A REVIEW OF RESPONSIBILITIES OF INTERNET SERVICE PROVIDERS TOWARD THEIR CUSTOMERS' NETWORK SECURITY

SHUAIBU HASSAN USMAN[1]

[1]Department of Management and Information Technology
Abubakar Tafawa Balewa University Bauchi, Nigeria
Email: hasusman@gmail.com

ABSTRACT

The use of the internet in the 21st century is indisputable to the people worldwide. People have become dependent on the internet's connectivity to conduct business, share information, and collaborate. Yet, some people use the internet as an avenue for illegal activities such as breaking into other people computers or networks, damaging and stealing information, and blocking or denying legitimate users from services they subscribed. Actually, these illegal activities are made possible because the internet is based on all end users being trusted to act appropriately [20]. Nevertheless, security experts have suggested in some researches that Internet Service Providers (ISPs) should be called to the chain of security responsibilities because they believe that ISPs are in suitable position to protect (police) the internet. They argue that ISPs control the gateway through which internet security breaches pass to their customers. Moreover, they consider that ISPs can use advanced technologies to detect illegal activities. In addition, ISPs have broader knowledge of cyber threats that affect internet users and businesses. The purpose of this paper is to review literatures on the responsibilities of ISPs in securing their customers' network, and find out whether there are legal provisions, or liabilities that are bindings on the ISPs to provide security for their customers. The questions here, are ISPs responsible for end users' network security? Are there legal provisions binding ISPs to provide the network security to their subscribers? In addition, what are the recommended security considerations they should be responsible to provide?

Keyword: *ISPs, Users, Internet Security, Legal provisions, Responsibilities*

1. INTRODUCTION

The use of the internet in this 21st century is indisputable to the people worldwide. People have become dependent on the internet's connectivity to conduct business, share information, and collaborate. Therefore, the internet is the interconnection of different networks together with the help of Internet Service Providers (ISPs). However, the interconnection of these networks together poses security challenges. Some people use the internet as an avenue for illegal activities such as breaking into other people computers or networks, damaging and stealing information, and blocking or denying legitimate users from services they subscribed. Actually, these illegal activities are made possible because the internet is based on all end users being trusted to act appropriately [20]. Security is the major concern that surrounds the internet users.

This paper aimed at looking into the responsibilities of the ISPs in securing their customers' networks. Although, many people have the wrong perception that network security is the responsibility of users only. However, the ISPs have a vital role to play when it comes to the issue of network security. Because it is unlikely that most Internet users will have the technical expertise required to properly patch, or upgrade operating systems and software, update antivirus programs, and install hardware or software firewalls. It is in the area of technical security expertise that ISPs have a responsibility to their customers [23]. In addition, Hathaway and Savage said in their report that "ISPs own and operate a critical infrastructure that facilitates the delivery of essential goods and services. As intermediaries and stewards of this infrastructure, they have an important role to play in fostering security. Given the rapid rise in the Internet's complexity and the critical role the Internet has come to play in the global economy, providers should be obligated to be stewards of the global enterprise. We can no longer be one click away from an infection, disruption, or worse yet, no service” [15].

1.1 Statement of the Problem

Internet attacks are the cause of damage to information and loss of profit to many individuals and businesses in the world. This could be from theft of intellectual property, lost business and productivity for network outages and emergency response, and clean up costs [11]. There are different types of attacks that include Brute force, Denial of service, back door, Guessing password, sniffer, Trojan horse, virus, etc. furthermore, the internet provides different sources of information on security defect in hardware and software. For example, attackers can use search engines on the internet and quickly find information describing how to break into various systems by exploiting known security weak points of the hardware or software. Attackers may also use automated tools to query network systems, then exploiting any identified security weaknesses to gain unauthorized access to the network [2].

However, to provide defensive measures against these attacks, firewall and network filtering technology must be implemented to secure the network. In addition, the use of security monitoring that provides a means by which to confirm that information resource security controls are in place, effective, and are not being bypassed is very important. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. Early detection and monitoring can prevent possible attacks or minimize their impact on computer systems [19]. Accordingly, internet users generally do not have adequate knowledge and expertise to implement these security infrastructures. Besides, the internet users usually do not know that their network systems are compromised, this constitute part of the problem. For example, Malware may be distributed and used in many ways, including e-mail messages, USB devices, infected websites, malicious advertising, and browser vulnerabilities [16]

Furthermore, Security measures that address end users directly – includes creating awareness and information campaigns, but they have proven to be insufficient to reduce the overall problem [17]. Some surveys indicated that internet users adopt more secure practices, such as using anti-virus protection, a firewall, and automatic security updates for their software [12]. The attackers also formulate their new strategies to perpetrate the evil act. The network result is an inadequate defense against malware infections: while the capabilities and practices of end users are improving, they lag behind the increasingly sophisticated threats of attackers [17].

Therefore, security experts have suggested in some researches that Internet Service Providers (ISPs) are in better position to provide internet security to their Subscribers, as they are the gateway through which internet security breaches pass to their customers. Moreover, they believe that ISPs can use advanced technologies to detect illegal activities. In addition, ISPs have broader knowledge of cyber threats that affect internet users and businesses. Hence, the need for ISPs to shoulder more responsibilities of the Internet has become more obvious according previous research [8] [21] [23] [15].

1.2 Purpose of this paper

The main objective of this paper is to review literatures on the responsibilities of ISPs in securing their customers’ network. Furthermore, the paper seeks to find whether there are legal provisions, or liabilities that are binding on the ISPs to provide security for their customers. To achieve this aim, three questions were developed.

1. Are ISPs responsible for the security of their customers’ network?
2. Are there legal provisions binding ISPs to provide the network security to their subscribers?
3. What are the recommended security considerations the ISPs should be responsible to provide?

1.3 Methodology

The method used in this paper was secondary source of data. Where online articles and journals were reviewed to provide the solution to the questions raised in this paper. The main reason of using this type of method was to review previous research on the ISPs’ responsibilities in provision of security to their subscribers, and find out whether there are legal provisions for liabilities that are bindings on the ISPs to provide such service to their customers.

1.4 Internet Service Providers

Internet service provider (ISP) is a company that provides Internet connections and services to individuals and organizations. In addition to providing access to the Internet, ISPs may also provide software packages (such as browsers), e-mail accounts, and a personal Web site or home page. ISPs can host Web sites for businesses and can build the Web sites themselves. ISPs are all connected to each other through network access points, public network facilities on the Internet backbone [5].

According to Jennie Ness, a Regional IP Attaché at U.S. Commercial Service reported that the Functions of ISPs include:

1. Transitory communications (serving as an information carrier): ISP acts as a mere data conduit, transmitting digital information from one point on a network to another at a user's request.
2. System caching: Retaining copies, for a limited time, of material that has been made available online by a person other than the ISP. Caching is technologically necessary to ensure Internet speed and efficiency, particularly in terms of providing rapid access to popular content without overloading servers.
3. Storage of information on systems or networks at direction of users (hosting): Allowing users to post materials and host website for users and
4. Information location tools (searching): ISP provides Internet search engines and Hyperlinks Internet directories [13]

2. LITERATURE REVIEW

A research by Rowe, Wood, Reeves, and Braun reported, "security experts have suggested that Internet Service Providers (ISPs) may be in a good position to cost-effectively prevent certain types of malicious cyber behavior, such as the operation of botnets on home users' and small businesses' computers. Similar to a neighborhood security checkpoint that provides a measure of security to all houses branching off the private roads therein, individual Internet users would be much better protected if their ISP played a larger security role"[4].

Allan and Jim argued that ISPs have a responsibility to help protect user computer and data from malicious attack. They provide a variety of services to user and must employ best practices to ensure security [21].

The role of the internet service providers is changing and expanding, ISP are transformation themselves to offer a wide range of service to their subscribers. They protect customs from attack coming from infrastructures (tool) or other customers. Each ISP has to ensure that certain security practices are followed to ensure that their network is operationally available for their subscriber [6].

Orill said, "an ISP's position as gateway to the Internet requires it to assume a host of legal and ethical duties. The ability of anonymous users to freely exchange information over the Internet creates legal responsibilities for ISPs to act in the public's interest. Customers rely on the Internet for personal communication, information, and to conduct business, giving ISPs a duty to deliver reliable service and access to the websites and services their customers depend on" [14].

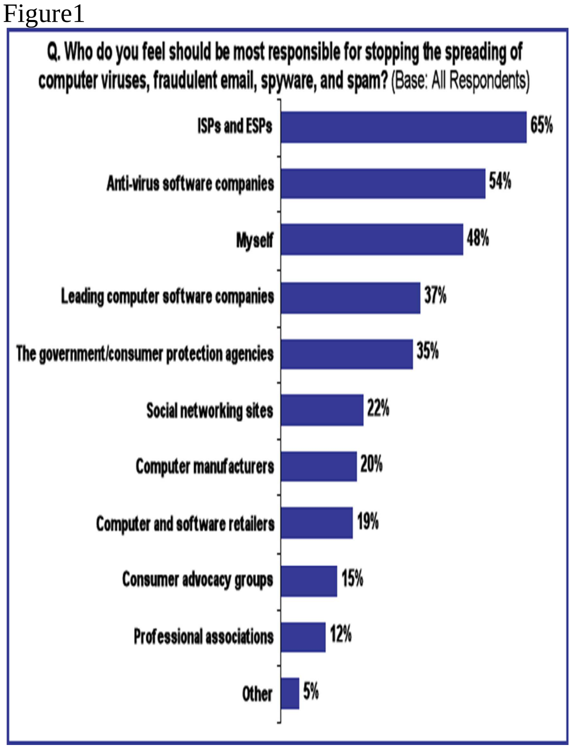
3. DISCUSSIONS

Question 1: Are ISPs responsible for the security of their customers' network?

It has become obvious through previous research that there is no law mandating ISPs to provide users with secure internet access, however, there are laws that deal with privacy [23]. Although, there are number of people that believe ISPs are in good position to handle the security of the internet for their users since there are the intermediaries who provide Internet access. They believe that users do not have knowledge and expertise to handle security of the internet [23] [4]. Even they users have the knowledge; they lag behind the increasingly sophisticated threats of attackers [17]. In the same vein, Laura said, "the ISPs and intermediaries must bear some responsibility to maintain an Internet. They should and must maintain records that store a digital address of anyone who is entering their sites. This will allow law enforcement, investigators alike to trace an individual engaging in any illegality on the Internet" [1].

Therefore, it is assumed that ISPs are in good position to protect their customers' network because they connect users to the internet. In addition, they have the equipment and the expertise to monitor and block unauthorized or illegal access. The current suggestion from scholars is that ISPs can take cost effective steps to provide security for the internet users [23] [24]. The need for ISPs to intervene in security situation of internet has become obvious, as subscribers believe that they are responsible to stop the illegal activities of attackers. In the research conducted by MAAWG in 2010, 65% of the users indicated that their ISPs and ESPs are responsible for mitigating or stopping the spread of computer viruses, fraudulent emails spyware and spam in general, followed by antivirus vendors with 54% and user accounted for 48% (see Figure1) [18].

Figure1



Source: *MAAWG Survey* (*2010)*

Notwithstanding, some experts pointed out that holding ISPs solidly accountable for end users' security have it own downside. According to Purcell, "providing equipment and properly trained security professionals is a costly expense, there could be legal consequences once an ISP provides the user with security, and receiving cooperation from users in order to secure home machines could be difficult and time consuming for the ISP" [23]. Furthermore, Barriers preventing ISPs from becoming more involved include a variety of technical costs and legal issues, as well as uncertainty regarding who would pay these costs [4].

However, the ISPs have a role to play when it come to internet security. For example, if an ISP's network design is not properly secure, compromises could result in service disruptions to thousands of users. Moreover, if the system load gets too heavy, legitimate customers will get upset and leave then ISP loses income. In contrary, ISP-based security offers a new source of revenue as well as builds customer loyalty and reduce customer turnover [4]. "The steps that ISPs take to ensure security on their networks could also have a direct effect on the security of their subscribers" [23]. Therefore, it can be seen that ISPs have a vital role to play when it comes to security in order to retain customers and increase revenue, since their income generations are base on the number of customers that subscribe to them.

Question 2: Are there legal provisions binding ISPs to provide the network security to their subscribers?

Nowadays, internet security has become the foremost concern as the illegalities are in rising position such as spyware, hacking, virus, worm propagation etc. In view of this, many people blame ISPs for not taking responsibility of stopping and controlling these illegal activities on the internet, as they are the gateway through which internet virus and other illegal online activities pass through to their customers. The question here, are ISPs liable for handling of Internet security?

This paper found that there is no specific law putting ISPs liable for end users' security. Although, there are existing laws related to copyright, defamation, privacy, and similar crimes. Examples of these laws are; in the United States, the Communications Decency Act (CDA) and the Digital Millennium Copyright Act (DMCA) were thus passed respectively in 1996 and in 1998, while the Electronic Commerce Directive (e-commerce Directive) in Europe was adopted in 2000 [3]. However, the laws did not put the ISPs liable for the users illegal activities or end users' internet security instead were more of providing immunity for Internet service providers, which have created some controversies in legal system in these two continents. Farano said, "Over the past ten years, the potential liability of online service providers for third party content has raised one of the most spirited and fascinating debates in the legal arena, putting right holders, service providers and Internet users at loggerheads. In the United States and in Europe, lawmakers have endeavored to resolve this tension by enacting, more than ten years ago, a set of essentially consistent regulations – most notably the U.S. D.M.C.A. and the EU E-commerce Directive – aimed at fostering the growth of the digital economy, while not hampering the protection of IP rights in the digital environment. However, courts in Europe and in the United States are facing increasing difficulties in interpreting these regulations and adapting them to a new economic and technical landscape that involves unprecedented levels of online piracy and new kinds of online intermediaries. As a result, courts in Europe and in the United States have reached contrasting conclusions and have failed to offer consistent guidelines in an increasingly global market" [3].

Generally, section 512 of the Copyright Act (DMCA) laid down four specific "safe harbors" exempting qualifying service providers from copyright infringement liability for four specific activities (namely: mere conduit, caching, hosting and linking), subject to their compliance with (a) some general and (b) specific requirements[3].

However, according to online essay contributed by Stephen W. Workman for Internet Business Law Service, reported, “The E-Commerce Directive adopts the definition of Information Society Service of Article 1.2 of Directive 98/34/EC, and addresses the civil and criminal liabilities of ISPs acting as intermediaries. The Directive provides that ISPs will not be held liable under any field of law where an application of strict liability would impair the expansion of electronic commerce within the EU. This approach is termed "horizontal" because it addresses liability regardless of the grounds of claim by a rights holder or injured party. Accordingly, this Directive addresses not only copyright, but also liability under other areas of law such as defamation and obscenity. Under the E-Commerce Directive, an ISP is exempt from liability when it serves as a "mere conduit" or provides "temporary caching" for the sole purpose of making the transmission of content more efficient, is of a mere technical, automatic and passive nature, and where the ISP has neither knowledge nor control over the content being transmitted or stored” [10].

In view of the above stated laws, Hilary E Pearson has explained on how courts in these continents go about judging cases. She said, “Liability will depend upon how a court faced with a case of first impression analogizes a particular Internet service provider to more conventional categories of information providers. For example, should the service provider be viewed as the equivalent of the telephone company, purely a conduit for information? This might be the right analogy for the telecommunications link provider, but clearly does not fit the publisher. On the other hand, if the provider is viewed as analogous to a publisher of a printed publication, there is a much greater exposure to liability. The provider of a host computer for third party Web pages could be compared to a printer or perhaps a distributor of printed publications. It could also be argued that a Usenet group of bulletin board is analogous to a library, so that the provider should be treated as the librarian” [9]

It is essential to mention that an ISP may be held liable for spreading viruses. If an ISP knowingly allows or does not take reasonable steps to prevent the dissemination of a virus from their host computers under the U.S. Computer Fraud and Abuse Act of 1986 [7].

In conclusion, from all the literatures reviewed none of them explicitly said that ISPs are Liable for end users’ internet security. Although, some literatures are calling for lawmakers to bring ISPs to the chain of responsibility because they feel that ISPs are in suitable position to protect (police) the internet. Most famous among them was “*Holding Internet Service Providers Accountable”* by Lichtman and Posner in which they argue that ISPs should be called to the service of the law. They believe that Service providers control the gateway, as such ISPs to some extent should be held accountable when their subscribers instigate an awful behavior on the Internet. Moreover, they even compare vicarious liability that compels an employer to supervise and guide his/her employee and feel that ISPs should be held to the same tort law of liability [8].

Question 3: what are the recommended security considerations the ISPs should be responsible to provide?

ISPs have a vital role to play in providing secure network for themselves and their users. However, the security concern of the ISPs is very wide because the security measures they take might affect the network operations. For example, weak security implementation can result to the security threats or breaches that will disrupt the services of thousands of users. When this occurs, users may become upset and may change ISP. People believe that ISPs must provide the three basic Data security- Data Confidentiality, Data Integrity, and Data Availability. Therefore, ISPs need to defend against attacks and intrusion attempts to their networks by implementing secure network design in order to provide the security. Killalea reported, “The way an ISP manages their systems is crucial to the security and reliability of their network. A breach of their systems may minimally lead to degraded performance or functionality, but could lead to loss of data or the risk of traffic being eavesdropped (thus leading to 'man-in-the-middle' attacks)” [22].

Purcell explained the ISP Secure Network Design. This paper has summarized his explanation in the following points:

1. ISP should use different subnet in network access hardware from the main server(s). This will minimize the risk of intrusions, as the attacker must force to pass through switching and Intrusion Prevention system or Intrusion Detection system.

2. ISP should implement Access Control List (ACL). The ACL uses IP address and port number to deny access or allow access. Access control lists can serve as a first line of defense against port scans and other malicious activity that originates from the Internet or from home users.
3. They should Place a firewall between the ISPs servers, the Internet, and the ISPs users. A firewall creates another level of security that must be overcome before gaining access to the servers on the interior network.
4. ISPs should implement a strong password policy. All passwords should be at least six characters long, and contain alphas, numeric, and special characters.
5. ISPs should keep logs of information, such as which user was connected at what time, and from which IP address. Logs of information allow them to monitor the trends in the logs and help to protect them against Legal action.
6. ISPs should implement Secure Shell Layer (SSL) on mail and web servers, if they provide such services to their subscribers.
7. They should implement Network based Intrusion Detection System (NIDS). This security tool monitors network traffic and watch for packets that violate a specific set of rules. It then alerts the administrator and can proactively destroy any bad packets.

Therefore, he said that the measures listed are precautions that an ISP can take to ensure security of their network and servers. He believes that these can protect the ISP from compromise and from legal action, while helping to provide the user with a more secure environment. However, he lamented that the steps the ISPs take to secure their network effects the users, the most effective measures will take place at the home of the user. He mentioned, “When users contract for Internet service, the ISP should make their customers aware of the security risks that exist for them as Internet users. This could be in the form of a disclaimer or ISP policy statement. The disclaimer and policy is also important legally for the ISP. It serves as proof that the user was informed of the risk of Internet use, and that they accepted that risk. The customer should also be given printed literature that explains the security risks and what they can do to prevent them. In addition to printed material, an ISP can also offer this security information on their website, along with links to other security-oriented websites and software”. [23]

In another article Hathaway and Savage argued that, “ISPs must have a duty to avoid aiding and abetting criminal activity and must play an important role in addressing and deterring illegal activity, fraud, and misleading and unfair practices conducted over their networks and services” [15].

Furthermore, they believe that the internet is very important tool on its own and plays a vital role in supporting economic and social activity worldwide. Therefore, they said, “Precedents are emerging around the world for ISPs to shoulder more responsibility for the stewardship of the Internet”. Their article listed Eight (8) responsibilities of the ISPs that they called “*ISPs’ written responsibilities and the unwritten*” [15]. However, these duties or responsibilities are:

1) Duty to provide a reliable and accessible conduit for traffic and services
2) Duty to provide authentic and authoritative routing information
3) Duty to provide authentic and authoritative naming information
4) Duty to report anonymized statistics on security incidents to the public
5) Duty to educate customers about the threats
6) Duty to inform customers of apparent infections in their infrastructures
7) Duty to warn other ISPs of imminent danger and help in emergencies and
8) Duty to avoid aiding and abetting criminal activity

An essay titled “*Recommended Internet Service Provider Security Services and Procedures*” by Killalea, shows the expectation of ISPs with respect to security. The security is part of the Internet Engineering Task Force (IETF) recommendation to the ISPs. This paper has outlined the security requirements mentioned in the essay as:

a. ISPs have a duty to make sure that their contact information, in “Whois”, in routing registries (RFC1786) or in any other repository, is complete, accurate and reachable.
b. ISPs should have processes in place to deal with security incidents that traverse the boundaries between them and other ISPs.
c. ISPs SHOULD have clear policies and procedures on the sharing of information about a security incident with their customers, with other ISPs, with Incident

Response Teams, with law enforcement or with the press and public.

d. ISPs SHOULD be able to conduct such communication over a secure channel. Note, however, that in some jurisdictions secure channels might not be permitted.

e. ISPs SHOULD be proactive in notifying customers of security vulnerabilities in the services they provide. In addition, as new vulnerabilities in systems and software are discovered they should indicate whether their services are threatened by these risks.

f. Whether or not an ISP has a Computer Security Incident Response (CSIRT), they should have a well-advertised way to receive and handle reported incidents from their customers. In addition, they should clearly document their capability to respond to reported incidents, and should indicate if there is any CSIRT whose constituency would include the customer and to whom incidents could be reported.

g. Every ISP SHOULD have an Appropriate Use Policy (AUP). Whenever an ISP contracts with a customer to provide connectivity to the Internet that contract should be governed by an AUP. The AUP should be reviewed each time the contract is up for renewal, and in addition, the ISP should proactively notify customers as policies are updated.

h. In addition to communicating their AUP to their customers, ISPs should publish their policy in a public place such as their web site so that the community can be aware of what the ISP considers appropriate and can know what action to expect in the event of inappropriate behaviour.

i. Many jurisdictions have Data Protection Legislation. Where such legislation applies, ISPs should consider the personal data they hold and, if necessary, register themselves as Data Controllers and be prepared to use the data in accordance with the terms of the legislation.

j. ISPs are responsible for managing the network infrastructure of the Internet in such a way that it is reasonably resistant to known security vulnerabilities and not easily hijacked by attackers for use in subsequent attacks.

k. ISPs are commonly responsible for maintaining the data that is stored in global repositories such as the Internet Routing Registry (IRR) and the Asia Pacific Network Information Centre (APNIC), American Registry for Internet Numbers (ARIN) and Réseaux IP Européens (RIPE) databases. Updates to this data should only be possible using strong authentication.

l. They should ensure that the registry information that they maintain can only be updated using strong authentication, and that the authority to make updates is appropriately restricted.

m. ISPs should proactively filter all traffic coming from the customer that has a source address of something other than the addresses that have been assigned to that customer. This reduces the incidence of attacks that rely on forged source addresses.

n. They should proactively filter all traffic going to the customer that has a source address of any of the addresses that have been assigned to that customer. This reduces the exposure of their customers to attacks that rely on forged source addresses

o. Routers MUST NOT be configured to allow directed broadcasts onto a specific subnet [RFC2644].

p. ISPs should implement techniques that reduce the risk of putting excessive load on routing in other parts of the network. These include 'nailed up' routes, aggressive aggregation and route dampening, all of which lower the impact on others when your internal routing changes in a way that is not relevant to them.

q. ISPs should filter the routing announcements they hear, for example to ignore routes to addresses allocated for private Internets, to avoid bogus routes and to implement "BGP Route Flap Dampening" [RFC2439] and aggregation policy.

r. It is widely accepted that it is easier to build secure systems if different services (such as mail, news and web hosting) are kept on separate systems.

s. All systems that perform critical ISP functions such as mail, news, and web hosting should be restricted such that access to them is only available to the administrators of those services. That access should be granted only following strong authentication, and should take place over an encrypted link.

t. ISPs should take active steps to prevent their mail infrastructure from being used by 'spammers' to inject Unsolicited Bulk E-mail (UBE) while hiding the sender's identity [RFC2505].

u. ISPs should also strongly encourage their customers to take the necessary steps to prevent this activity on their own systems.

The essay said that the purpose is to express what the engineering community as represented by the IETF expects of Internet Service Providers (ISPs) with respect to security [22].

In summary, this paper found that there are recommended security considerations that the ISPs have some responsibilities to provide for themselves and their subscribers

4. CONCLUSION

The nature of the internet has made it in such a way that no single user's systems can be made adequately secure unless all the interconnected systems are made secure. With this regard, ISPs are in better position to provide security, as they are the central gateway to the Internet that interconnects these systems.

Furthermore, given the increasing incompetence of the subscribers to defend against attack, together with the emergence of the Internet Service provider as the significant gateway and custodians of the infrastructure, it is hypothesized that the most damaging attacks can be better mitigated with an Internet Service Provider's centric security approach to enhance the existing layered defense methodology [20].

Therefore, this paper has reviewed some literatures to examine the available security responsibilities of the ISPs, and found that though there are no legal bindings that put ISPs into responsibilities of internet security for their subscribers, however, there are handful researches from scholars calling for the Lawmakers to bring ISPs into the chain of responsibility.

As a result, this paper suggests that more research and policy work should be conducted to examine how ISPs could be called to the chain of security responsibilities of the internet. For example, if ISPs could provide adequate security for their networks, this can reduce the cyber attacks. Furthermore, ISPs are technically capable and more knowledgeable to provide internet security, as such making them responsible for the Internet security could be of benefit since they control the gateway.

REFERENCES:

[1] A. C. Laura, “Cyberspace & Internet Law”, This Week (Week 8): *Copyright Liability for Intermediaries*, October 12, 2007. Available at www.cheesman**law**.com/Docs/Paper4.doc

[2] AIs, “Examples of common types of online attacks and possible preventive and detective measures”. Accessed 22nd October, 2012 from www.hkma.gov.hk/200007061a2.doc

[3] B. M. Farano, “Internet Intermediaries' Liability for Copyright and Trademark Infringement” *Reconciling the EU and U.S. Approaches*, 2012, TTLF Working Paper No.14, http://www.law.stanford.edu/organizations/programs-and-centers/transatlantic-technology-law-forum/ttlfs-working-paper-series

[4] B. Rowe, D. Wood, D. Reeves, and F. Braun, “The Role of Internet Service Providers in Cyber Security”, *Institute for Homeland Security Solutions*, *Applied research* Focus result*, 2011. Available at http://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf

[5] Britannica online encyclopedia, 2012. Available at http://www.britannica.com/EBchecked/topic/746032/Internet-service-provider-ISP

[6] Cisco Certified Network Associate (CCNA Discovery), “Networking for home and small business” *Cisco Networking Academy*, 2007, chapter 8.

[7] D. A. Craine, “Internet Law”, *Attorney at Law*, 400-112th Ave NE Suite 140 Bellevue, Washington 98004. Accessed from www.NWPatents.com/internetLaw.html

[8] D. Lichtman, and E. Posner, “Holding Internet Service Providers Accountable”, *Chicago John m. Olin law & economics working paper (2D Series), 2004, NO. 217. Available at http://www.law.uchicago.edu/Lawecon/index.html*

[9] H. E. Pearson, “Liability of Internet Service Providers”, 1996. Available at http://www.leginetcy.com/articles/Liability%20of%20Internet%20Service%20Providers.pdf (accessed 28th October, 2012)

[10] Internet Business Law Service, “INTERNET LAW - Developments in ISP Liability in Europe”, *IBLS E-Commerce University-Diploma Programs- Student Contributions:*

Stephen W. Workman, Esq. Accessed 28th October, 2012 from http://www.ibls.com/internet_law_news_portal_view.aspx?id=2126&s=latestnews

[11] ISPSAA, "Internet Service Provider Security & Accountability Act of 2004". Available at http://www.stanford.edu/class/msande91si/www-spr04/readings/analysis/ispsa.pdf (accessed 28th October, 2012)

[12] J. Fox, "Consumer Reports Putting Consumers Back in Control", 2007. Available online at www.ftc.gov/bcp/workshops/spamsummit/presentations/Consumers.pdf

[13] J. Ness "The Role of Internet Service Providers in Stopping Internet Copyright Infringement", *Regional IP Attaché at U.S. Commercial Service*. Available at http://www.aseansec.org/21391-3.pdf

[14]J. Orill, "Duties & Responsibilities of ISPs. Available at http://www.ehow.com/list_7760725_duties-responsibilities-isps.html (accessed 24th October, 2012)

[15] M. Hathaway, and J. E. Savage, "Stewardship of Cyberspace: Duties for Internet Service Providers" *Canada Centre for global security Studies, University of Toronto*, 2012. Available at http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_hathaway-savage.pdf

[16] M. Jakobsson, and R. Zulfikar, (), "Crimeware: Understanding New Attacks and Defenses", *Addison-Wesley Professional*, 2008. Available at http://ptgmedia.pearsoncmg.com/images/9780321501950/samplepages/0321501950_Sample.pdf

[17] M. Van Eeten, J, Bauer, H Asghari, S. Tabatabaie, and D. Rand, "The Role of Internet Service Providers in Botnet Mitigation" *An Empirical Analysis Based on Spam Data OECD Science, Technology and Industry Working Papers*, 2010/05, OECD Publishing, 2010. Available at http://weis2010.econinfosec.org/papers/session4/weis2010_vaneeten.pdf

[18] MAAWG, "Ipsos maawg security awareness, 2010. Available at http://www.maawg.org/sites/maawg/files/news/2010_MAAWG-Consumer_Survey.pdf

[19]Michigan Technological University, "Information Security Plan", *Approval by Information Security Board of Review Members*, Rev 3 – 10/13/2011. Available at http://www.security.mtu.edu/policies-procedures/ISP_Final.pdf

[20] P. D. Price, "Toward an Internet Service Provider (ISP) Centric Security Approach", *Thesis completed in cooperation with the Institute for Information Superiority and Innovation, Naval Postgraduate School Monterey, California, march* 2002. Available at www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA402645

[21] R. Allan and L. Jim, "Working at small-to-medium business or ISP: CCNA Discovery Learning Guide". Indiannapolic IN: Cisco Press, 29th April 2008.

[22] T. Killalea, "Recommended Internet Service Provider Security Services and Procedure", *Network Working Group, Request for Comments*, 2000: 3013 BCP: 46. Available at http://www.ietf.org/rfc/rfc3013.txt

[23] T. Purcell, "User Security and The Internet Service Provider", *SANS Institute 2000 – 2005, 14th May, 2002. Available at http://www.giac.org/paper/gsec/1950/user-security-internet-service-provider/103393*

[24] Y. Huang, G. Xianjun, and A. Whinston, "Defeating DDoS attacks by fixing the incentive chain" *ACM Transactions on Internet Technology*, 2007, 7(1), article 5, 1-5. Available at http://portal.acm.org/citation.cfm?doid=1189740.1189745