Crime Analysis & Investigation
Computers & Technology

Academic paper by Peter John Lynch (PJL) of Lynch Investigations & Countermeasures Pty Ltd.

Grad. Cert. Fraud Investigations (CSU)
Adv. Dip. Gov Fraud Control Management
Adv. Dip. Security Risk Management
www.pjlinvestigations.com.au

Introduction

It should be recognised that in the past there has been much more of a reactive approach to investigating offences committed in relation to technology.

Cybercrime is now upon us and it needs to be controlled and reduced. The investigator needs to adopt technology & apply it to the investigative problems to assist in limiting the opportunities for those who commit offences.

The investigator still needs to be able to respond to offences committed in a reactive manner, but with greater application of a proactive approach from adopting technology and applying it to their investigations will reduce the time spent reacting to offences committed & unsolved problems stemming from previous attendances of investigations by a reactive approach.

If the investigative teams can take this adoptive approach to technology and apply it to there investigations, the offences committed involving technology and cybercrime can be controlled and reduced. The working practices and the adoption of technology need to be reviewed to turn around the ineffective investigator to an effective and efficient investigator role.

A balance of skills, resources and experience from the industry can sustain a methodical approach to control and reduce the crime offences being committed in this technological revolution.

Strategic Approach

The strategies involve the need of funds, trained personnel, legislative updates, cooperation from the clients, international liaison and national liaison between law enforcement agencies.

The areas to be reviewed include the trends and issues within technological cybercrime from the Internet. The areas that should be reviewed and addressed are hacking motives, hacking techniques, hacking offences, copyright offences, child pornography offences, child exploitation, phishing, phreaking, smurfing account harvesting and spamming.

Through the implementation of a proactive approach to adopt technology and apply technology to investigate working practices, the opportunities will be limited for those who commit offences and thus less time and resources will be spent on a reactive investigative approach which only leaves matters unresolved and perpetual.

The areas of technology and cybercrime need discussing & addressing to reveal the understandings between the client, law enforcement, national and international liaison, from a legislative and training perspective.

There needs to be further;

1. Education
2. Improved security
3. Legislation
4. Encryption
5. Defence through prosecution

The major areas of concern are mainly;

Information

'STEAL IT – (HACKING)
DAMAGE IT – (VANDALISM)
ALTER IT – (REVENGE)
DISTRIBUTE IT – (CRIMINAL SYNDICATES)
HIDE IT – (CRIMINAL SYNDICATES)

Services

STOP (COMMERCIAL COMPETITION)
DESTROY (WAR)
INTERFERE WITH/DISRUPT (REVENGE)
HINDER (MISTAKE)' (K, Day 1998, p.4).

Lynch Investigations & Countermeasures Pty Ltd's Strategic View

Our business recognises that Microsoft has partners with Australian law enforcement agencies to combat cybercrime. We think that it would be beneficial to have our investigators attend some of the latest investigation training from the short period work shops that are held at the AFP College in Canberra ACT.

The training targets issues relating to cybercrime including forensic work, tracking down online paedophiles, information sharing procedures and communication protocols.

G, Stone (2005, p.2) National Technology Officer Microsoft Australia states, 'cyber criminals have advanced from fairly simple virus writing to much more clever attacks, sometimes using more than one attack mechanism.' G Stone (2005, p.2) states, 'these range from elaborate phishing scams that use phoney web sites to steal credit card numbers and perpetrate identity theft; fraudulent spam that launches viruses or spyware and malware such as trojans that enable criminals to take remote control over thousands of computers for a massive distributed attack.'

Lynch Investigations & Countermeasures Pty Ltd has an online business, a web site www.pjlinvestigations.com.au including an online store that sells investigation equipment, books and investigative services. The store is online twenty-four hours per day seven days per week, allowing clients to purchase as they desire.

Our web host has server based security software that protects our client's information. The other areas of the web site where investigation forms are completed on request of an investigation, is completely password protected to the secure server. The administrator controls security access to this area.

Our computer system uses Broadband Internet Services that has virus scan, spyware scan and spam detection software. The Broadband incoming line delivers to our service provider Ninemsn. Ninemsn also has firewall protection, virus scan, spyware scan and spam detection programs.

In addition to this, the computer system runs Microsoft Windows firewall and virus protection with automatic updates. We have also installed on the computer system AVG Security Software that scans all incoming and out going emails. AVG has automatic or manual updating, anti virus scanning at executable files, automatic triggering of tests and updates and virus vault to hold and assist delete trojan horses.

We have found in considering that we are commercial & private inquiry agents; we are dealing with highly confidential information from our client's and colleague's where we can't afford to have our system infiltrated, damaged, changed, destroyed or security breached. In addition to this our email is domain based and uses our web site server that is heavily secured.

The remote server is imaged daily. There are two backups that are created and stored in separate machines in separate physical locations.

The hardware firewalls network runs various detection systems particularly against denial of service (DoS) attack and hacking attempts. The security software monitors the flow and consistency of hits and the moment there is a sudden rise in hits, the server implements a sort of funneling protocol. The incoming data is then made to line up in single file. The system is Unix running Apache OS. The hosting company is very particular about its latest updates & patches.

We have used this proactive adoptive approach to technology and applied these measures due to our previous findings from investigations of our computer systems. We have also learnt from our training and experience the dangers and threats that the cybercrime criminals use in the practices of hacking, phishing, spamming, smurfing, phreaking and account harvesting.

Malicious hacking is separately labeled as cracking in order to differentiate from benign or good hacking. These labels give way to legal tests laid out for hacking offences that include recklessness as to the harm or inconvenience that a hacker may cause. There are many possible motives of the hacker which are important to understand of issues of intent and recklessness is at the heart of the criminal liability. A proactive approach is best taken by implementing additional technology tools to help control the hackers intrusion to the computer system used by investigators.

Intrusion Detection

Intrusion detection systems should be implemented in a proactive manner; these are computer programs that can detect many attacks while they are happening. Also tools to detect attacks that may have occurred are also required.

A good intrusion detection system can monitor both information about your computer and the connection between it and the internet. With an intrusion detection system running on your computer system, you can be alerted of an attack or of an attack being attempted. An intrusion detection system may be able to supply useful information for fixing the problem or an active intrusion detection system can act to block attacks it detects. An intrusion detection system can inspect log files to detect possible hacking by other programs.

File Integrity Tools

File integrity tools are programs to detect a file that has been changed. The tools assist for detection of an attacker by evaluating important files or programs. The file integrity tools detect when files integrity has been lost by access from the attacker.

Security Preventative Measures (Proactive Approach)

There are many ways in which to safeguard a computer system by being proactive and preventing complete and successful attacks from occurring.

Sharing

It is best to leave Windows software program settings for file sharing and printer sharing between computers turned off. Many home computers including those running Windows come equipped with settings to allow file sharing and printer sharing between computers. This can allow other internet users to view the content of your hard drive that is definitely not wanted.

Patches

It is also advisable to use security software that includes an automatic updater that can check the company's web site for the required patch needed and apply them as soon as they are available. A patch can secure a vulnerability found in a software program that is used by an investigator's computer network or web site.

Virus Scanners

Damage caused by viruses can be horrific. Viruses can cause problems ranging from reformatting the hard drive to deleting data. Viruses target areas like hard drives via email downloads, disks and other hardware that moves from one computer to another.

Introducing a good virus scanner program can secure many viruses before viruses cause damage to the computer system.

Firewalls

A firewall is like a wall of many intrusion detection systems or firewall like functions. The firewall performs a check point between the computer system and the internet. When information attempts to enter or exit the firewall, it must first pass through the firewall and be examined.

Firewalls are effective when used in combination with an intrusion detection system (IDS). The firewall being the initial contact with data, the first line of defence while the IDS detects more complex attacks that make their way through the firewall.

Vulnerability Scanning

There are vulnerable areas (weak points) within a computer system. The vulnerabilities are usually system or software flaws that allow adversaries access to the computer system or network.

Commercial scanner programs are used to scan computer systems and detect potential vulnerabilities & problem areas. Where vulnerability is found you can use patches or change the software set up to repair the problem. By eliminating the vulnerabilities in the computer system or network you can prevent a hacker from finding the vulnerability and using it in an attack on the computer system or network.

General Desktop Security

In addition to these proactive measures, the computer operator can control blockers, identify spam and phishing. The operator of the computer system can further secure the computer system through trained computer systems operations common sense skills.

Harnessing Resources - Adopting Technology and Planning Proactive Investigative Strategies to Control Crime

Methods Required

1. Covert Operations	Provide successful covert operations used to detect and prosecute those who do offend.
2. Case Screening (Analysis)	Certain criteria can be applied to information about a case that will predict with reasonable accuracy how likely that case will be solved.
3. Research	Research has found the importance for the public is in reporting crime and providing evidence needed to arrest and convict offenders.
4. Interviews	Cognitive interview training is required. It has been shown 30 – 35% more correct information is produced with cognitive interviewing (GH, Gudjonsson 1992).
5. Crime/Operational Analysis	Determine the methods of operation of individual criminals. Determine pattern recognition. Field interrogation and arrest data. Crime report data. Incident report information. Dispatch information.

Crime Analysis

Crime Analysis – the operations manager develops an appropriate plan of action if deemed appropriate. If no action appears appropriate then the field manager must justify the decision. In order to eliminate a non – responsiveness, the client receives a copy of all reports.

1. ‘Ensure Accountability

2. Have the crime analysis unit release only thoroughly developed trend and pattern analysis reports that have clear implications for assisting field operations.

3. Built in feedback loops to ensure that the results of directed surveillance missions are documented and that the crime analysis unit can better understand how improvements in reporting can be achieved.

4. Have crime analysis personnel work closely with field staff to encourage inquiries regarding observed problems developing in the community.

5. Staff composition of the crime analysis unit should be carefully considered.

6. Selection of investigative officers for participation in field investigations.

7. Responsibility for planning the missions to be carried out by directed investigations must be clearly established.

8. Training is essential at all levels.

9. Finally, there needs to be a system of positive rewards for those who carry out the assignments in a commendable manner’ (MJ, Palmiotto (ed.) p.88).

The problem oriented approach calls for developing preferably within a private inquiry agency the skills, procedures and research techniques to analyse problems and evaluate agents effectiveness as an integral continuing part of management.

Definitions of Intelligence Led Investigations

Proactive Approach Using Technology

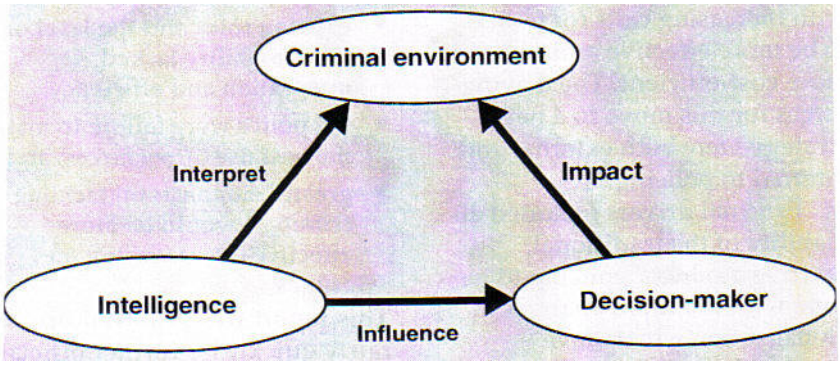
Surveillance - targeting offenders (especially the targeting of active criminals through covert means).

Crime Mapping - the management of crime and disorder hotspots. The investigation of a linked series of crimes and incidents.

Communication - (Internet) (Telephone) (Camera & Footage Review) (Monitoring) the application of preventative measures, including working with local partnerships to reduce crime and disorder. NCIS 2000 (JH, Ratcliffe 2003).

Quality intelligence analysis is extremely important. Research is also essential to identify crime reduction strategies that actually work and have solid evidential support. Intelligence led investigation is the process of applying criminal intelligence analysis as an objective decision making tool in order to facilitate crime reduction and prevention through effective investigative strategies and external partnership projects drawn from an evidential base (JH, Ratcliffe 2003).

In most private inquiry agencies the intelligence unit or section is a recognised organisation with people, skills, methods and an organisational structure. Intelligence is also a process incorporating a continuous cycle of tasking, data collection, collation, analysis dissemination and feedback prior to the next or refined task. The continuous process is responsible for the generation of an intelligence product, which is designed to shape the thinking of decision makers.



Intelligence Led Investigations Model (JH, Ratcliffe 2003 p.3).

An effective system needs investment in people, tools, systems and also an understanding of the functions and limitations of an intelligence system, analytical tools and training to enable the maximum benefit to be derived.

At the strategic levels this also requires the ability of staff to have systems in place to share intelligence within and outside of the agency (JH, Ratcliffe 2003).

Tools & Technology

Software Crime Mapping
Forensic Software
Data Mining Software
Video Cameras
Profiling Software

Crime Scene Analysis – what, why and who?

Model for criminal profiling – involving profiling inputs, decision process models, feed back loops, crime assessment, personality assessments and investigative strategies from which the profile and the investigation was developed to then theoretically at least led to an apprehension. The process more commonly known as criminal investigative analysis.

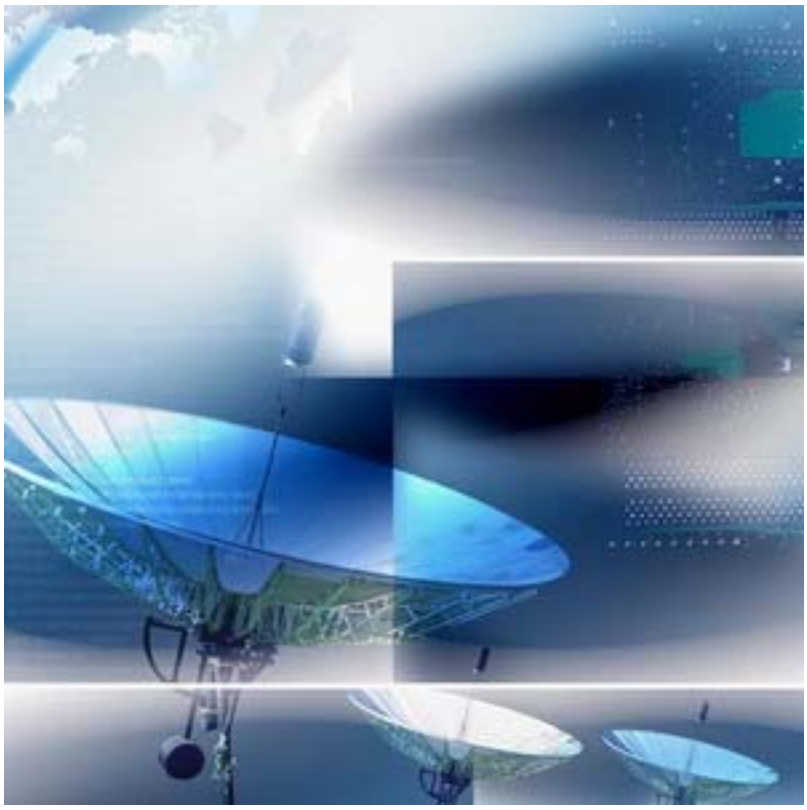
Geographic Profiling

P Branca (1998, p.17) states, ‘geographic profiling is concerned with the geographic behavior of the serial offender with a view to predicting his/her most probable home location.’

Geographic Profiling is a crime investigation strategy that makes use of geographic analysis techniques drawn from the approaches of Environmental Criminology.

A computer mapping program developed by Environmental Criminology Research INC (ECRI) has been able to successfully assist many local and international investigations regarding serial crimes such as murder, rape, arson, robbery and offences.

It has been stated that computer mapping programs assist in the criminal analysis for Criminal Geographic Targeting. It is thought after predictions are made, investigators are then able to prioritise suspects according to where they live or work. The computer mapping programs can be used as proactive investigation tools especially where they may assist in finding a serial crime offender or preventing further serial crimes from occurring (K, Rossomo (P, Branca 1998).



Past Work

I have worked in law enforcement & security in country and metropolitan areas in Australia for seventeen years. I was deployed to Glebe in Sydney as security for three years at the Broadway Shopping Centre and to North Sydney at the same time as armed protection for commercial business. These locations were crime hot spots for armed robbery and larceny in 2001-2004.

Our team initiated a proactive approach by the use of team cooperation, good communication, rapport with the local police and the public with support from our management and the clients. Our customers were also at the fore front of our approach when protection or customer service was needed. This was our proactive approach to our intelligence led operations.

Our team continued at the site for three years while I was onsite using communication technology, computer programs, CCTV and devices for monitoring and covert surveillance techniques. The same security company still services this client today.

The Glebe community was lacking in welfare services with a heavy tourist traffic stream. There was also a large range and mix of cultural values from different social classes and various ethnicities. The urban area was becoming heavily populated with these factors contributing to the crime issue.

The crime rate was relatively high in the area where commercial business was trading. There was also a reactive approach at the site to the crimes that were occurring with a level of proactive investigation underway on occasions when it was considered to be peak trading periods.

Police attendance mainly occurred at the Broadway Shopping Centre site when crime seriousness exceeded management's onsite set standards. It was not relevant to have police attending petty offences at Broadway Shopping Centre always, due to the damage that could be created for the public in the community in busier policing periods.

More training, tools, technology, mapping, and geographic profiling would have been beneficial for the security staff of the Broadway Shopping Centre in Glebe NSW, to assist in adopting a higher level of proactive approach to solving the crimes there with investigative strategies from a crime analysis perspective. The crime issues that had been occurring could have been controlled in the environment more strategically for longer term benefits of the community.

Recent Work

I have been working with workers compensation claims recently using surveillance to investigate claimants.

Various matters have involved a reactive approach, where claimants investigated for fraud have finalised there claim by lump sum payment, then continued with some type of work. This sometimes being heavy work for the injury that was claimed for.

I performed surveillance from a reactive perspective. A proactive approach to these matters would have been more suitable for the management of the workers compensation cases.

Surveillance in the majority of matters is used as a last resort. The red flags of fraud need to be established and confirmed earlier in the claims process where an adoptive proactive approach should take place. More technological tools need to be available to the investigator to be used in an appropriate time frame and capacity with earlier recognition of the red flags of fraud from the insurer's claims management. Some tools needed are data mining and claims analysis software programs.

The red flags of fraud need to be evident and analysed by the managers of the insurance companies. Then a complete examination of the facts of the case needs to occur for further corroboration.

It is in the insurer's best interest to adopt a proactive approach in the claims management process and to collect as much intelligence as possible early in the case to be objective with the outcome as opposed to the reactive investigations I have been involved with recently.

Conclusion

Investigators should be encouraged to professionalise in order to develop specialist expertise in a relevant area of interest necessary to deal with crime effectively. There are openings for further research and training in computer investigations in electronic commercial cybercrime and the use of technology for solving crimes.

With the growth in the use of technology and the processes of online banking, online overseas trading, international technology crime and e-commerce, expertise in computer crime solving is needed.

There is a greater need for a proactive approach to crime through early investigation of matters where it has been proven the reactive approach has failed to deal effectively with the crime problems that are still growing due to the initial reactive approach to the crime offences that were the more accepted means of dealing with these matters.

Resources have a significant effect on how organisations can approach the issues of crime that occur in the private sector. Management and resource allocation become the most crucial areas that management needs to balance here.

There is a need in the private sector to retrain staff, supply technology, redraw policies and procedures.

With some time and patience a better model can be achieved where investigative agencies can adopt a more integrated, systematic and proactive approach to crime solving using criminal investigative analysis with the application of technological resources.

Bibliography

Branca, P 1998, *Geographic Profiling: A new tool in serial crime investigation*, Intelligence Digest, August, pp. 16-17.

Carozza, D 2006, *Fraud Magazine, Journal of the Association of Certified Fraud Examiners*, January/February 2006 Volume 20, no.1 ACFE.

Chalmers, AF 1982, *What is This Thing Called Science?* University of Queensland Press, St. Lucia.

Day, K 1998 *Investigation & Policy Issue*, Australian Federal Police, Canberra ACT Australia, pp. 1-6.

Goldstein, H 1990, *Problem Oriented Policing*, McGraw-Hill, New York, pp. 1-206.

Gordon, A 2006, *Agent: Essential Reading for Collectors, Investigators, Process Servers & Repossession Agents*, February/March 06 Volume 39 issue 7 IMA.

Gudjonsson, GH 1992, *Interviewing: Basic Principles & Theories in the Psychology of Interrogations Confessions & Testimony*, Wiley, Chichester.

Kinsey, R, Lea, J & Young, J 1986, *Losing the Fight against Crime*, Basil Blackwell, Oxford, pp. 1-221.

Krone, T 2005, *Hacking Motives*, High Tech Crime Brief, Australian Institute of Criminology, Canberra ACT Australia, pp. 1-2.

Krone, T 2005, *Hacking Offences*, High Tech Crime Brief, Australian Institute of Criminology, Canberra ACT Australia, pp. 1-2.

Krone, T 2005, *Phishing*, High Tech Crime Brief, Australian Institute of Criminology, ACT Australia, pp. 1-2.

Krone, T 2005, *Hacking Techniques* High Tech Crime Brief, Australian Institute of Criminology, Canberra ACT Australia, pp. 1-2.

Microsoft 2005, *Microsoft Partners with Australian Law Enforcement Agencies to Combat Cybercrime,* Australia Microsoft.

Palmiotto, MJ (ed.) 1988, *Crime Pattern Analysis: An investigative tool, in Critical issues in criminal investigation,* 2nd edn, Anderson Publishing, Cincinnati, Ohio, Chapter 5, p. 88.

Poultney, B 2005, JST426 *Crime Analysis & Investigation,* Faculty of Arts Readings, Charles Sturt University, Albury-Bathurst-Wagga Wagga, New South Wales Australia.

Poultney, B 2005, JST426 *Crime Analysis & Investigation,* Faculty of Arts Study Guide, Charles Sturt University, Albury-Bathurst-Wagga Wagga, New South Wales Australia.

Poultney, B 2005, JST426 *Crime Analysis & Investigation,* Faculty of Arts Subject Outline 200640, Charles Sturt University, Albury-Bathurst-Wagga Wagga, New South Wales Australia.

Ratcliffe, JH 2003, *Intelligence- Policing: Trends & Issues in crime and criminal justice*, Australian Institute of Criminology, pp. 1-6.

Smith, RG, Woolanin, N & Worthington, G 2003, *e- Crime Solutions & Crime Displacement,* Trends & Issues, Australian Institute of Criminology, Canberra ACT Australia, pp. 1-6.

Smith, RG 2004, *Impediments to the Successful Investigation of Transnational High Crime,* Trends & Issues, Australian Institute of Criminology ACT Australia, pp. 1-6.

Smith, RG 2003, *Investigating Cybercrime: Barriers & Solutions,* Australian Institute of Criminology, Canberra ACT Australia, pp. 1-6.