National
College of
Ireland

The college for a
learning society

A Computer Forensic Methodology for Ireland

Niall McGrath

Mícheál Ó hÉigeartaigh

Pramod Pathak

Working Paper NCIRL- 012-2003

A Computer Forensic Methodology for Ireland

Niall McGrath, Niall.McGrath@boimail.com
Mícheál Ó hÉigeartaigh, National College of Ireland, moh@ncirl.ie
Pramod Pathak, National College of Ireland, ppathak@ncirl.ie

0. Abstract

The advent of the Internet has initiated a huge change in society. It exists symbiotically with us in our daily lives (i.e.) it is a medium for work, entertainment, knowledge, and communication. Since it is part of our social fabric, it has spawned a new phenomenon known as Cybercrime. This is fraud, theft of intellectual property or confidential data, harassment, defacement of a website, illegal use or abuse of a network (i.e.) the perpetration of any crime with the use of a computer. Due to the relative infancy of the Internet, there is a dearth of technical and legal knowledge on how to protect society from the influence of Cybercrime.

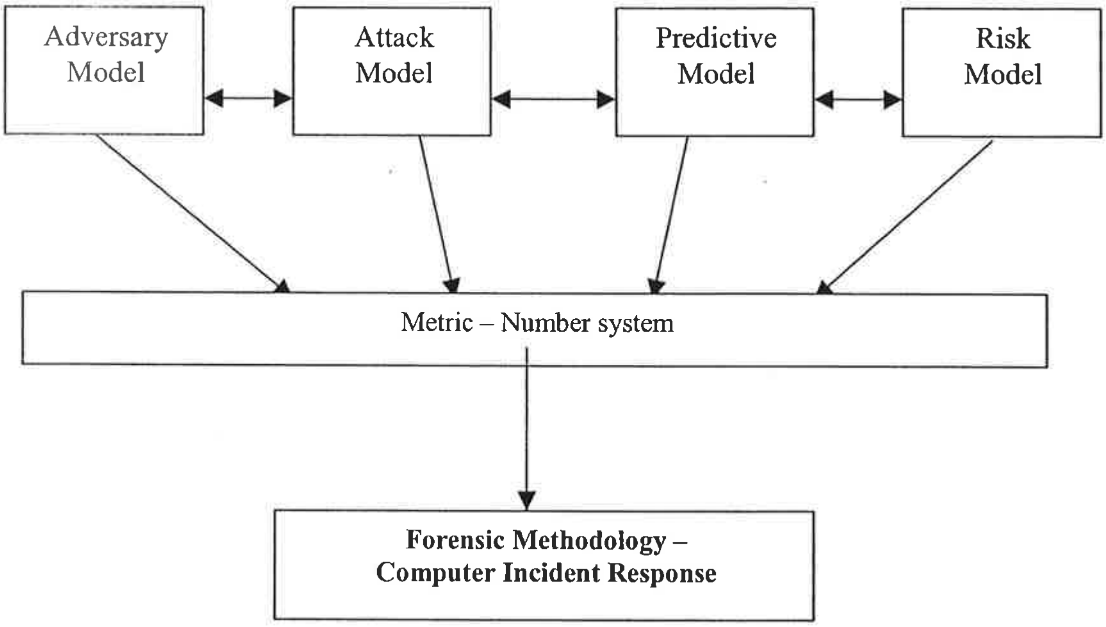
This research intends to build a full forensic profile of the Cybercriminal (i.e.) their techniques of attack, motivations and identities. It is motivated by the need to protect ourselves, our confidentiality and our assets, so that Cybercriminals will no longer be able to operate with impunity.

1. Introduction

The ubiquity of the Internet guarantees itself a permanent position in society today. It is a wonderful resource that has resulted from the evolution of various technologies like mathematics, software and hardware. It is also a vital channel of business for most organisations. The highly technical skill behind the building of the Internet is awesome. Equally, the skill set of the people that abuse it is also very sophisticated and advanced. Hackers, fraudsters, opportunists, terrorists, vandals, extortionists, thieves (i.e.) *Cybercriminals* seem to be able to operate with relative impunity. Their anonymity and the present lack of legal precedent weighs heavily in their favour.

A Forensic Methodology would facilitate the profiling of the *Cybercriminal* –their methods, their type of attack, their motivation and their use of technology. The threat posed by *Cybercriminals* can be based on their ability to select the times, dates and subject of their attack. With the help of a forensic methodology, we can begin to try to predict future incidents and implement a formal procedure of handling present incidents. Great care is needed in the treatment and handling of digital evidence before it is used in court. A major part of a forensic methodology is the implementation of a Computer Incident Response procedure that will be implemented by the Computer Incident Response Team. This is iterative by nature and, as people become very familiar with it, it will serve as a very good mechanism of prediction.

The components that provide input into the methodology are 1) An Adversary Model, 2) Attack Model, 3) Predictive Model and 4) Risk Model



Adversary Model

Adversary	Objectives	Money	Expertise	Access	Risk Tolerance
Insider	Revenge, retribution	Low	Low	High	high
National Intelligence	Information, Political, military, and economic power	High	High	Med	Med
Info Warrior	Military advantage,chaos	High	Med	Med	High
Terrorist	Political change, chaos, publicity	Med	Low	Low	High
Industrial Espionage	Competitive advantage	Med	Med	Med	Low
Organised Crime	Monetary gain	Med	Med	Med	Med
Hacker	Thrill, challenge	Low	Med	Med	Low

1. Adversary Characteristics

Risk Tolerance - This is the level of risk the adversary is willing to take to achieve his/her goal.

The Objectives - These are the adversary's desired outcome, which serves as motivation to attack.

The Resources - These include technical expertise, money and access to potential targets that an adversary might have.

I The Insider

The Insider with malicious intent is a very serious issue for companies. They already have prior knowledge of resources or potential targets like machines, databases. When equipped with knowledge of passwords, file and directory hierarchies and even physical location, the malicious insider can be regarded as a serious threat. The Insider could be a member of a team or maybe acting solely on his/her own.

II Info Warrior

The Info Warrior is a military adversary whose objective is to cause infrastructural damage and chaos to computer networks, telecommunication and communication systems that have the effect of crippling opposition strategy and intelligence.

III National Intelligence

This adversary's objective is to gain long-term political, economic and military advantage by collecting and distributing information.

IV Terrorist

The terrorist attacks are usually done with the objective of gaining publicity, revenge, chaos and making political statements.

V Organised Crime

This is primarily motivated with the objective of making money and taking control of systems.

VI Industrial Espionage

This is the objective of the industrialist who wishes to gain competitive advantage by stealing secrets or plans.

VII The Hacker

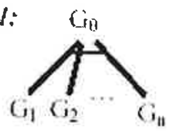
The Hacker is described as the person who has the technology and high skill level that can carry out attacks like system compromises for personal satisfaction.

Attack Modeling – Attack Tree

Attack trees are used to characterise enterprise security. The root of each tree symbolises a potential security compromise that would impact key service functionality of any business (i.e.) survivability. The tree iteratively describes graphically or textually the various steps that would have to be taken for an attack's objective to be achieved. Typically, the enterprise's security system is represented by a forest of trees or a system of forests.

Attack trees consist of a root node and subnodes. Subnodes are also called subgoals. An attack where all of its subgoals have to be achieved in order for a root goal to be achieved, is classified as an AND decomposition of a tree. Alternatively, if an attack's root goal can be achieved by only taking the path through one of its subnodes, then the attack tree that represents this attack is classified as an OR decomposition. Collectively, an attack tree can consist of AND/ OR decompositions.

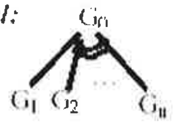
Graphical:



Textual: **Goal** G_0
AND G_1
G_2
...
G_n

1. Attack Tree – AND Decomposition

Graphical:



Textual: **Goal** G_0
OR G_1
G_2
...
G_n

2. Attack Tree – OR Decomposition

Example: Typical Webserver Attack of gaining privileged information

AND 1.Identify domain name

2.Identify Firewall IP address
OR 1. Interrogate Domain Server
2. Scan for Firewall Identification
3. Trace route through Firewall to Webserver

3.Determine Firewall access control
OR 1. Search for specific listening ports
2. Scan for any ports that are listening

4.Identify Webserver OS and type
OR 1. Scan OS services' banners for OS identification
2. Scan TCP/IP stack for OS characteristic information

5. Exploit Webserver vulnerabilities
OR 1. Access sensitive shared resources directly
2. Access sensitive data from privileged account Webserver
3. A Typical Webserver Attack

This intrusion can also be represented by the notation <i , j , k >:

<1, 2.1, 3.1, 4.1, 5.1> , <1, 2.2, 3.1, 4.1, 5.1> , <1, 2.3, 3.1, 4.1, 5.1>
<1, 2.1, 3.2, 4.1, 5.1> , <1, 2.2, 3.2, 4.1, 5.1> , <1, 2.3, 3.2, 4.1, 5.1>
<1, 2.1, 3.1, 4.2, 5.1> , <1, 2.2, 3.1, 4.2, 5.1> , <1, 2.3, 3.1, 4.2, 5.1>
<1, 2.1, 3.2, 4.2, 5.1> , <1, 2.2, 3.2, 4.2, 5. 1>, <1, 2.3, 3.2, 4.2, 5.1>
<1, 2.1, 3.1, 4.1, 5.2> , <1, 2.2, 3.1, 4.1, 5.2> , <1, 2.3, 3.1, 4.1, 5.2>
<1, 2.1, 3.2, 4.1, 5.2> , <1, 2.2, 3.2, 4.1, 5.2> , <1, 2.3, 3.2, 4.1, 5.2>
<1, 2.1, 3.1, 4.2, 5.2> , <1, 2.2, 3.1, 4.2, 5.2> , <1, 2.3, 3.1, 4.2, 5.2>
<1, 2.1, 3.2, 4.2, 5.2> , <1, 2.2, 3.2, 4.2, 5. 2>, <1, 2.3, 3.2, 4.2, 5.2>

From an attack pattern, we can characterise an individual type of attack. Thus by combining various attack patterns we can organise attacks into profiles. An attack profile will compromise of a common reference model, a set of variants, set of attack patterns and a glossary of defined terms. By categorising attack like this, it makes it easier to search for and apply various attack scenarios. Libraries of attack patterns and profiles can be assembled and can be reused. As times goes on and new technologies and techniques of attack emerge, attack patterns and profiles can be refined.

2. Risk Analysis and Assessment

Risk analysis is a procedure used to estimate potential losses that may result from system vulnerabilities and to quantify the damage that may result if certain threats occur. The ultimate goal of risk analysis is to help select cost-effective safeguards that will reduce the risks to an acceptable level. The evaluation should take into consideration all physical assets including the buildings, computers, and other equipment and, of course, the information contained therein. An assessment should look at the various types of information maintained by the agency to determine how important it is, how vulnerable it is, the cost of losing the information, and the cost of protecting it. [3]

Risk assessment is the mechanism through which the current standing of a company's system security is assessed. It is used to highlight, at a managerial level, the potential risks of threats and vulnerabilities and their impacts on various mission critical systems. It also makes recommendations and proposals on how to mitigate those risks.

An Approach to Predictive Network Analysis

Present network security procedures are primarily not adequate enough. They are reactive rather than proactive. The problem is exacerbated by the very fast rate at which new vulnerabilities emerge. Risk analysis gives a very static impression of the true nature of threat assessment because it is mistakenly understood that threat changes slowly.

It is far more beneficial to get an understanding of the driving factors that are behind computer security incidents networks. Analysts must choose a perspective from which to view their networks. There are four perspectives:

- ***Local Perspective:*** observes the network from the area of the firewall i.e. the connection point of the Internet with the actual network. The advantage is that the knowledge of any strange network behaviour is directly related to you. However, the disadvantage is that it gives very little time to react.
- ***Proximate Perspective***: arranges for observation at the wide-area network point of presence.
- ***Remote Perspective***: arranges for a variety of points of observation at contracted points on the wide area network.
- ***Endemic Perspective:*** builds a framework of allied network analysis groups.

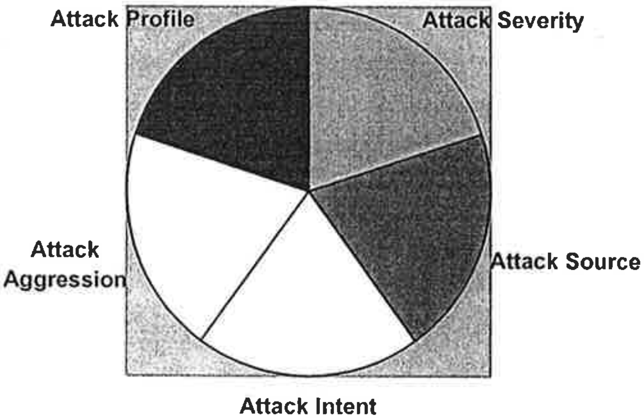
Establishing a baseline profile of normal behaviour helps to understand what is normality in relation to the perspectives listed above. It must be decided on how to establish profiles and how to isolate aspects of interest. From this, trends and cycles of political, economical, social and technological influences can be seen. With an effective baseline profile in place, the next challenge is to be able to identify exceptional behaviour. Each organisation needs to develop its own set of criteria to identify which behaviours are exceptional and which exceptional behaviour prompts warnings. These reflect mission priorities.

The decision support role for predictive analysis plays a crucial role also.
It provides a mechanism to inform decision-makers of the available courses of action in response to alerts, with their consequences and the threat associated with any defensive actions.

To assess the effectiveness of the actions, criteria need to be formulated and validated with observations - hypotheses of effectiveness can be refuted or made. Various inputs from Bargaining, Equilibrium and War Gaming theories have yet to be evaluated and explored. The expected input from these areas could provide an insight into how to pre-empt the actions of the adversary. In addition, the potential use of the *Observation, Orientation, Decision and Action loop* (OODA) in combating Cybercrime has to be investigated.

3. A Metric System

It is wise to put an attack metric system in place, which will enable the analysis, categorisation and evaluation of attacks in a uniform manner. [6] Has put forward notions like Attack Severity, Attack Source, Attack Intent, Attack Aggression, Attacker Profiles and Cyber-Terrorist watch lists. These provide individual metrics on attacks from diverse perspectives. However, a fusion of all these would provide a more accurate picture of an attack. This will be indispensable for the proper implementation of a CSIR procedure.



A basic unit of attack

This is a simplistic illsutration of the various attributes that should constitute a basic metric unit of attack. (Each segment should elaborate on various other subsegments, so there is rarely an even distributon of the five constituents. The illustration above is misleading from that point of view).

A Numbering System

To characterise an attack, a numbering system should be developed to represent an attack. This should include and represent the measure of each atttribute , illustrated above, that constitutes the attack. This has not been completed yet.

4. Computer Incident Response (CIR)- the Forensic Approach

In any organisation, it is very important to have a consistent approach to security procedures and practices. When any number of computer incidents occur across various departments in an organisation, they must all be handled with the same procedure and consistency. If they are handled in such a predefined manner, it removes any tension or anxiety that an individual incident may bring. Therefore, they can be treated entirely objectively. In case of an incident, that warrants the seizure of digital evidence or the seizure of an evidence artefact like a hard drive, it is best that a prescriptive approach is taken. These are forensic details that should be noted in resolving a computer incident.

If a digital medium like a disk or a hard drive contains evidence, the only way that this will be admissible to court is if a "chain of custody" is provided. It must also be proven that the evidence was not altered in anyway. Especially, in the analysis stage of evidence like a log file, the data could be inadvertently manipulated. This means that if it is not the originally seized then any case built on this evidence can fall down in a court of law. Evidence can also be accidentally damaged in transporting from one area to another. It can also happen that a piece of malicious code is triggered when a machine in going through its "power-down" cycle and will purposely destroy any designated files or wipe a disk drive.

A system administrator's job is to monitor network traffic or monitor logs from an Intrusion Detection System, a Firewall or an Antivirus system. If these logs indicate irregular or exceptional behaviour, it is crucial that the person knows how to respond in a manner that eliminates the threat or mitigates its risk.

Alternatively, if it is possible to predict exceptional behaviour from irregular network traffic patterns this could lead to taking pre-emptive steps. To put an effective CIR is place it is important to have a core team i.e. a CIR team (CIRT). The CIRT's exclusive task is to co-ordinate its response to incidents that are reported. The response entails details of incident detection, containment, elimination, prevention, reporting, handling of evidence and inclusion of law enforcement (LE).

CSIRT Framework

A basic framework is required to represent the various components of a CSIRT model.

The organisation should encapsulate the goals and objectives in a mission statement that is clear, concise and unambiguous. This can also be supplemented with a vision statement that explains the reasons of why the team was established.

Over the time of the CSIRT's existence, it will have to interact with a number of groups. Its constituency could be of two types: bounded and unbounded. An unbounded CSIRT's constituency means that the team will service anyone who requires its services. A bounded constituency would only service requests from a designated entity (e.g.) the source of funding of the team.

The place a CSIRT holds in an organisation is reflected in its mission statement. It is important to establish how enthusiastic senior management is on the overall concept of a CSIRT. It may constitute the entire security team or may be totally distinct from the organisation. However it is structured, the team must play an important role in the risk management and be well embedded in the business structure of the organisation.

Experience has shown that as the effectiveness of the CSIRT becomes widespread and as company partners or groups initiate their own CSIRTs, the issue of relationship with other groups becomes more apparent. In the US where national bodies or agencies are concerned, the teams operate in a hierarchically structured environment. The US department of Defence co-ordinates across the various military teams like the Army, Air Force, and Navy.

CSIRT Service and Quality Framework

A CIRT can offer a range of services to a constituency. The services should be documented to cover details of the Objective, Definition, Function Description, Availability, Quality Assurance, Interactions and Information Disclosure, Interfaces with Other Services and Priority of the service offered. These descriptions are indispensable when defining and implementing the service.

Typical services offered include Incident Response, Announcements, Vulnerability Analysis and Response, Artefact Analysis and Response, Incident Tracing, Intrusion Detection, Auditing and Penetration Testing, Risk Analysis, Collaboration, Security Consulting etc. Whatever the number of services offered, there will also be some inter-relationship between them. It will be necessary to specify any interfaces and information flow between those cases. Care should be taken to ensure that information sharing is handled consistently and appropriately because different services will have different handling requirements.

A policy is a governing principle adopted by the team. It is important to understand the relationship between policies and procedures since these are often intermingled and mixed. Procedures detail how a team enacts activities within the boundaries of its policies. The success of the policy often depends on the correct procedures being enforced or followed. The basic attributes of a policy are, they should be clear, concise, necessary and sufficient, useable, implementable and enforceable.

Adapting to Specific Needs

The CSIRT is usually set up to provide a service or response to a certain type of incident. For example if a company, which has no CSIRT in place, is continuously being attacked by viruses, the CSIRT should be set up with the primary function of virus related incident response handling. However, a CSIRT needs to be prepared to address an incident of any type. CSIRTs must have flexible procedures and policies to enable the team to easily adopt to change.

Incident Response Service
Fundamental components and procedures should be in place to support the operation of an IR service.

IR Service Description
A clear description that is derived from the CSIRT mission statement must be put in place.

CSIRT Type	Nature of Mission	IR Service Objective
Corporation	Improve corporation's information infrastructure and reduce risk of intrusion	Provide a centre of support in incident response for network administrators and system users.

4. Typical Corporate CSIRT with mission.

Objective
To achieve a clear description, the definition of the objective must also be clear.

Definition

The IR service is composed of four functions i.e. Triage, Incident, Announcement and Feedback.

Availability

The Availability of a service is about "Who can contact when?" but also "under what conditions". Quality Assurance sets the standard of expectation from the service.

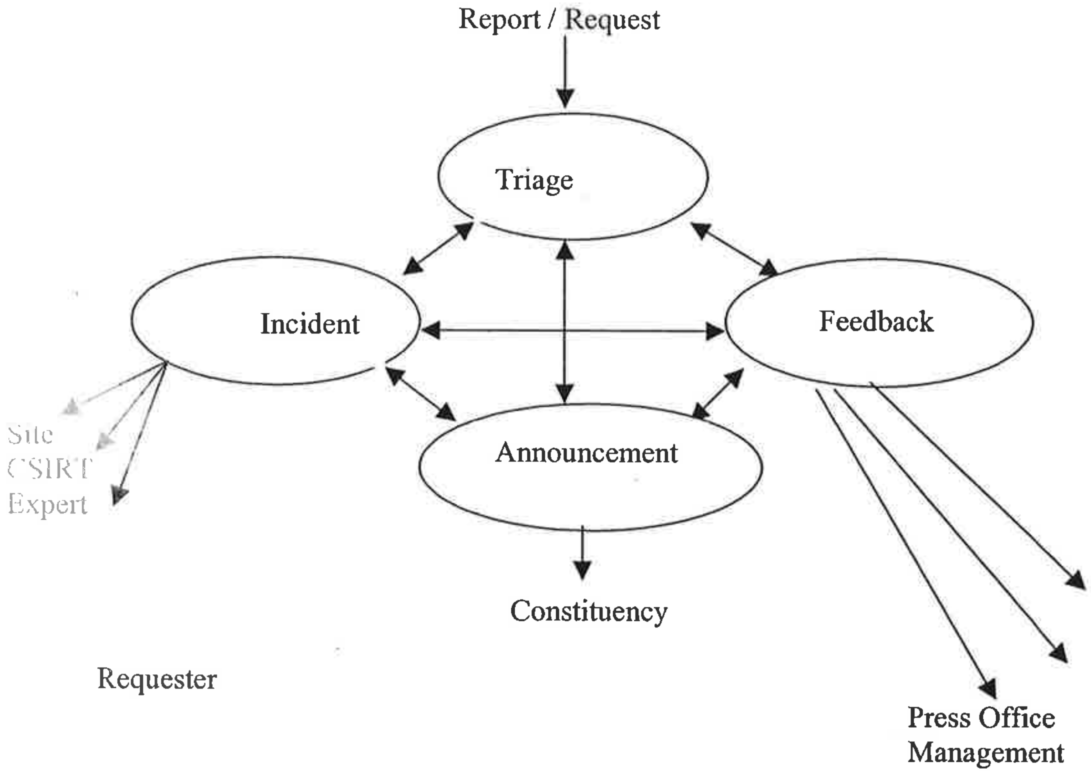
Interactions and Information Disclosure

The users of the service need to understand what interactions take place between the CSIRT and how the information, especially disclosure is handled.

Interfaces with Other Services

The criteria of information flow depend on the type of service that is provided and how it interacts with other services.

IR Service Functions Overview



Interactions

As a large proportion of the activities of a CSIRT involve interactions with other parties, it is necessary to have points of contact in place. It is of equal importance that this interaction is carried as securely as possible i.e. ensuring integrity, confidentiality and authenticity

Information Handling

Information plays a central role in incident resolution. Therefore, effective information handling is crucial. This entails collection, verification, categorisation, storage, sanitisation, disposal and disclosure.

Team Operations

All of the above depends on operational elements, policies, security management and staff issues being in a proper structure.

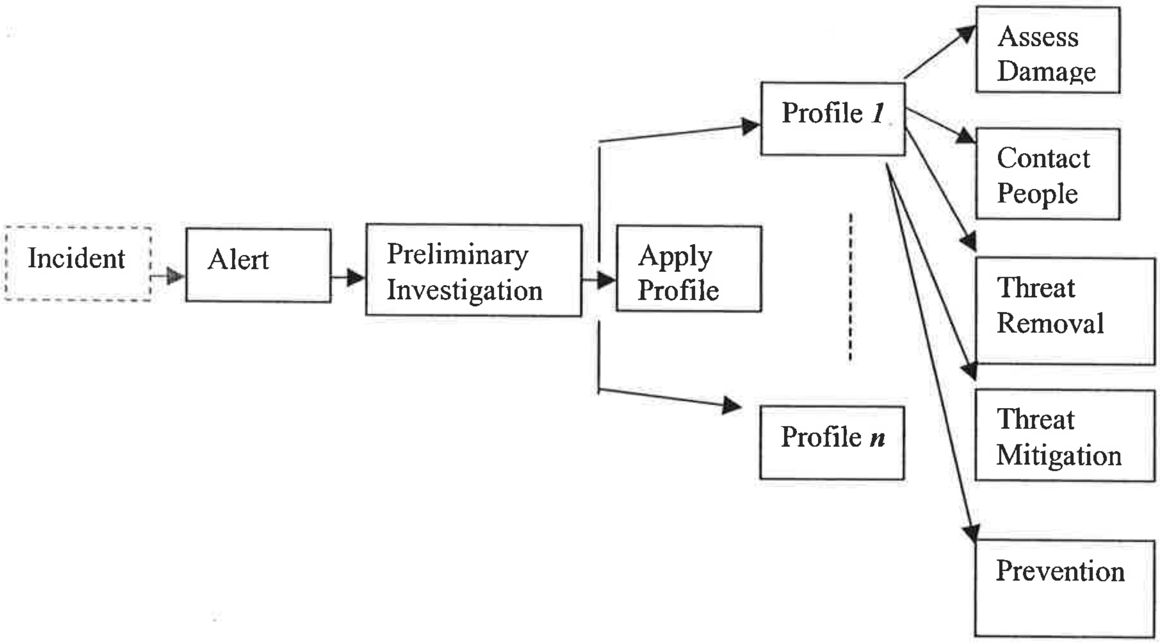
5. Conclusions

The four models listed above will have to be designed and built. These will provide the absolute information that is required to achieve the research objective i.e. building a forensic methodology that will facilitate the construction of a detailed profile of the Cybercriminal.

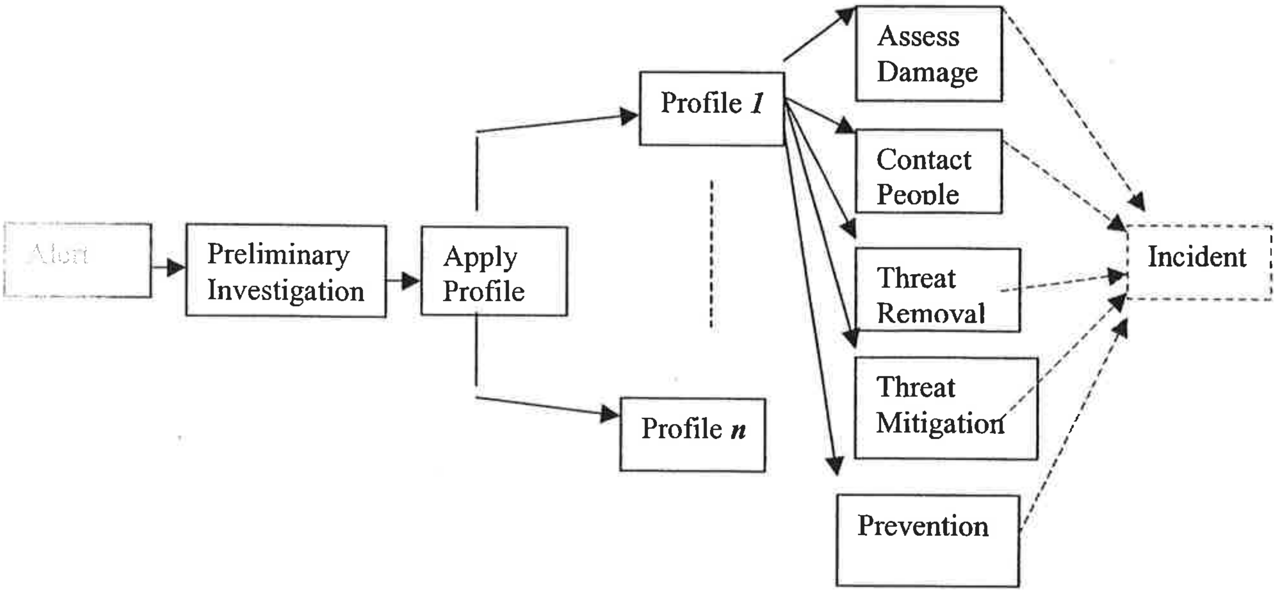
The Adversary model will provide us with information on the perpetrators of cyber attacks. We will learn of their motivations i.e. financial, political, revenge etc. The Attack model will provide an insight into what techniques and methods are used by these individuals to launch attacks. This will reflect changes or developments in technologies used for attack. The predictive model will form the basis of being able to foresee or anticipate future attack. This will be based on trends or cycles of activity that can be observed from logged output of network traffic and activity.
The gathering of data and its statistical analysis will provide the capability of forecasting impending attack with relative confidence levels. The risk model provides an essential method of evaluating the resource, asset or service provided that is to be secured from attack. The evaluation is the value of the item, from the company perspective. This could be customer confidence, stock value, credit card information, money, and intellectual property etc.

In order to quantify and qualify the information provided by the models, it is necessary to measure it according to a metric system. This will have to be developed to provide an indication of severity, level of aggression, source, intent and the type or profile of the attack. This will facilitate the drawing up of a Computer Incident Response Procedure i.e. a forensic methodology. So when an incident occurs, the basic sequence of events that is encapsulated in the forensic methodology can be carried out by the CSIRT, see below (Figure 5, this is a crude representation of the sequence of events). However, this is an iterative process and over time, CSIRT members will become more proficient at their work. Assisted by artificial intelligence capabilities, a situation will arise where incidence occurrence can be predicted with relative ease and confidence (Figure 6). Internet security, from a corporate perspective, will no longer be a random quessing game but a well-rehearsed and defined procedure.

This methodology can provide assistance to the legislators. Cybercrime is relatively new in this jurisdiction and since there is very little legal precedent for reference, it could be regarded as being "unchartered territory". As a result of this lack of knowledge, Cybercriminals can operate with impunity. The methodology can provide support and guidance to help redefine aspects of the law that are concerned with Cybercrime. Thus providing the first step to properly policing the Internet.



5. Incident Event Sequence Diagram



6. Incident Event Sequence Diagram

References

[1] Figure 1: "Threat and Vulnerability Model for Information Security", Report to the President's Commission on Critical Infrastructure Protection, 1997

[2] Figure 2: "Attack Modelling for Information Security and Survivability", Carnegie Mellon University/Software Engineering Institute, March 2001

[3] "Defining a Risk Assessment Process for Federal Security Personnel", Kathleen Federico, January 26, 2002

[4] "Challenges of Predictive Analysis for Networks", CERT Analysis Center, Timothy J Shimeall , Casey J. Dunleavy and Linda Pesante

[5] "Handbook for Computer Security Incident Response Teams (CSIRTs)", Carnegie Mellon University/Software Engineering Institute, December 1998, West-Brown, Moira .J, Stikvoort,Don , Kossakowksi, Klaus-Peter

[6] "Symantec Internet Security Threat Report, attack trends Q1 and Q2", Symantec Enterprise Security, 2002