CYBER-CRIME CONTROL, PREVENTION AND INVESTIGATION

A PhD Research Proposal

Submitted to

Cranfield University
College of Management and Technology
Defence Academy of the United Kingdom
Shrivenham SN6 8LA
United Kingdom

On July 31st, 2013

By

Engr. Effiong Ndarake Effiong,

CEng, MBCS, CITP, CEH, CHFI, MCSE, CCNA, MCTS, NCLA, DCTS, MIAM, B.Sc., M.Sc., ACE, Security+

Chartered Engineer, Chartered IT Professional

CYBER CRIME CONTROL, PREVENTION AND INVESTIGATION.

Preamble:

Over dependent of Governments and Businesses in technology give birth to the rising wave of cybercrime. Cyber terrorism is also on the increase. In the near future, wars between nations will be shifted from the physical combat to cyber space. Cyber wars will be valuable tools in the hands of the enemies against world powers; cybercrime will also be a million dollar business. In the light of this, we will need clear and concise techniques in fighting cybercrime thereby reducing it to the barest minimum. This crime can be difficult to control or prevent as the attackers are often times faceless, the attacker can be your next door neighbor or a person in a different geographical location or continent. This type of crime can be targeted toward Government, Agencies, Ministries, and Businesses irrespective of size and even individuals. The skills required of an attacker is dropping by the day as there are freely available and downloadable tools on the internet that even script kiddies can download and run against any vulnerable target without understanding what the tools does. Attacks techniques are also getting sophisticated as more and more tools are out there that try to make the attacked extremely difficult if not impossible to detect.

With this, it is therefore my desire to research into ways of controlling, preventing and investigating where possible the cybercrime activities of the cyber space, thereby making our cyberspace maximally secured since there cannot be total security. By so doing it will boost our economic gains from the cyber space.

INTRODUCTION:

Cybercrime is a crime involving computers or digital devices, in which a computer can be either a target of the crime, a tool of the crime or contain evidence of the crime. Since most information processing these days depends on the use of information technology, the control, prevention and investigation of cyber activities is paramount to the success of the Organizations, Government's agencies and individuals. The procurement and retention of highly skill cybercrime expert by Government and Business Enterprises cannot be overemphasized. This will ensure compliance with international acceptable standard of usage of computer and other technological devices in the work places.

Although prevention as they say is better than cure, irrespective of the deterrent measures to prevent and or control cybercrime, there may still be breaches, where this occur, Forensics Experts will be called in to conduct a sound digital forensic investigations, analysis, documentation and reconstruction of the crime scene and present the evidence of the findings to

the appropriate authorities or the Jury as the case may be, that can lead to arrest, prosecution and conviction of the culprit.

Digital Asset need to be protected to guaranteed it Confidentiality, Integrity and Availability (CIA triad). Information stored in Human brain, electronic devices physical media and those on transit needs to be protected. Hence the urge for this research topic.

This research will therefore be broken down into three major categories namely:

1. **Cyber-Crime Control (CCC)**
2. **Cyber-Crime Prevention (CCP)**
3. **Cyber-Crime Investigation (CCI)**

Cyber-Crime Control (CCC):

This will deal with the formation of adequate policies to control cybercrime activities. The policies should also spell out appropriate punishment for cyber criminals if convicted by appropriate court of competent jurisdiction, this will be a deterrent measures to other who may want to engage in the act.

Cyber Crime Prevention (CCP):

In this section, I will be focusing here on the training of both users and administrators of the cyber space, best practices, security awareness etc. to prevent cyber incidents, however, the underground hacking techniques will be taught to security administrators and managers. Hackers mind set will also be a focus, the tools and techniques of the hackers will be exposed and the various ways of preventing and detecting cybercrime activities will be the core of the training to be evangelized here. Bearing in mind that users are the weakest security link.

Tools that will help in this will be both commercial and open source tools which will include but not limited to:

Core Impact Pro, Immunity canvas, Metasploit pro and framework, BackTrack 5r3 and Kali-Linux, email tracker pro, Saint, Cain and Abel, Nmap, Nessus, NetCat, GFI Languard, Retina, etc. the list is endless, the good thing is that majority of them are free and open source.

Cyber Crime Investigation (CCI):

Since there is no such thing as total security and an unbreakable system, I have to assume that at one point or the other, the system can be broken into irrespective of the controls and prevention. However, should this happen. The issue of investigations set in, unraveling the mysteries behind the attack, tracing the hacker through the cyber space. This is a very interesting module as

forensic investigation of both network based attacks and computer systems including mobile devices will be covered. From identification, collection, preservation analysis, documentation and presentation of facts of cybercrime investigation will be a treated. Here I will also look into

Victimology:

- Victimology is the study of victims of crime and the psychological effects on them.
- Victimology may not necessarily means a person, it can be a server, bank, website, ministry, agency or any other target

Links to the Victims

Links to the victim may include the following:

- Geographical
- Work related
- Schedule oriented
- Hobby related
- Family related
- ✓ A careful study of the victim will reveal why the victim was chosen and what risk did the offender take to get the target
- ✓ As a rule the victimology research will include a thorough search for cyber trails. Neglecting to follow cyber trails may not only risk losing valuable evidence, may also undermine professional competence for negligence.

Tools that will be used here will include but not limited to the following

Encase, Access Data FTK, Imager, Registry viewer and password recovery toolkit, DNA, all Access Data tools can be gotten from a single package called Access Data Ultimate Toolkit, ProDiscover, X-ways forensic, Sleuth kit, Autopsy, Raptor, SMART, Passware Kit, Simple carver, Data Lifter, Hardware write blocker and Duplicators, etc.

AIMS AND OBJECTIVE:

As cybercrime incidents are on the increase, and it menace is affecting both Government organizations, Individuals and businesses, the main aim of this research will be to find out the truth which about cybercrime that is hidden and which has not been discovered as yet as it relate to the rate of increase, the sophistication of attack, motivation of the cybercriminals and ultimately find a way of reducing cybercrime activities and it effect on businesses to the barest minimum. Where prevention and control is not totally possible, the research will focus on deterrent measures like recommending maximum and appropriate punishment for offenders. In this regard, the research will review the existing law and suggest amendments where necessary, develop a detail and acceptable measures of tracking the cyber criminals (tracing the hacker to the cyber space). Cyber Forensic techniques are the deal here. The research will be both descriptive and exploratory or formulative in nature.

RESEARCH QUESTIONS:

There are many research questions that need to be address in detail, issues like

What are we trying to protect? Our Assets, Network Infrastructure, Availability Network Resources, Confidential Personal Data can be classified into three categories.

i. Information stored electronically or on transit in the network (digital)
ii. Information stored physically (hard copies)
iii. Information in human brain.

There may be more to it that need to be researched into, all these and many more need maximum protection.

Why are intrusions so often successful? There is need for us to know why we often fall for these cybercrime activities, issues concerning our cybercrime detection, response, and escalation process needs to be reviewed, policies where applicable needs to be thoroughly looked into, sometimes, there may be no procedures for proactive auditing, or event management, focus have been may have been shifted to reactive measures to detect what happen which are often not successful. Use of authentication and/or authorization systems, Ignorance of logical and/or organizational boundaries within a network Infrastructure and many others will form the basis of research in this aspect.

What are the greatest challenges that we face today? Environment complexity, new technologies, new threats and exploits, limited focus on security, limited budget for security, shortage of qualified security experts. There is no doubt that what some mobile devices like smart phones and others can do today, some desktop and even servers computers of the early day were not able to do. There must be a perfect trade off and an acceptable level of compromise between the security, functionality and ease of use.

Why are most attacks gone undetected? Most companies don't even know if they have been a victim of cybercrime activities or not, this is very alarming, knowing fully well that been hacked is bad, but not knowing if you've been hacked is worst. This research will dig deep into why attacks often gone undetected, again focus will also be on detection, response, escalation and monitoring mechanism. Although lack of skilled personnel in cyber security or incident response may be a cause, we'll find out!

Why are attackers not getting appropriate jail terms? Sometimes even when intrusion is detected the offenders are either not being detected or there is no enough evidence to convince the jury to convict a cybercriminal. Where there is evidence, the get light sentence. There is no international law that operates everywhere. Whereas cybercrime is a global crime, there should be no geographical boundaries in implementing cyber laws as the entire cyber space should be regarded as a single entity for a single jurisdiction. The research will see what is obtainable, desirable and applicable.

What are the motivations for the cybercriminals? Although cyber criminals often carry out their activities for financial gains, there are some who does what they do for other reason's other than financial gains; it may sometimes be for personal reasons either as a retaliation for unlawful termination, for pride or political reasons, whatever the motivation maybe, it can also be a pointer to the type of evidence, where and how to collect evidence for a successful prosecution.

What risk is the attacked willing to take in other to get the target? The attacker must be willing to take certain amount of risk for the attack to be successful, this we must find out.

How can we tired the loose ends and make our cyber space more secure that it is currently? This very question will lead us to the aim of this result, making sure that our cyber space is secured, and to ensure that offenders are punished accordingly.

LITERATURE AND KNOWLEDGE GAP:

Documents such as but not limited to the following will be our anchor for this research project. The United Kingdom Legislation and the United States Legislations will be our main focus, Other laws like The Securely Protect Yourself Against Cyber Trespass (SPY) ACT, the U.S. Federal Laws, United Kingdom's Cyber Laws, European Laws, Japan's Cyber Laws, Australia: The Cybercrime Act 2001, Indian Law: The Information Technology Act and Indian Evidence Act, Germany's Cyber Laws, Singapore's Cyber Laws, Belgium Law, Brazilian Law, Canadian Laws, France Laws, Italian Law, Nigerian Evidence Act, and the Freedom of Information Bill and Other laws like USC 18, the Privacy Act 1974, Federal managers financial Integrity Act 1982, Freedom of Information Act, Federal Information Security Management Act (FISMA), USA Patriot Act 2001, Government Paper work Elimination Act (GPEA), UK Computer Misuse Act 1990, Data Protection Act 1998, Police and Justice Act 2006, Health Insurance portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA), SOX, FACTA, Their respective website will be visited for research purposes, **my concentration will be on what constitute a crime and the penalties for various crimes committed.**

METHODOLOGY

As it is indicated above, the problem is complex and the method and methodology to be used in resolving the issue will be diverse and far reaching, the following methods will be used to collect data for analysis.

1. Direct Observation: we will collect data by observing the environment and users alike without actually interviewing them.
2. Organize seminar and conferences inviting some of the season ethical hackers, penetration testers, computer forensics investigators, legal luminaries and policy makers in the industry, there will share ideas and answers questions, valuable datas will be collected by this method.
3. Online chatting with the underground community, discussions and posting of questions in the forums, creating a virtual scenarios and asking for help will be immensely valuable.
4. Setup a research Honeypot to attack attackers to attacked the box and we can learn more about their attacking techniques and various actions they took in compromising a system.
5. Survey and questionnaires, taking surveys online and sending the links to the survey to security professionals will be adopted. It therefore implies that there will be website specifically design for this research survey.
6. Through personal interview: I will conduct a personal interview to some selected corporation and agencies with a set of predefine questions that will help in answering the questions and providing the solution to the problems of cybercrime. Persons who maybe

important to the survey but could not be reach physically may be contacted by phone for the interview.

7. By mailing the questionnaires. I will mail out the questionnaires where necessary to identified personalities who may not be rich physically or through phone. A mailing list of selected person will be compiled prior to the time of collecting data and will be used accordingly.
8. Excursion to Computer crime lab, interaction and interview with the computer forensics examiners. At least two of such labs would be visited, examples of proposed labs to be visited include but not limited to Federal Bureau of Investigations (FBI) computer crime lab, MI5, Scotland Yard, or London Metropolitan Police Crime lab will be a valuable source of data collection.
9. Attending court proceedings where cybercrime cases are tried and judgments of cybercrime related cases delivered will be a source of evidence collection and will help in understanding of what the judges how such cases are tried, understanding of the applicable law and what is necessary to convict a cybercriminal with digital evidence.

Depending on the financial resources available and the time frame to complete the task, a few options from above will be taken, I will prefer that most if not all of the defines methods be taken will respondent from across the globe and from small, medium to large enterprises. Data collected will be systematically and logically analysis, where possible I may come up with hypothesis for further testing, proof or disproof existing hypothesis as the case may be.

POTENTIAL IMPACT OF THE RESEARCH:

This research will make constant progress possible or even give us victory in the fight against cybercrime. It will also inculcate innovative and inductive thinking and it promotes the development of security consciousness in organization.

The outcome of this research will have its special significance in solving various information security related problems of Government Agencies, the business community and individuals alike. When all these are achieved, we will end up making our cyber space a safer place for business transaction, there by indirectly affecting the economy. The internet will be a better and safer place for transactions and users will be better informed of security tips for the safety of their transactions.

A detail report will be written and submitted as the case may be.

These and many more are expected to be carried out during the research period.

I will try to cover the topic in detail with many other areas that needs to be research into, to do justice to the topic.

Thank you.

Engr. Effiong Ndarake Effiong