or organization across the globe. Internationally, progress against cyber crime is haltered by the fact that governments around the world are imposing different and often conflicting legislation to deal with what is a global issue.[18] Progress is being made; the Council of Europe's Convention on Cyber Crime has taken significant steps toward creating a treaty intended to establish international standards for combating cyber crime. However, a great deal of work remains in creating global acceptance and ratification of the treaty.[19]

In particular, cyber crime against business is growing. The reported total loss from cyber crime increased annually in 2000, 2001, and 2002 to $265 million, $378 million, and $450 million, respectively.[20] Additionally, the total loss from 1997 to 2002 reported to the authorities is almost $2 billion.[21] The very way that business is now conducted nourishes the growth of cyber crime. One European survey points out that 43% of over 3000 surveyed companies, organizations and government agencies believe that cyber crime will be the biggest and most damaging class of criminal activity in the future.[22] The increasing role of Internet sales, the massive amount of data transferred through the computerized information systems inside and outside organizations, much of which is very sensitive and is related to the core of business; the immense use of the Internet in the workplace; and increased access to confidential information, are all factors that contribute to the growing threat of cyber crime.[23]

A major element of cyber crime, which accounted for $170 million of loss in 2002, was theft of proprietary information: customer databases; product databases; R&D data; etc. And while the total loss in 2002 was 28 times more than the total loss for 1997, the number of respondents reporting any loss had grown by only 24% for the same period of time.[24]

One logical explanation is that the perpetrators are getting better equipped and have more knowledge. An additional factor is that organizations are putting more value on the information nowadays than few years ago. The value of the information has increased and organizations have recognized it: the information being stolen is ''worth more'' today than in the past.

Insider cyber crime and abuses

Insider abuse of Net access and unauthorized insider access are two concerns for employers. While insider abuse of net access went up to US$50,099,000 from US$35,001,650 in 2001, the unauthorized insider access decreased to US$4,503,000 from US$6,064,000 (Power, 2002).[25] Upwards of 70% of all computer crime directed toward companies is committed by insiders.[26] The insider abuse of Net access includes small violations at first glance such as reading newspapers online, following sporting events while at work, gambling online. Though these crimes may seem innocent and petty, they hit the companies where it hurts most — productivity. On top of that, a company hoping to curb insider abuse of Net access by conducting surveillance over the employees' Internet use has to deal with issues such as privacy at the workplace and psychological and mistrust issues which often arise when implementing such a policy. This may ultimately result in resistance and conflicts between the management and the employees.[27] More so, while the organizations can simply deploy security technologies to limit the insider unauthorized access, they may have to use more of a profiling approach to monitor

[17] Dictionary.com. www.dictionary.com. Accessed: Jan. 21, 2005.

[18] Nykodym, Taylor. ''The world's current efforts against cybercrime''. *Computer Law and Security Report* 2004;20:390—5.

[19] Op cit note 18.

[20] Swartz N. ''Cyber crime soars''. *The Information Management Journal* 2002, May—June.

[21] Power R. ''2002 CSI/FBI computer crime and security survey''. *Computer Security Institute* Spring 2002;VIII(1).

[22] Krempl Stegan. ''Web of deceit''. *Financial Times*. Ft. com. Connectis, September 2001, <http://specials.ft.com/connectis/FT3NKDS3TRC.html>: April 1, 2005; 2001.

[23] Nykodym N, Kehayov R. ''*Cybercrime from the inside*''. Unpublished manuscript; 2005.

[24] Op cit note 21.

[25] Op cit note 21.

[26] Demers Marie Eve. ''Prioritizing internet security''. *Electronic News (North America)* 2001;47(4):46.

[27] Ariss S, Nykodym N, Cole A. ''Trust and Technology in the Virtual Organization''. *Advanced Management Journal* 2002; 67:22—5.

their employees in order to decrease the Net abuse from inside. It may be helpful for organizations to understand the types of people that are likely to commit Net abuse. Some common characteristics of a person who commits Net abuse on a regular basis are: willingness to show no fear from the managers around, inclination for breaking the rules, and perhaps a keen sports fan. While the person who commits unauthorized access from inside is more likely to be secret, hard to communicate with, and quiet.[28]

The position of the attacker in the company has a significant influence on cyber crime. Cyber Crimes committed by managers, account for greater amount of money on average, while the cases are fewer. This is because managers may have more access capabilities and it may be easier for them to hide their crimes. While the employees perform more of the cyber crimes, they lack the control over or access to the companies' assets, consequently the companies' loss will be less. An alliance between a manager and an employee in committing a crime may be very difficult to detect and stop because their working on different levels of hierarchy may allow them more options to hide or disguise the crime.

According to a sample of computer crime cases given by Computer Crime and Intellectual Property Section of the US Department of Justice, 34% of the insiders committing cyber crime are between 20 and 29 years, 36% between 30 and 35 years, and 27% over 35 years. And although more perpetrators are between 30 and 35 years old, the most damage is done by persons over 35 years like Roger Duronio, 60, charged with more than $3 million, Timothy Allen Lloyd, 39, charged with over $10 million, and Kevin Mitnick, 37, charged with over $1 million of theft.[29]

Profiles and cyber criminals

There are many differences between cyber crime and conventional crime both in committing the crime and in prosecuting it. All of which seem to favor the criminals. This makes it very difficult to track, catch, and prosecute cyber criminals within the current legal system. Many times, the cyber criminal may be far away from the place where the crime takes place. The attackers can choose the place they will be at the time that the crime is to be committed because cyber crime does not require a physical presence from the perpetrator. A simple program can be written at any time by the attacker and entered into the organizational network. The program can be set to be executed at any time the perpetrator wants. There is a resemblance with a clock bomb, but the small program is far easier to hide and disguised within the network. It is not even necessary for the program to be within the network, it could be released from any place on the Earth with a computer and Internet connection.

When stealing information, the attackers have several choices from where they can actually steal the data. First, they can steal from the main server, second from the back up server, which holds a full copy of the main server, third while the data are in transition between two points, and fourth from a web page, which shows the data to the end user. It does not matter what method the perpetrator will choose as there is a great chance that the attack will go unnoticed if the information is not immediately released.

Think of conventional crime versus a cyber crime. A conventional crime, stealing cash for example, will be immediately noticed the next time the money is counted. Stealing data on the other hand is different. All the information is still on the server and it may seem untouched as there might be another copy of the data made by the perpetrator.

Cyber crime victims are typically organizations, whose systems are penetrated, and the customers of that organization. In case of data theft, the data could be strictly related to the organization or it could be a customer database with data like social security numbers, credit card information, mailing addresses and other details. Therefore organizations may suffer substantial losses in the form of lost customers and/or stolen or compromised confidential information. Customers can also suffer financial losses, when their identity is stolen.

The attackers may be experts in the field where they do their crime — hackers, computer security experts, programmers, Internet experts. On the other hand the organizations have to rely on employees like them to protect their networks.[30] Also the attackers may act as an organized group by sharing information without revealing their identities on the Internet and thus make the task

[28] Op cit note 26.

[29] United States Department of Justice. Computer Crime and Intellectual Property Section (CCIPS). Computer Intrusion Cases. United States Justice Department; <www.cybercrime.gov/cccases.html>, as of June 16, 2003.

[30] Piper T. ''An uneven playing field: the advantages of the cyber criminals vs. law enforcement — and some practical suggestions''; SANS Info Sec Reading Room; <www.sans.org/rr/legal/ueven.php>, 09/10/2002; 2002.

of the law enforcement even harder. The Internet itself offers more opportunities for the attackers to communicate without revealing who they are, and gives them a great advantage against the authorities.[31]

The differences mentioned above make the tasks of profiling and catching the cyber criminal much more difficult. Comparing the application of the four stages of Behavioral Evidence Analysis to the cyber crime and conventional crime will reveal better the advantages of the cyber criminal over the authorities and the difficulties in profiling a cyber criminal. In the first step — *Equivocal Forensic Analysis* — all the evidences are considered and evaluated, but in cyber crime most of the times there is no physical evidence, cyber evidence is easier to destroy by the perpetrator. There is no DNA, no finger prints or any physical presence. Therefore, it is much harder to find any significant evidence that may lead to the attacker. In step two — *Victimology* — a profile of the victim is done. But as mentioned before there may be two separate victims — the organization and the customers of the organization. It should be decided first which is the ultimate target, or are they both. Conventional crime makes identifying the victim much easier. For step three — *Crime Scene Characteristics* — it is even more difficult to profile the cyber criminal because of the advantages of choosing the time and place by the cyber attacker. Limited amounts of evidence and the very complicated nature of the crime can make the first three steps very complicated and inconclusive.

The final step — the *Offender Characteristics* — is perhaps even more challenging. Criminal profiling is relatively new as an official method to investigate conventional crimes, and cyber crimes are much more difficult to spot and to prosecute than the conventional crime, law enforcement finds itself in a very complex situation when trying to create a profile of the cyber criminal.

Applying profiles to insiders

In order to make the most precise profile of an inside cyber criminal, the first step will be to divide the type of cyber crime into one of many possible subcategories. Insider cyber crime can be generalized in four main categories: espionage, theft, sabotage, and personal abuse of the organizational network.

A spy is: ''a person who keeps close and secret watch on the activities and words of another or others'' or ''a person who seeks to obtain confidential information about the activities, plans, methods, etc., of an organization or person, esp. one who is employed for this purpose by a competitor''.[32] Therefore, the spy could be employed by a competitor, trained, and placed in the organization. The spies are after confidential or sensitive information, thus they must be placed high in the organizational hierarchy. They could be a part of the management team and would be an excellent source of very secret data. They could even be from the senior management staff. For that reason spies may not be very young at the time of the crime, maybe in the 30s as a junior manager or in their 60s for a more senior management position. Also depending on the race structure of the management team, they could be white, when there are more white managers in the organization, or black, if the organization has more people of color at higher positions, or both, if the organization is more diverse. The cyber-criminal is careful of what they are saying, and how they look. They do not want to look different, and always try to blend in among others. They are calm and secret persons. In order to catch a spy, you have to look for ordinary people who always try to hide their steps.

There are a lot of similarities between the espionage and the sabotage. But these two crimes are also very different. They both can be influenced by a competitor, but the saboteurs are not necessarily employed by the organization. They could act from a distance. The saboteur and the spy should possess a sound knowledge in the IT area so they would be able to commit the cyber crime and hide their steps. Both saboteurs and spies are secret persons, trying not to be seen. But the saboteur can act to harm the organization with personal motives like revenge for a lay off, or a missed promotion. A saboteur could be a person recently laid off, or an employee who feels neglected by the organization in some way. Saboteurs are probably between 25 years and 40 if employed by the company, so they have enough experience within the organization to learn the weaknesses and to feel offended if not offered a promotion or bonus. If employed by a competitor the age could vary significantly.

Unlike saboteurs and spies, the thief is guided only by mercantile motives for his own gain. The only goal in front of the cyber thief is to steal

[31] Op cit note 29.

[32] *New Universal Unabridged Dictionary*, 1996; Barnes & Nobles Books.

valuable information from an organization and use it or sell it afterwards for money. According to a sample from prosecuted intellectual crimes, provided by the US Department of Justice (Computer Crime and Intellectual Property Section) there is a strong pattern in the age of the cyber robbers. If the crime is for less than $100,000 most likely the attacker is young 20—25 years old, male or female, still in the low hierarchy of the organization. If the crime is worth between $100,000 and $1,000,000 the committer is probably 25—35 years old male, and if the crime accounts for more than $1,000,000 the attacker is over 35 and from the top management staff. The thief is confident in his actions. He is comfortable in his position. His crime is not driven by hate or revenge but by greed and hunger for money.

The most common insider cyber crime is the Net abuse for personal use like reading magazines on the workstation, online gambling, surfing the Net. This type of crime does not account for much money loss. Taken together, however, all the cases of Net abuse can hurt the organization's productivity, and there is a lot an organization can lose. The person who does this type of crime may openly: oppose supervisors; be non-conformant to rules; and regularly break rules.

In conclusion, it is important to say again that profiling is not a totally new method. The concept has been deployed in fighting crimes for centuries. While it is not 100% accurate, the system has had its hits and has a legitimate track record. Continued work and research will inevitably result in more advanced and useful identification processes and strategies. It is impossible to build the right profile for each and every cyber crime, because each cyber crime is done under different circumstances and different motives maybe at the center of the crime. The motives and the circumstances should always be considered when a profile is constructed.

Further reading

Kocsis R, Irwin H, Hayes A, Nunn R. Expertise in psychological profiling. Journal of Interpersonal Violence 2000;15:311—31.

<www.crimelibrary.com/criminology>; 2003.

Riem A. Cybercrimes of the 21st century. Computer Fraud & Security 2001;4:12—5.

Speer D. Redefining borders: the challenges of cybercrime. Crime, Law & Social Change 2000;34:259—73.

Available online at www.sciencedirect.com

SCIENCE DIRECT®