Analyzing the impact of cyber crime on the department of defense research paper e...

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Abstract

Computer technology has evolved over time with increase in processing speed and ease of application for different purposes. With the evolution of computer and internet technology, so has the evolution of criminal activities evolved. In the past, for one to be able to hack effectively into a system or a message, it would require uninterrupted exposure to over ten computer workstations incurring costs that range from $ 10, 000 in terms of time consumed and resources. Currently there are faster computers and super computers that make processing easier and thus ability to attack target takes less time. From time to time, the Department of Defense acronym DOD comes under attacks ranging from virus and worm attacks to brute force attacks, to hackers eavesdropping, stealing classified information and some denial of service attacks among others. The emergent risks of cyber-crimes

cannot be overlooked and thus policies have been created to ensure that cyber-crime is dealt with according to the law.

Cyber crime

Introduction

According to Price (1999), internet connectivity started back in the year 1969 where the military were mandated to make connectivity between different departments for information sharing (p. 103). Over time, internet connectivity has evolved to become a worldwide platform where information is shared and connections are made. With this respect, some of the users are not genuine in their work and instead of using the internet constructively, opt to destructively use the internet and make efforts to destroy systems by infecting them with worms, viruses through brute attacks of exploitation of flaws within a cryptographic algorithm (Price, 1999, p. 103). The Department of Defense has not been spared in these forms of attacks as more people try to infiltrate into the department's database and steal some information or just for the fun of intrusion. In this research paper, the learner will make analysis of the Department of Defense's scale of impact that an intrusion would have on it and the regulatory requirements, liability issues as well as policy issues during and after cyber-crime attacks.

About Department of Defense

The Department of Defense is one of the oldest departments in the United States (DOD, 2012). The Department of Defense traces its roots in the pre-revolutionary era and has evolved over time (DOD, 2012). Due to the sensitivity of the department, there has been evolution in the department as

well as growth to become one of the largest institution and the greatest employer in American history employing millions both in the military and civilian status (DOD, 2012). The nation’s defense is reliant on the Department of Defense being at the right place at the right time and ready to respond to real-time threats with defensive installations being in place and having the right quantity of response gear to protect the nation’s vast resources (DOD, 2012). The mission of the Department of Defense is to provide multilateral defense force that is well equipped and capable of deterring war as well as provide security to the country (DOD, 2012). The headquarters of the Department of Defense is at the Pentagon that has ease of access between offices and having about 1. 7 miles span of corridors therein (DOD, 2012). Under the directive of the U. S. president, the Secretary of Defense is in charge of the Department of Defense as well as being the principal defense policy advisor to the president and the Secretary of Defense is given the mandate to exercise authority, control and direction over the Department of Defense (DODO, 2012).

The DOD has in the past come under attack that has left the department almost crippled. The threats that are posed to the department of Defense range from physical attacks like it happened on September 11, 2001 on the department’s headquarters, Pentagon. However most of the attackers like to remain anonymous and on the net where tracing their physical location is tasking and the possibility of escape after initiating an attack is imminent. The most common types of attacks are computer viruses and worms that keep evolving as the technology evolves. Another form of threat is eaves dropping by either human or non-human agents so as to gain access to

potentially confidential information as well as classified information. Overill (2003) and Price (1999) identified that one of the fundamental attack on the Department of Defense is having hackers who try to infiltrate into the DOD database that contain classified and personal information as well as records of all military operations in the past, present and in the future and potentially sensitive information that cannot be release to the media.

Hackers exploit flaws that might be present on the encryption algorithm like most viruses locate holes in operating systems like Windows operating system and using it as an access route to the entire system (Overill, 2003) and (Price, 1999). In some instances, there is utilization of brute force attacks to gain access to the systems (Overill, 2003) and (Price, 1999). Some of these attacks are quite systematic such that some hackers major in breaking through the firewalls and encryptions upon hundreds of acres of hardware on the Department of Defense's system while the next hackers make use of these breaches to steal information from the department's database and servers.

Regulatory Requirements

As early as 2002, in a survey on the impact of security breaches on 503 organizations show that about ninety percent of these organization had reported security breaches while over seventy percent of these business enterprises found it hard to continue doing their usual business after these breaches (Chang & Yeh, 2006). It was estimated that the total cost of these breaches amounted to a whopping $ 202 million as reported by CSI/ FBI (2003; Chang & Yeh, 2006). There are voluminous amounts of attacks and

their numbers keep increasing by the day as more people indulge in this quest, some for prowess hype and others for fun. A major problem is the fact that the financial implications that come after an attack are enormous.

With respect to this, Hinde (2003; Chang & Yeh, 2006) argues that as far as security is concerned, it is an issue for both the organization as well as the people since the effects have a way of trickling down to these people. As per of regulatory requirements, it is anticipated that security measures should be taken to either detect, prevent as well as minimize the impact of such attacks (Chang & Yen, 2006). There is one matter that brings in a whole lot of issues as far as regulation is concerned. By definition, the term jurisdiction is used in the essence of the power of a State to make decisions that affect people; their property which includes the clause that bar's the State from interfering with affairs that are domestic (Zekos, 2002, p. 57). However, flaws have been identified as to the extent of application of this term especially when dealing with threats that might emanate from regions outside of the physical reality of jurisdiction (Zekos, 2002, p. 57). For example, in Overill (2003), the United Kingdom Computer Misuse Act 1990 defines a basic hacking offense as an authorized modification of information or systems aspect (p. 64). Additionally, it continues to bar active defense force from retaliatory hacking on an intruder's computer since that would amount to a foul on the former offence (Overill, 2003, p. 64). The law is similar to that of the United States and thus, despite the urge to retaliate, the regulation demands otherwise.

According to Loch et al. (1992; Chang & Yeh, 2006), there are four dimensions of an information systems' threat that the Department of

Defense utilizes in threat eradication. First, there is identification of the source of the threat, which can either be an insider threat or from outside. Secondly, upon identification of the source, there needs to be clarification of the perpetrator that can either be a human agent or a non-human agent for which appropriate actions are taken to locate the perpetrator. Thirdly, the intention for the attack is identified as to whether it was accidental or intentional and finally an evaluation of the consequences of the intrusion like DoS attack, disclosure, destruction or modification of information (Loch et al. 1992; Chang & Yeh).

Kanuck (2010) adds to the debate on online jurisdiction terming it as a misnomer as far as virtual jurisdiction is concerned (p. 1573). Infrastructure as well as the contents therein for a predefined and globally accepted cyberspace is subject to the nation’s jurisdiction as the battle ranges by governments trying to extend their virtual jurisdiction into new realms (Kanuck, 2010, p. 1575).

Liability Issues

There are liability issues that are raised as far as security intrusion by scrupulous people. According to the United States’ National Information infrastructure Protection Act 1996 (NIIPA 96) that was created as a replacement for the former Computer fraud and Abuse Act 1986, bars the DOD from imposing posse comitatus, by unilaterally taking actions within the United States region against the United States Citizens (Schwartau, 2000; Overill, 2003). This means that although there are imminent attacks, the Department cannot make a unilateral decision that will block a substantial

number of U. S. citizens from accessing some information and communication infrastructure. This means that although threats are evident and imminent, there should be ways of isolating and eliminating the threats individually and this call for proactive threat and intrusion detection before substantial damage is done by deployment of advanced security control software and surveillance as noted in Kankanhalli et al. (2003; Chang & Yeh, 2006). Since some threats might emanate from within the agency, it is expected that the agency carryout education on its staff as to what might constitute illegitimate use of the system and the implications on the infrastructure as well as the individuals (Chang & Yeh, 2006).

Policy Issues

There are various policies that have been issued to ensure that there is proper utilization of the rule of law and proactive surveillance of the systems. In a research on the number of students enrolling for technical courses on computing, there was noted a steady decline from the peak in 2004 to almost half of that enrolment in 2007/ 2008 intake, an issue that has raised many questions (Cyberspace Policy Review, 2009, p. 14). Due to the magnitude of the impact of the cyberspace threats, there has been an urge for the increase in the federal workforce on the information technology section to be coordinated by ICI-IPC (Cyberspace Policy Review, 2009, p. 15). Secondly, the policy demands an increase in cyber security education beyond the workforce to the departmental heads and management (Cyberspace Policy Review, 2009, p. 14).

The policy also demands sharing of responsibilities as far as cyber security is

concerned. According to the Homeland Security Act of 2002 (HSA) it is the responsibility of the Department of Homeland Security to protect critical national infrastructure across all sector divide especially telecommunication and information technology infrastructure (Cyberspace Policy Review, 2009, p. 72).

Conclusion

References

Baldwin, F. N. Jr. (2002). Money laundering countermeasures with primary focus upon terrorism and the USA Patriot Act 2001. Journal of Money Laundering Control, 6(2), 105-136. Retrieved from http://search. proquest. com/business/docview/235947606/fulltextPDF/134DB6F9DC050A0C7F1/5? accountid= 45049

Chang, A. J., & Yeh, Q. (2006). On security preparations against possible IS threats across industries. Information Management & Computer Security, 14(4), 343 - 360. doi: 10. 1108/09685220610690817

CSI/FBI (2003). CSI/FBI 2003 Computer Crime and Security Survey. San Francisco, CA: Computer Security Institute.

Cyberspace Policy Review. (2009). Assuring a trusted and resilient information and communications infrastructure, Department of Defense. 1-76.

First anniversary of military campaign in Afghanistan; Al Qaeda attacks in Bali. (2003). Foreign Policy Bulletin, 14(1), 238-287. doi: 10. 1017/S1052703600006122

Hinde, S. (2003). The law, cybercrime, risk assessment and cyber protection.

Computers and Security, 22(2), 90-95.

Kankanhalli, A., Teo, H-H., Tan, B. C. Y., Wei, K-K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23, 139-154.

Kanuck, S. (2010). Sovereign discourse on cyber conflict under international law. Texas Law Review, 88(7), 1571-1597. Retrieved from http://search. proquest. com/docview/722437541? accountid= 45049

Loch, K. D., Carr, H. H., Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly, 16(2), pp. 173-186.

Overill, R. E. (2003). Reacting to cyber-intrusions: The technical, legal and ethical dimensions. Journal of Financial Crime, 11(2), 163-167. Retrieved from http://search. proquest. com/docview/235988535? accountid= 45049

Posthumus, S., von Solms, R. (2004). A framework for the governance of information security. Computer & Security, 23, 638-646.

Price, S. A. (1999). Understanding contemporary cryptography and its wider impact upon the general law. International Review of Law, Computers & Technology, 13(2), 95-126. Retrieved from http://search. proquest. com/docview/213376068? accountid= 45049

Schwartau, W. (2000). Can you counter-attack hackers?. 7th April, Retrieved from www. cnn. com/2000/TECH/computing/0407/self-defense. idg

Zekos, G. I. (2002). Legal problems in cyberspace. International Journal of Law and Management, 44(5), 45-102. Retrieved from http://search. proquest. com/docview/196364963? accountid= 45049