Cyber Perspectives: Internet Exploitation and Business Survivability

Daniel Udo-Akang, CGEIT, PhD
Northcentral University
Prescott Valley, AZ 86314, USA
&
Adjunct Faculty, American Military University
Charles Town, West Virginia

Abstract

The purpose of this article is to present an overview of the challenges of cyber threats and the survivability of businesses. The ubiquitous and uncontrollable nature of the internet has caused the cyberspace to become a battleground for hackers and cyber warriors who exploit assets of businesses and institutions. The very technologies that empowers businesses and institutions to create, innovate, and operate also empower those that disrupt, steal, and destroy. No organization, business, institution, or industry is immune to cyber exploitation due to the sophistication of attacks. Thus, this article examined the changing nature of cyber-attacks and techniques in the context of an online marketplace and provided a taxonomy of tools and best practices that could create awareness and enhance the survivability of businesses in a highly collaborative yet insecure environment.

Key Words: Cyber Attacks, Internet Exploitation, Business Survivability, Cyber Technologies, Cyber Security, Cyber Weapons, Cyber Criminals, Cyber Transactions

1.0 Introduction

Over the past two decades, the cyberspace has integrated business and people around the world more than ever before. However, the insecurity of the cyberspace is a major threat to the survival of organizations, businesses, critical infrastructures, and government institutions (Batra & Wibowo, 2010; Vasilogambros, 2013). According to the Department of Defense (2011), the security of the U.S. critical infrastructure, including banking and finance, energy, power, supply chain, transportation, communication, water, government services, and defense industry rely on cyberspace, distributed control systems, supervisory control systems, and information technology resources that may be vulnerable to exploitation or disruption. Unfortunately, the same digital infrastructure and systems that process a full range of applications pose serious security challenges to the government and business organizations (Clapper, 2011). The U.S. national security strategy 2010 stated "the very technologies that empower us to lead and create also empower those who would disrupt and destroy" (p. 27).In the early 1990s, the Advanced Research Projects Agency (ARPA) sponsored the National Research Council (NRC) to study the security and trustworthiness of American computing and communications systems and the NRC report of 1991 noted "tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb"(NRC Report, 1991, p.7).

In a publication by Israel Homeland Security, Udo-Akang (2013) described cyber-attacks as a contemporary warfare that impact businesses, organizations, infrastructures, and assets of many nations. According to Udo-Akang (2013), the widespread automation of global financial transactions in an ever-increasing interdependence world has similarly witnessed a rise in various forms of information exploitation and compromise on the internet. In addition, the explosion in information sharing has exacerbated cyber espionage against government institutions and financial losses to many businesses (Udo-Akang, 2013). Although businesses around the world recorded an estimated $1 trillion revenue loss in 2009 due to cybercrimes (Mills, 2009), organizations all over the world continue to rely on the internet as the most productive medium to conduct business. According to Tucker (2008), the internet is still considered a strategic tool for electronic commerce, especially for product trading and purchases at competitive prices worldwide. Thus, Rotchanakitumnuai and Speece (2009) posited five positive determinants for the usefulness of the internet resources in the global marketplace: (a) the ease of use, (b) accessibility, (c) information quality, (d) trust in transactions, and (e) control in the trading processes.

However, the insecurity and untrustworthiness of the internet are major challenges to organizations (Jensen, 2010), especially organizations that are dependent on e-commerce, e-business, e-marketing, and e-finance (Bojnec & Ferto, 2010; Flavian, Gurrea, & Orus, 2009). The perspectives and insights in this paper are expected to create awareness for business stakeholders in the areas of cyber technologies, the capabilities of cyber exploitation, and the survival of businesses within the cyber environment. In addition, it will contribute new knowledge to the academic enterprise.

2.0 Literature Review

The purpose of this article is to examine the changing nature of the cyberspace, cyber-attacks, and techniques in the context of online marketplace. It is designed to provide a thoughtful discussion on the challenges of cyber threats and the survivability of businesses. The literature review is structured using three major constructs: (a) Cyber technologies, (b) cyber security, and (c) critical infrastructure in relation to business perspectives. This literature review is designed to provide a generic knowledge of cyber perspectives for a better understanding of (a) cyber-attacks, techniques, and sophistication; (b) the challenges of cyber weapons in the marketplace; (c) cyber criminals and online marketplace; and (d) cyber transactions and business survivability that are discussed in subsequent sections of this article.

2.1Cyber Technologies and Business Perspectives

The advancement of information technology and the rapid interconnectedness of businesses through the World Wide Web have mitigated distances between origin of goods and services and their demands at different places around the world (Anderson & Vincoop, 2004; Hill, 2009). Apart from information, money, goods, and services that flow more quickly, the capabilities of the internet are generating opportunities that inspire strategic long-term alliances and enhance a collaborative business-to-business (B2B) environment (French, Hollenbeck, Song, & Zinkhan, 2009). According to Digital Marketing Analysis by Camelia, Cristian, and Elena (2008), "digital marketing promotes products and services using digital distribution channels to reach consumers in a manner relevant, personal, and cost effective" (p. 982). Similarly, the internet as an innovative business tool promotes interactivity and has the potential to reduce trade costs, simulate manufacturing trade, creates addiction, enhances the growth of market places and provides easy tools for Web users (Head & Wang, 2007). Head et al. (2007) stated that the internet provides ready "access and availability of information about new markets for sellers and about goods for buyers everywhere around the world, facilitates logistics and serves as an advertising and marketing channel, which reduces market-specific fixed entry costs" (p. 130).

Many companies, such as American Online (AOL), Apple, Google, Microsoft, and Yahoo have improved technology resources to further enhance and improve the marketability of goods and services on the internet (Camelia et al. 2009). To enhance internet marketing through cooperative and collaborative relationship, Google, AOL, Apple, and Yahoo have developed the technology to advance mobile marketing using short message service (SMS) and multimedia messaging service (MMS), including Skype that allows users vocal and video calls on the Web for prices far lower than traditional telephone services (Camelia et al. 2009). Apart from the pay-per-click (PPC) internet marketing system developed by internet organizations such as Google, blogging has become a major audience attraction on the internet (Camelia et al. 2009). Business blogging as a major business tool has witnessed a revolutionary increase from 8 million blogs in 2005 to about 72 million blogs in 2007 and these days, about 120,000 blogs are published daily (Camelia et al. 2009). Blogging has become more popular, more embedded, and a mandatory addition to business and marketing repertoire (Dawson & Dawson, 2007). Dawson's (2007) study stated "the power of blogs is in their connection, either business-to-business (B2B) or Business-to-consumer (B2C)" (p. 22). Microsoft Bill Gates discussed the mammoth increase in business blogging as a fantastic thing in the business world (Wyld, 2008). Business web blogging is getting a lot more attention with its unique characteristics, such as content-specific, keyword-rich, accessibility, interactivity, personable, public consciousness, and high ranking in search engines (Dawson et al., 2007). According to Economist Intelligence Unit(2007), business winners and losers will be determined by "who figures out how to use the network" (p. 10).

Apart from the use of blogging, businesses are taking advantage of collaboration, sharing, and participatory platforms associated with other Web 2.0 technologies to create business value and boost their growth and profitability through customer acquisition(Economist Intelligence Unit, 2007).Web 2.0 is considered a leading edge that has exploited social networking, community of dialogue, user generated content, and other internetworking effects to (a) harness business intelligence, (b) facilitate business viability, and (c) drive significant competitive business advantage (Chen, 2009).

Although security is a major concern in the use of Web 2.0 technologies, such as wikis, blogs, podcasts, folksononmies, mashups, and social networks, collaboration and communication serve real value (Androile, 2010), especially in the context of web businesses regarding four interrelated perspectives (a) service, (b) technology, (c) organization, and (d) finance (Chen, 2009). The power of Web 2.0 in online commerce continues to create business models, and fuel business opportunities to sustain, build, and generate revenue (Androile, 2010; Bell, 2010; Chen, 2009). Androile's (2010) study used six constructs (a) knowledge management, (b) rapid application development, (c) customer relationship, (d) collaboration and communication, (e) innovation, and (f) training to describe the advantages of Web 2.0 solutions as an innovation platform for business explosion.

Advances in web technologies have enabled organizations to adopt complex technologies to transact businesses with their customers, offer substantial information on commodity trend, offer opportunities for competitive prices, and understand consumer interactions and communities (Bell, 2010; Chau & Xu, 2012). According to Bell (2010), "Web 2.0 has brought about a paradigm shift; next generation computing is now in the age of open innovation, close collaboration, co-creation, networking, and creativity in the use of existing technologies to develop new offerings" (p. 215). Many researchers (Eckman, 2008; Musser, O'Reilly, & O'Reilly Radar Team, 2006) have described Web 2.0 technologies as a fundamental business change platform with transformative force that propels businesses in all industries towards a new business practice with substantial user participation, collaboration, openness, and network effects. The explosion in consumer-generated content due to business growth and broad application of Web 2.0 (Bell, 2010; Chau & Xu, 2012; Eckman, 2008), has presented an environment that is becoming increasingly collaborative yet insecure (Androile, 2010). Although collaboration and communication have significantly leveraged the web-business landscape (Bell, 2010), organizations are concerned about intellectual property issues regarding proprietary information, privacy, confidentiality, security, and information control (Androile, 2010). Yet, many businesses are anticipating third generation technologies even though Web 2.0 technologies have provided capabilities and opportunities for cyber warriors and disgruntled employees to exploit businesses and critical infrastructures (Androile, 2010).

2.2Cyber Security and Critical Infrastructures

The rapid transformation and growth of the internet over the past two decades, including the sophistication of embedded technologies have forced the concerns of cyber security to the forefront of nations' national security and economic challenges (Chertoff, 2010; Melnitzky, 2012; National security Strategy, 2010). In the United States, for example, the automation of all critical infrastructures, such as electrical grid, energy distribution, financial transactions, supply chain services, defense industry, nuclear plants, banking transactions, communication, fuel supply, switching offices, transportation, water supply, and government services presents opportunities for disruption and exploitation by cyber hackers (Andress & Winterfeld, 2011; DHS, 2003; DoD, 2011). Although the U.S. critical infrastructures are interconnected within the cyberspace, the internet channels associated with each of the critical infrastructures are not controlled by the government (Clarke & Knake, 2010).Yet, the "U.S. and international businesses trade goods and services in the cyberspace, moving assets across the globe in seconds" (DoD, 2011, p. 1). The cyberspace has become an entrepreneurial incubator that facilitates trade, drives the global economy, and provides effective operations of the U.S. critical infrastructure (DoD, 2011). While the use of industrial control systems, such as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Programmable Logic Controllers, Human Machine Interface (HMI), Remote Terminal Units (RTU), and Master Terminal Units for interconnectivity of critical infrastructures within the cyberspace has several advantages (Andress et al., 2011), the security of these systems is a challenging endeavor. Given the integrated nature of the cyberspace, internet crackers and foreign adversaries are increasingly exploiting vulnerabilities to launch sophisticated attacks on networks and systems that control critical infrastructures (Andress et al., 2011).

The ubiquitous and uncontrollable nature of the internet has caused the cyberspace to become a battleground for hackers, crackers, and cyber warriors of various nations with critical infrastructures as major targets (Andress et al., 2011; Clarke & Knake, 2010). No organization, institution, business, industry, or infrastructure is immune to cyber threats or cyber risk (Clarke et al, 2010; Lute, 2013). Many industries and businesses may have the confidence that their firewalls and other intrusion detection and prevention systems are sufficient to prevent unauthorized access to information but later discovered that an attack was launched and valuable information and trade secrets were compromised (Lute, 2013).

According to Lute (2013), "Cyberspace is woven into the fabric of our lives…this global network of networks encompasses more than two billion people with at least 12 billion computers and devices, including global positioning systems, mobile phones, satellites, data routers, ordinary desktop computers, and industrial control computers that run power plants, water systems, and more" (p. 2). Financial institutions also confront dangerous combinations of threats, such as denial of service, distributed denial of service, social engineering, and introduction of viruses, malware, spyware, and Trojans remote access capabilities (Andress et al., 2011; Lute, 2013). For example, in October 2012, a group called Izz ad-Din al-Qassam Cyber Warriors issued a warning that some U.S. banks, such as Bank of America, Citigroup, Wells Fargo, JPMorgan Chase, CapitalOne, Regional Financials, and Sun Trust Banks would be attacked (Armerding, 2013).Despite the advanced warning, including the message posted on *Pastebin*, the "hacktivists" successfully used sophisticated attack techniques to bypass all security measures of the financial institutions to conduct denial of service (Lemos, 2013).The denial of service attacks flooded and overwhelmed the banks' websites with illegitimate traffic that prevented legitimate customers or users from gaining access.

3.0 Cyber Attacks –Techniques and Sophistication

Businesses all over the world are facing increasingly accurate, challenging, and sophisticated attacks despite spending hundreds of millions of dollars on firewalls, anti-virus or anti-malware and data protection implementations (Bodhani, 2013). Similarly, many companies have employed highly skilled hackers to conduct vulnerability scans or penetration permissive tests (Bodhani, 2012). Yet, hackers still discover flaws in the security perimeters of several organizations' networks (Bodhani, 2012). As witnessed during the Izz ad-Din al-Qassam Cyber Fighters denial of service (DoS) attacks on the U.S. banks, the method was highly sophisticated because they bypassed all security measures and systems of the biggest banks (Lemos, 2012). It was reported that financial institutions, such as CapitalOne suffered outages and their sites were inaccessible for several hours (Lemos, 2012). Earlier in 2012, twitter, a social networking site was hacked by anonymous hackers with over 55,000 usernames and account passwords leaked (Bawaba, 2012).In recent times, cyber attackers have succeeded in using advanced evasion techniques (AETs) to circumvent standard DoS defenses (Lerner, 2012). According to Lemos (2012), hackers craft packets designed to evade IT/IS defenses of their target organizations, specifically by sending a massive influx of DoS traffic to bombard targeted sites with between 70-100Gigabytes/sec of peak requests. "By crafting the data to look like valid encrypted Web requests, the network packets are allowed to get through to the customers' own computers to decipher the information. Even if that system blocks the requests as invalid, the avalanche of data buries the computer, which can't keep up" (Lemos, 2012).

Lerner (2012), for example, examined advanced evasion techniques (AET) that allow network hackers to bypass security detection and logging of organizations. Lerner argued that AETs are dangerous to financial institutions and money service businesses because of the challenges of managing extremely sensitive information in relation to a highly regulated environment. The risk stake of AET requires (a) zero-day AET protection in all layers, (b) deep packets inspection across multiple network layers and communication protocols, (c) infrastructure patch capabilities, (d) high manageability, and (e) integration capabilities (Lerner, 2012). According to research conducted at Cloud Security Firm, Lemos (2012) reported that with a variety of hacking tricks, such as an addition of a single character, evasion techniques are capable of causing problems for Web Application Firewalls (WAFs). Thus, distributed denial of service (DDoS) mitigation may not be a cure-all unless businesses have enough protocol decoding capabilities, not just partial defenses (Lemos, 2012). As stated, the security landscape is changing and cyber threats have grown in scale and sophistication in recent times. Cyber attackers have invested more money and time in the design of more sophisticated evasion techniques to exploit unidentified *zero-day* vulnerabilities of organizations' cyber defenses (Juuso, Kittilä, &Takanen, 2013).

The sophistication of cyber-attacks is rapidly advancing and unique vulnerabilities associated with various networks have exacerbated the challenges of information security professionals (Anderson, 2012). The architecture of organizations' network security such as intrusion prevention systems (IPS), unified threat management (UTM) devices, network firewalling, evasion detection, and advanced suppression detection are more challenging to manage in the contemporary hostile internet environment. According to Ilkka Hiidenheimo, founder and CEO of Stonesoft, the majority of IPS, UTM, and next generation firewalls (NGFW) systems and devices have not proven capable to secure businesses and institutions against AETs (cited in Kivikoski, 2012). Hiidenheimo argued that security breaches occur because of incomplete combination of network firewalling, IPS, and NGFW devices against network exploitation or cyber rogues (Kivikoski, 2012).

As Blackhouse and Willison (2006) argued, opportunities for cyber rogues to exploit a network are created through deficient security. For example, hackers could launch DDoS attacks against vulnerable targets that configure consumer devices to accept domain name service (DNS) queries from unknown sources, otherwise called *open recursive or open resolver* (Mcmillan, 2009).According to Duane Wessels, the Measurement Factory President, some modems are configured to use some specialized DNS server software, such as Trick or Tread Daemon (TOTd) with open recursive configuration problem (cited in Mcmillan, 2009). However, modern evasion techniques, as Phil Lerner described is "a hallmark of data obfuscation, also known as hiding data" (cited in Ginovsky, 2012, p. 26). Lerner stated "Many AET attacks leave no trace to current management and monitoring systems, logs, or reporters – leaving the devices blind and creating an illusion of security" (p. 26).

Internet security is a problem to all users because (a) there is no central authority, (b) a network can be used by any application on the computer connected to it, (c) online rogues can easily overwhelm their targets or circumvent their infrastructures, and (d) transmitted information can be manipulated (Harrowell, 2006; Nachreiner, 2013; Savvas, 2007). Limiting access to a public network does not necessarily guarantee protection against threats originating from a private network (Harrowell, 2006). As known, millions of PCs can be exploited simultaneously, without manipulating the operating environment of each computer (Savvas, 2007). As revealed by surveys conducted by Infoblox and The Measurement Factory, because organizations rarely pay adequate attention to configurations and deployment, the DNS are still vulnerable to exploitation despite marked improvement in information security architecture (Savvas, 2007). DNS infrastructures are the most vulnerable to outages through DNS cache poisoning, malicious attack using recursive query, DNS spoofing, DNS amplification or DDoS server lock down (Nachreiner, 2013; Savvas, 2007).For example, an attack on the DNS system could send legitimate users to malicious websites where identity theft may be harvested or malware covertly installed on their computers (Nachreiner, 2013). Cyber attackers could create DNS amplification by generating huge amounts of malicious traffic than the organizations network infrastructure was designed to handle (Gilmer, 2013; Nachreiner, 2013). Because DNS uses a UDP connectionless communication protocol, source verification of the communication is not required before a computer accepts or responds to spoofed requests. According to Nachreiner (2013), attackers may leverage both a botnet and DNS amplification to implement a DDoS amplification attacks.

The spoofed DNS requests are magnified by various open DNS servers on the internet and when the final DNS amplification are combined, a huge volume of traffic is generated that slows down internet processing activities and eventually shutdown the service – denial of service occurs (Gilmer, 2013; Kim, 2013; Nachreiner, 2013). In recent years, DDoS or DoS attacks or amplification attacks occur frequently - a cache domain name server is used as a malicious tool to attack several hundreds of thousands of Zombie PCs to generate several tens of gigabytes per second traffic to disable an internet infrastructure of a targeted network (Kim, 2013). However, it takes more time to harvest enough zombie PCs to generate enough network traffic needed to implement a large-scale DDoS attacks using DNS amplification techniques (Kim, 2013; Nachreiner, 2013). Cyber space attacks never stay the same. Sophisticated cyber rogues employ increasingly powerful intrusion techniques to (a) disrupt businesses confidentiality, integrity, and availability (CIA) and (b) interrupt service, such as data in processing, data on transit, and data in storage (Ginovsky, 2012). Every activity in the cyberspace is visible and accessible. News headlines in recent months have revealed that cyber intruders are using several weapons to access internet activities, shutdown systems, destroy data, steal information, or deny service in businesses and organizations (Ginovsky, 2012).

3.1 Challenges of Cyber Weapons in the Online Marketplace

The success of modern businesses and commerce depends on free-flowing communication, shared resources, secure encryption, and networks free from rogues, hackers, and crackers (Gutmann, 2010). Unfortunately, cyber rogues are always sniffing the internet using techniques such as password cracking, phishing, backdoors, social engineering and other deception and intrusion techniques to (a) exploit existing vulnerabilities and (b) compromise the integrity, confidentiality, and availability of a network (Udo-Akang, 2012). Cyber hackers discover new vulnerabilities every day and there are several ways to exploit such vulnerabilities (Boyer, 2011). Immediately after Robert Tappan Morris of MIT launched what was considered the first Internet attack (Morris worm) in 1988, the cyber space began to witness attacks with disruptive and destructive capacities that threaten the global e-business environment (Marsan, 2008; Udo-Akang, 2012). Although the impact of the Morris worm was not fully acknowledged, it served as a wake-up call to the internet users regarding the risk of cyber bugs (Marsan, 2008).

However, the high profile worm with self-replicating and infectious capabilities exploited thousands of computers, disrupted internet connectivity, and caused some organizations including the U.S. Department of Defense to isolate their gateways (AP, 1990; Marsan, 2008; Udo-Akang, 2012).Marsan (2008) posited "the Morris worm foreshadowed how future denial-of-service attacks would be used to overload systems and knock them off the internet" (p. 1). Although the Morris worm occurred when the usage and capacity of the internet was very limited, it was considered a precursor to the emergence of high caliber worms such as Mellissa of 1999, ILOVE YOU of 2000, 2001's Code Red, SQL Slammer of 2003, Mydoom of 2004, 2004's Sasser, Leap-A of 2006, Conficker of 2008, Stuxnet of 2010, Duqu of 2011, and Flame of 2012 (Udo-Akang, 2012).Every virus, worm, or malware has its unique design attributes with a mix of sophistication, evasion capability, ability to establish new links, and trusted relationship to enhance replication (Orman, 2003). For example, the unique characteristic of Code Red worm was its resurrection capability, the ability to hide in Adobe Reader and Microsoft packages to infect systems, and the ability to leave a back door or Trojan horse so that it could be revived if the original version was deleted (GAO, 2001). The Mellissa worm, just like the ILOVE YOU, had the capability to replicate, create copies, and overload the internet to the extent that computer and software investors were worried about the proliferation of the destructive worm (Udo-Akang, 2012). Prior to the emergence of highly aggressive and sophisticated Flame and Stuxnet worms, Conficker emerged with the capability to disable anti-virus protection and block access to malware vendors (Heater, 2009). Conficker posed a significant threat to businesses, especially to the Microsoft marketplace to the extent that Microsoft offered a $250,000 reward to bring the code writer to justice (Heater, 2009).

Stuxnet was described by many analysts as "cyberwar-caliber malware" that was written and coded to invade industrial control systems (ICS), such as the supervisory control and data acquisition (SCADA) network, distributed control systems (DCS), and programmable logic controllers (Andress et al., 2011; Udo-Akang, 2012). The 2011's Duqu virus was considered a successor to the Stuxnet with similar capabilities (Arnold, 2011). The Duqu virus was designed for high-level espionage capable of stealing data from critical infrastructures such as power plants, energy installations, water facilities, and chemical plants (Arnold, 2011; Lappin, 2011). Apart from paving the way for another sophisticated and high caliber weapon – the Flame, Duqucreated .DQ file extensions and infected over 30,000 business and personal computers in Iran (Arnold, 2011). In addition to other unique features, the Duqu virus was capable of penetrating Microsoft and custom-made operating systems to gather information that hackers could use to prepare for future attacks (Dhabi, 2011; Lappin, 2011).

Further, the ability of a virus to gather information was coded and enhanced in the Flame virus which was labeled a *sister-virus* to Duqu and Stuxnet (Arnold, 2011; Lappin, 2011). The Flame virus, the most active and sophisticated virus, was designed with unique abilities to (a) turn on internal computer microphones, (b) record activities, (c) activate cameras, (d) capture screen images, (e) encrypt and transfer those images undetected and (f) silence infection detected alarms. Despite these unique abilities associated with the Flame virus, Stuxnet and Duqu worms were considered most dangerous with high cybernetic abilities. For example, they could alter the settings of instrumentations used in a chemical plant or refinery - change the settings of pressure or flow controllers and cause a chemical storage tank to build up pressure and explode (Lappin, 2011). Cyber-attacks are diverse and multifaceted across industries and have been much in the news lately, conducted either by cyber criminals for financial gain or hacktivists motivated by sociopolitical ideologies.

3.2 Cyber Criminals and the Online Marketplace

Cyber criminals are increasingly sophisticated, making cybercrime a growing global concern, especially to (a)law enforcement stakeholders, (b) business communities, and (c) financial institutions (Ginovsky, 2012; Mclaughlin, 2011). According to Mclaughlin (2011), "Organizations are constantly under attack, and while their automated systems such as firewalls, intrusion detection systems (IDSs), and antivirus software repel the majority of attacks, they do not prevent or deter all attacks" (p. 58). As early researchers (LaPlante, 1987; Nance & Straub, 1990) revealed, 50-90 percent of businesses located in the U.S. suffer financial losses annually due to network abuse. Such abuse, according to Nance and Straub (1990) "is likely to continue in the future" (p. 45).In their paper, Austin and Darby (2003) posited that 90% of all businesses have been attacked by cyber criminals with an annual cost of $17 billion. Electronic commerce and e-service have battled public fears about online consumer risk associated with phishing and rampant social engineering within the cyberspace (Baker, Baker, & Tedesco, 2007; Boss, Chen, Guo, & Leung, 2009; Boulton & Knapp, 2006).

Phishing is a method used by cyber criminals to acquire personal identifiable information, such as username, passcode, social security numbers, credit card details, and date of birth from unsuspecting internet users by using fraudulent social engineering acts (Almahroos, 2008). Cyber phishing technique involves four phases: (a) phishers create fraudulent websites of target businesses, (b) phishing is initiated by sending out numerous emails to vulnerable users, (c) phish is successful when users release their confidential information on the phishers' website, and (d) the phisher exploits the user's confidential data (Almahroos, 2008; Baker et al., 2007).However, the sophistication of internet fraud is manifested in two forms of phishing. First, spear phishing targets a specific group of internet users, such as (a) users of a particular product line, and (b) a group of online bankers, and employees of a targeted company or government institution. Spear phishers send emails that appear plausible and legitimate to members of these groups to request information (Almahroos, 2008; Andress et al., 2011). Second, pharming is a method in which the phisher spoofs the domain of the internet user using a Trojan program to compromise the domain name system (DNS) of a user by rerouting the user's request to an illegitimate site to exploit their personal and confidential information (Almahroos, 2008; Andress et al., 2011).Prior to using these methods, phishers use social engineering techniques to acquire information about users to ensure effective and successful phishing (Jansson & Solms, 2011).

According to Baker et al. (2007), "Phishing is particularly damaging because it involves two victims: the consumer whose information is swindled and the legitimate organization whose brand is stolen for malevolent purposes" (p. 328). In his research, DeMarrais (2003) reported that falsified accounts involving cyber thieves have cost businesses $32.9 billion and consumers $3.8 billion. Internet-based financial fraud involving phishing produces three major adverse effects. First, the financial institution is forced by the Federal Deposit Insurance Corporation (FDIC) to absorb a major part of the financial loss (Almahroos, 2008). Second, the FDIC regulations "limit consumer liability for unauthorized transactions in their bank or credit card accounts to fifty dollars" (Almahroos, 2008, p. 600).Third, the reputation and goodwill of affected financial institution could be jeopardized (Almahroos, 2008). As a result of these negative consequences, Singh (2007) reported that companies are reluctant to disclose information related to financial loss caused by internet phishers and social engineers for fear of negative reaction from customers and investors. Thus, there are discrepancies in research reporting regarding financial loss due to cybercrimes. For example, Singh's (2007) study on international phishing found that financial loss ranging from US $900 to $6.5 million are imparted to businesses and their customers per phishing incident. Similarly, Bose et al. (2009) investigated phishing alerts on a public database and found that about 3.6 million people were phished between September 2006 and August 2007 with an estimated financial loss of $3.2 billion. Phishing and other crime wares within the online marketplace are unanticipated by cyber victims but designed uniquely to yield financial benefits to the attackers (Emigh, 2006). Thus, the attacker benefits in many ways: (a) theft of store confidential data, (b) extortion using DOS or DDOS, (c) spamming, and (d) compromised information for further criminal activities (Emigh, 2006).

Van Der Molen's (2013) study posited that the exploitation of targets by cyber criminals represents money when proven successful and the more attractive an exploit on certain vulnerabilities, the more such exploits are revised for further attacks (Van Der Molen, 2013). In 2011, Symantec Corporation revealed a Norton study report of $114 billion global annual loss from cyber crime and an additional $274 billion in business downtime. According to Symantec (2011), "With 431 million adult victims globally in the past year and at an annual price of $388 billion globally based on financial losses and time lost, cybercrime costs the world significantly more than the global black market in Marijuana, Cocaine, and heroine combined ($288 billion)" (p. 1).

According to Norton cybercrime report 2012, the global price tag of consumer cybercrime was $110 billion - China $46bn, USA $21bn, Europe $16bn, Brazil $8bn, India $8bn, Australia $2bn, Mexico $2bn, Russia $2bn, and Japan $0.5bn (Symantec, 2012). Despite the escalation of cybercrime cost, the risky behavior of cyber consumers continues to grow with indiscriminate use of mobile devices and resources. For example, the use of free unsecure WI-FI infrastructure to access personal e-mails, access social network accounts, shop online, and access their bank accounts has exposed consumers to high risks (Symantec, 2012). Although the power of the cyberspace has increased the speed, reach, and interactivity of businesses in the marketplace, the ability to build strong defenses to secure networks of assets posed serious challenges to business stakeholders and a community of consumers.

4.0 Cyber Transactions and Business Survivability

The advancement of cyber-attacks and the emergence of highly sophisticated cyber criminals have caught businesses and organizations around the world off guard. The survival of businesses and institutions in a cyber-exploited environment could be ranked first among security priorities in the twenty-first century. The security of data in storage or on transition from unauthorized access is a critical function of information assurance and technology (Kapoor, Pandya, & Sherif, 2011). The survivability of cyber transactions and electronic commerce is based on the seven pillars of security (a) authentication, (b) authorization, (c) privacy, (d) integrity, (e) non-repudiation, (f) availability, and (g) audit (Kapoor et al., 2011). Although consumers expect reasonable online security in a complex, interconnected marketplace, all forms of online activities such as credit card processing, bank transactions, product purchases, and all forms of government sales and e-commerce are continuously compromised by hackers because of weak data encryption that does not provide for end-to-end and unbreakable communication across wired and wireless networks.

The horrible mindset of businesses, according to Cronkrite, Park, and Szydlik (2011) is that "when electronically stored customer credit card information is stolen from a store the financial institutions are often responsible for the loss not the store that had badly configured security" (p. 72). Although cryptography is not the only security technology essential for protecting electronic or online transactions, it is a significant tool for information safeguard. Digital signature technology, certificates authority, public key infrastructures (PKI), and key escrowing technology are areas that require the development of standards based on governments' interoperability to protect consumers and safeguard online transactions against potential cyber criminals(Blain, 2000). The robustness and quality of online services is dependent on the underlying cryptographic construction and implementation (Dzemydiene, Jasiunas, Kalinauskas, & Naujikiene, 2010; Kim, 2010).

In his study, *Cryptography and Electronic Commerce*, Blain (2000) suggested that "international organizations and national governments prescribe minimum standards for the use of cryptography in order for electronic commerce transactions to reasonably engender certainty and general consumer protection" (p. 4). Such capabilities as (a) real-time communication, (b) electronic financial transactions, (c) data transfers, and (d) access to government services made possible by the internet emphasize the need for mandated certification authority (CA) and the importance of using strong encrypted instruments for cyber transactions. The increasing number of online fraud has exposed many businesses to several security solutions and protocols such as Secure Socket Layer (SSL), Kerberos framework, and Secure Hypertext Transfer Protocol (HTTPS) used for transferring encrypted data through the internet based on the Secure Sockets Layer (SSL) protocols (Dzemydiene et al., 2010; Kim, 2010). SSL protocol is used to prevent data eavesdropping during transmission process – employs asymmetric key encryption to enable the customer to authenticate the identity of the merchant using digital certificate (Kim, 2010).In many cases, however, credit card information are stored in the merchants' database, which provides an open opportunity for hackers to crack and steal those information or the insiders within the marketplace could illegally take advantage of the customers' information (Kim, 2010).

As Kevin Mitnick noted in book, *the Art of Deception*, all the firewalls and encryption in the world will never stop a gifted social engineer or a savvy *skiddie* from rifling a corporate database or an irate employee determined to crash a system (cited in Mitnick & Simon, 2011). For example, cyber rogues could use instruments such as SSLstrip based on secure hypertext transfer protocol (HTTPS) to trick victims into insecure web browser or HTTP connections instead of HTTPS with secure socket layer - Man-in-the-middle attack against SSL (Adeloye, 2013; Seifried, 2010). Due to this kind of vulnerability, Secure Electronic Transactions (SET) protocol was developed to secure financial card transaction on the internet – it prevents illegal re-use of customers' credit or debit card information by the business owners (Kim, 2010). However, the implementation of SET suffered acceptance despite dual signature assurances in which cardholders share order information with business owners and share payment information with the bank (Kim, 2010; Shamir, 2002).SET secure transaction was proposed by Visa, Mastercard, and Discover with the concept of single-swapped, single-use, and disposable number to remove the burden of fear from the customers (Shamir, 2002). Although the concept of single-use credit card suffered general acceptance, it is currently in use in the marketplace such as Discover, American Express, Visa Gift Cards, and MBNA (Kim, 2010). The growth of advanced persistent threats (APTs) from cyber criminals and warriors, the evolution of smartphones, tablets, and many mobile internet devices, and the phenomenal growth in information digitization present the need for secure communications and data. Thus, research continues to grow in an effort to identify the best information security techniques for online marketplaces.

4.1 Taxonomy of Cyber Tools and Best Practices

Although there are lots of secured cryptographic algorithms offered by some programming libraries, such as Mcrypt, symmetric key, public key algorithms, SHA1, SHA-256, and MD5hash functions to ensure data integrity in the marketplace (Smith, 2009; Kim, 2010), "attacks always get better, they never get worse" (Schneier, 2005, p. 7). For example, the improvement in SSL stripping capability could allow cyber crackers to inject destructive code into careless downloads from internet sites that do not either use HTTPS or use HTTPS without strict transport security (HSTS) policy (Adeloye, 2013). In the generic context, the connection between business customers and the Merchants is based on Secure Hypertext Transfer Protocol (HTTPS) or Insecure Hypertext Transfer Protocol (HTTP). Despite that HTTPS has been used to ensure end-to-end data integrity and confidentiality, some exploitation tools, such as Firesheep have been devised for use as a man-in-the-middle (MITM) tool to hijack web sessions and applications that process username and login identifications through HTTPS, including payment or session tokens (Adeloye, 2013; OTA, 2012). However, recent studies have shown a new secure card system called a *No Number Credit Card* (NNCC) based on Kerberos cryptographic framework was introduced with the capability of generating and exchanging payment tokens between online buyers and sellers without credit or debit card numbers (Kim, 2010). According to Kim (2010), "A token is cryptographically secure and valid only for a designated merchant, so it is robust against eavesdropping" (p. 2) and the security of customers' card information from disgruntled employees is guaranteed. Thomas (2008) discussed Mitnick's human vulnerabilities, "If an attacker wants to break into a system, the most effective approach is to try to exploit the weakest link – not operating systems, firewalls or encryption algorithms – but people" (p. 4).

This concept is based on the argument that the relatedness and connectedness between real issues and digital issues tends to easily entice people into believing that what is false is real, and vice versa (Thomas, 2008). For that reason, Kevin (2012) proposed several recommendations based on the U.S. Federal Financial Institutions Examination Council (FFIEC) Supplemental Guidance on Internet Banking Authentication: (a) dual authentication of customers, (c) layered security programs, (c) control over administrative functions, (d) device identification, and (e) customer awareness and education. Similarly, the Financial Services Information Sharing and Analysis Center (FSISAC), Automated Clearing House, and the Federal Trade Commission released 24 recommendations in 2009 to include financial safeguards for business and corporate customers (Kevin, 2012). Some of the recommendations were: (a) dedicated and hardened PCs for all online banking, (b) avoid email and general internet browsing on the dedicated PC, (c) daily reconciliation of all banking and financial transactions, (d) dual control process for all transactions, and (e) employee-to-employee transaction certifications among others (Kevin, 2012).

In the global business environment, there are compliance standards regarding Payment Card Industry Data Security Standards (PCI DSS) associated with user account management, encryption, and safe exchange and sharing of information (Anonymous, 2010; Ernie, 2011). The PCI DSS was revised to version 2.0 in 2010 to include Payment Application Data Security Standard (PA-DSS) for flexibility improvement in organizations regarding (a) implementation of controls, (b) threats management, and (c) reporting capabilities (Anonymous, 2010; Ernie, 2011). Primarily, this global Data Security Standard applies to all businesses that accept credit card payments and handle, store or transmit cardholder information (Ernie, 2011). In general, many intrusion detection systems (IDS) and evasion prevention systems (EPS) have been developed to manage risks associated with advanced evasion techniques (AETs), Zero-day exploitation and other advanced persistent threats (APTs) (Codenomicon, 2010; NewsRx, 2012). Such tools include (a) Evader 2.01 advanced evasion testing tools, (b) Fuzzers that identify zero-day vulnerabilities, (c) patch updates, (d) anti-virus applications, and (d) advanced firewall manager (AFM) for network security against incoming threats from widely deployed protocols (HTTP/S, SMTP, DNS, FTP). Even though these tools, standards, measures, recommendations, and practices are implemented to enhance the security of businesses and customers from cyber warriors, the survivability of businesses is constantly threatened.

5.0 Summary

The internet is an integral part of human livelihood that has ushered in a new era of prosperity dependent on e-business, e-marketing, e-finance and e-commerce (Rotchanakitumnuai et al., 2009). The convenience associated with accessibility, the ease of use, information quality, and control presents the internet as a strategic tool and the most productive medium to conduct business (Mills, 2009; Tucker, 2008). However, the insecurity and untrustworthiness of the medium are major challenges to the global marketplace (Jensen, 2010).

Cyberwar and cybercrime have become increasingly common with sophistication in the capabilities of cybercriminals and cyber warriors. The method and techniques employed by attackers are sophisticated and challenging. Although secured cryptographic algorithms and technologies have been offered, including standards, controls, and measures to safeguard data and information in businesses and organizations, cyber criminals have also designed tools and deceptive techniques to evade established barriers (Ginovsky, 2012).There is no organization or business that is completely immune to cyber threats and attacks (Clarke, 2010; Lute, 2013). Despite that businesses confront these threats on a daily basis, organizations all over the world continue to rely on the internet even though their firewalls and other intrusion detection and prevention systems are insufficient to prevent unauthorized access to their valuable information and business trade secrets (Lute, 2013). According to Dzemydiene et al (2010), the exponential growth of the internet triggered enhanced efficiency and capabilities of organizations and government even though the convenience has come with a price. Thus, businesses continue to lose billions of dollars yearly in a globally interconnected network with (a) unrestricted chains of criminals (Lute, 2013) and (b) sophisticated cyber weapons with DDOS capabilities.

However, advances in web technologies have enabled many companies such as American Express, Discover Financial Services, JCB International, Mastercard Worldwide, and Visa to develop PCI DSS standards to guarantee online business transactions between consumers and traders (Ernie, 2011). In addition, the development of technology resources by many companies, such as American Online, Apple, Google, Microsoft, and Yahoo to enhance the marketability of goods and services on the internet has triggered the design and development of cryptographic tools and several security solutions and protocols to safeguard data transaction from cyber weapons, phishers, and social engineers (Adeloye, 201; Kim, 2010).Yet, cyber criminals continue to devise unique methods and techniques to circumvent organizations' networks and exploit their resources. As noted by Kevin Mitnick, all the firewalls and encryption in the world will never stop a gifted social engineer from rifling a corporate database or a determined irate employee from crashing an organization's system network (Mitnick & Simon, 2011). "If an attacker wants to break into a system, the most effective approach is to try to exploit the weakest link – not operating systems, firewalls or encryption algorithms – but people" (Thomas, 2008, p. 4).Unfortunately, cyber rogues continue to sniff the internet using techniques such as password cracking, phishing, backdoors, social engineering, and other deception and intrusion techniques to exploit vulnerabilities and compromise the integrity, confidentiality, and availability of a network (Udo-Akang, 2012).

Recently, cyber criminals have devised tools such as AET to bypass security detection (Lerner, 2012); Firesheep for use as MITM to hijack victims' login identifications (Adeloye, 2013; OTA, 2012);and SSL stripping to inject code into careless internet downloads from sites that do not use strict transport security on HTTP (Adeloye, 2013). But the integrity, reliability, survivability, and confidentiality of business data on the internet depend largely on human ethical practices. A cyber expert Mitnick, posited that the weakest link for cyber exploitation is not operating systems, firewall, or encryption algorithms but the users (Thomas, 2008). For that reason, the recommendations of the FFIEC, FSISAC, ACH, and FTC centered on (a) control over administrative functions of businesses, (b) dual control process for online financial transactions, and (c) dedicated and hardened PC for all online financial, confidential, and classified transactions (Kevin, 2012). Internet is an innovative business tool that promotes interoperability of businesses, opens business opportunities for new comers, and offers opportunities for participation, collaboration, and competition. Thus, the survivability of businesses in a highly collaborative yet insecure internet environment depends on: (a) implementation of standards, (b) adoption of reliable and applicable technology, (c) implementation of best practices, and (d) employment and training of skilled and ethical cyber professionals to manage infrastructures, assets, capabilities, and resources of organizations.

References

Adeloye, B. (2013).*HTTPMan-in-the-middle code execution*. Retrieved from https://ritdml.rit.edu/bitstream/handle/1850/16646/BAdeloyeThesis5-30-2013.pdf?sequence=1

Anderson, J. E., & van Vincoop, E. (2004). Trade costs. *Journal of Economic Literature, 42*, 691-751.

Andress, J., &Winterfeld, S. (2011). *Cyberwarfare: Techniques, tactics and tools for security practitioners*.Boston, MA: Syngress.

Androile, S. J. (2010). Business impact of Web 2.0 technologies.*Communications of the ACM, 53*, 67-79.doi: 10.1145/1859204.1859225

Anonymous.(2010). *Data encryption; cyber-ark recommends steps for achieving PCI version 2.0 compliance*.Computers, Networks & Communications, *2*, 347.Retrieved from ProQuest.(Publication No 762044532).

Almahroos, R. (2008). Phishing for the answer: Recent developments in combating phishing.*A Journal of Law and Policy for the Information Society, 3*, 595-621. Retrieved from http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Almahroos.pdf

Anderson, J. (2012). *Stonesoft demonstrates true threat of advanced evasion techniques at SC Congress.* Retrieved from http://www.businesswire.com/news/home/20121002005140/en/Stonesoft-Demonstrates-True-Threat-Advanced-Evasion-Techniques

Armerding, T. (2013).*Islamic hacktivists' bank attack claims gain credibility*.Retrieved from http://www.csoonline.com/article/717355/islamic-hacktivists-bank-attack-claims-gain-credibility

Arnold, T. (2011, October). Computer virus poses threat to key installations. The National.ProQuest Document No 899835659. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/899835659?accountid=28180

Austin, R. D., & Darby, C. A. R. (2003).The myth of secure computing.*Harvard Business Review, 81*, 120-126.

Baker, E. M., Baker, W. H., & Tedesco, J. C. (2007). Organizations respond to phishing: Exploring the public relations tackle box. *Communication Research Reports, 24*, 327-339. doi: 10.1080/08824090701624239.

Batra, M. M., & Wibowo, K. (2010).Information insecurity in the globalization era: threats, governance, and survivability.*Competition Forum, 8*, 111-120.

Bawaba, A. (2012). *Over 55000 twitters' usernames, passwords leaked by hackers*. Asian News International.ProQuest Document No 1012128318.Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/1012128318?accountid=28180

Bell, F. (2010).New-wave global firms: Web 2.0 and SME internationalization.*Journal of Marketing Management, 26*, 213-229.doi: 10.1080/02672571003594648

Blackhouse, J. &Willison, R. (2006).*Opportunities for computer crime: Considering systems risk from a criminological perspectives.* European Journal of Information Systems, 15, 403-414. doi: 10.1057/palgrave.ejis.3000592

Blain, C. M. (2000).*Cryptography and electronic commerce: The role of the Canadian government in facilitating a domestic and global electronic marketplace*.ProQuest, UMI Dissertations No MQ52340.

Bojnec, S., &Fertö, I. (2009).Impact of the internet on manufacturing trade.*The Journal of Computer Information Systems, 50*, 124-132.

Boss, I., Chen, X., Guo, C., & Leung, A. C. (2009, November).*Analyzing the risk and financial impact of phishing attacks using a knowledge based approach*. Paper presented at the 9th International on Electronic Business, Macau, Peoples Republic of China.

Boulton, W. R., & Knapp, K. J. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management, 23*, 76-87.

Boyer, B. R. (2011).*Identification and ranking of critical assets within an electrical grid under threat of cyber attack.* ProQuest Document No 1500336.

Camelia, V., Elena, E., & Cristian, M. (2008).Digital marketing – An opportunity for the modern business communication.*Annals of the University of Oradea, Economic Science Series, 17, 982.*

Chau, M., & Xu, J. (2012).Business intelligence in blogs: Understanding consumer interactions and communities.*MIS Quarterly, 36*, 1189-1216

Chen, T. F. (2009). Building a platform of business model 2.0 to creating real business value with 2.0 for web information services industry.*International Journal of Electronic Business Management, 7*, 168-180.

Chertoff, M. (2010).Cyber security symposium: National leadership, individual responsibility.*National Security, Leadership & Policy, 1*, 1.

Clarke, R. A., &Knake, R. K. (2010).*Cyberwar: The next threat to national security and what to do about it*. New York, NY: HarperCollins

Clapper, J. R. (2010).*U.S. Intelligence Community: Worldwide threat assessment*. Retrieved from http://www.iranwatch.org/sites/default/files/us-hpsci-clapper-preparedstatement-021011.pdf

Codenomicon (2010).*Fussing best practices: Combining generation and mutation-based fuzzing*. Retrieved from http://www.codenomicon.com/resources/whitepapers/codenomicon-wp-generation-and-mutation.pdf

Cronkrite, M;Park, J;&Szydlik, J. (2011, March). The strategies for critical cyber infrastructure (CCI) protection by enhancing software assurance.*International Conference on Information Warfare and Security*, 68. Retrieved from http://connection.ebscohost.com/c/articles/60146009/strategies-critical-cyber-infrastructure-cci-protection-by-enhancing-software-assurance

Dawson, R., & Dawson, T. (2007).Building your business with video blogging.*JournalEventDV, 20*, 22-27. Retrieved from *share.pdfonline.com/.../14_references.htm*

DeMarrais, K. (2003, September). Identity theft on the rise, FTC warns. *Knight Ridder Business News*, pp. 1-4.

DoD. (2011). Department of defense strategy for operating in cyberspace. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf

Dzemydiene, D; Jasiunas, E; Kalinauskas, M; &Naujikiene, R. (2010). Evaluation of security disturbance risks electronic financial payment systems. *Intellectual Economics, 2*, 21-29.

Eckman, J. (2008). *We've only just begun: Web 2.0 and its impact on the modern enterprise*. A Paper Presented at the Web 2.0 Kongress, Hamburg, Germany.

Economist Intelligence Unit. (2007). *Serious business: Web 2.0 goes corporate*. Retrieved from http://www.socialmediagroup.com/wp-content/uploads/2007/06/smg_eiu_web20.pdf

Emigh, A. (2006). The crimeware landscape: malware, phishing, identity theft and beyond.*Journal of Digital Forensic Practice, 1*, 245-260.doi: 10.1080/15567280601049985

Ernie, S. (2011). *Payment card industry standards: The rundown on 2.0*. Multichannel Merchant, 28.2.Retrieved from ProQuest.(Publication No 863370306).

Flavian, C., Gurrea, R., &Orus, C. (2009).A heuristic evaluation of websites design for achieving the web success.*International Journal of Services and Standards, 5*, 17-41.

French, W., Hollenbeck, C. R., Song, J. H., &Zinkhan, G. M. (2009). E- collaborative networks: A case on the new role of the sales force. *Journal of Personal Selling And Sales Management*, 29, 127-138

Gilmet, B. (2013). Cyber attack. *Broadcast Engineering, 55.5*, 16-19.

Ginovsky, J. (2012). Cyber threat.*American Bankers Association Journal, 104*, 24-28.

Gutman, E. (2010). Hacker nation: China's Cyber Assault.*World Affairs*.70-79.

Heater, B. (2009, March).*Conficker C computer virus-nasty worm*.St. Joseph News.ProQuest Document No 380183443.

Harrowell, A. (2006). IMS: Menace to security.*Mobile Communications International, 130*, 1.ProquestDocument No 221226210.

Jansson, K., &Solms, R. V. (2013).Phishing for phishing awareness.*Behavior & Information Technology, 32*, 584-593. doi: 10.1080/0144929X.2011.632650.

Juuso, A, Kittila, K, &Takanen, A. (2013).*Proactive cyber defense: Understanding and testing for advanced persistent threats (APTs)*.12th European Conference on Information Warfare and Security. Retrieved from http://academic-conferences.org/eciw/eciw2013/eciw13-proceedings.htm

Kapoor, B., Pandya, P., &Sherif, J. S. (2011).Cryptography: A pillar for privacy, integrity, and authenticity of data communication.*Kybernetes, 40*, 1422-1439.doi: 10.1108/03684921111169468

Kevin, H. (2012, September). *Guest opinion: Thwarting cyber attacks*. Credit Union Times.Retrieved from ProQuest(Publication No 1037579730).

Kim, B. K. (2013). Methods of detecting DNS flooding attack according to characteristics of type of attacks. *Electronics And Telecommunications Research Institute*. Publication No US20130031626 A1. Retrieved from http://www.google.com/patents/US20130031626

Kim, J. E. (2010). *A secure online credit card transaction method based on Kerberos authentication protocol*. ProQuest UMI 1479067.

Kivikoski, J. (2012). *Stonesoft introduces industry's first evasion prevention system (EPS) to mitigate the threatof advanced evasion techniques (AETs)*. Retrieved from http://www.stonesoft.com/en/company/press_and_media/releases/en/2012/24072012-2.html

Lappin, Y. (2011, October). New 'stuxnet-related' virus may be set for cyber-attack. Jerusalem Post.ProQuest Document No 900479984.http://search.proquest.com.proxy1.ncu.edu/docview/900479984?accountid=28180

LaPlante, A. (1987). Computer fraud threat increasing, study says. *Infoworld, 18*, 47.

Lemos, R. (2013). *More banks come under denial-of-attack*. Retrieved from http://www.eweek.com/security/more-banks-come-under-denial-of-service-attack/

Lute, J. H. (2013).DHS Cybersecurity: Roles and responsibilities to protect the nation's critical infrastructure.*Testimony Before the House Committee on Homeland security*. Retrieved from http://docs.house.gov/meetings/HM/HM00/20130313/100390/HHRG-113-HM00-Wstate-LuteJ-20130313.pdf

Marsan, C. D. (2008). Morris worm turns 20. *Network World, 25*, 10.

McLaughlin, K. L. (2011). Cyber attack!Is counter attack warranted? Information Security Journal: A Global Perspectives, 20, 58-64. doi: 10.1080/19393555.2010.544705

Mcmillan, R. (2009). *DNS problem linked to DDoS attacks gets worse: Consumer modems are blame for the rise in open recursive DNS servers*. Retrieved from http://www.techworld.com.au/article/326280/dns_problem_linked_ddos_attacks_gets_worse/

Mitnick, K. D., & Simon, W. L. (2011*).The Art of deception: controlling the human element osecurity*.Indianapolis, IN: John Wiley Publishing.

Musser, J., O'Reilly, T., O'Reilly Radar Team.(2006). *Web 2.0 principles and best practices*. Retrieve from http://oreilly.com/catalog/web2report/chapter/web20_report_excerpt.pdf

Nachreiner, C. (2013). Attack of the network traffic: Understanding and avoiding distributed denial of service (DDoS) attacks. *Security Technology Executive*.36-38.

National Research Council. (1991). *Computers at risk: Safe computing in the information age*Washington, DC: The National Academic Press.

OTA. (2012). Protecting your website with always on SSL. Retrieved fromhttp://otalliance.org/resources/AOSSL/OTA_Always-On-SSL-White-Paper.pdf

Rhodes, K. A. (2001). *Code Red, Code Red II, Sircam attacks, highlight need for proactivemeasures.*Government Accountability Office. Document No GAO-01-1073T. Retrieved from http://www.gao.gov/new.items/d011073t.pdf

Rotchanakitumnuai, S., &Speece, M. (2009).Modeling electronic service acceptance of an e-securitiestrading system.*Industrial Management & Data Systems, 109*, 1069-1084. doi10.1108/02635570010991300

NewsRx. (2012). Stonesoft introduces industry's first evasion prevention system EPS to mitigate the threat of advanced evasion techniques AETs. *Computer Weekly News, 3*, 316.

Savvas, A. (2007). Domain servers still a security risk.*ComputerWeekly, 27*, 16.

Schneier, B. (2005). Attacks on cryptographic hashes in internet protocols. Retrieved from http://tools.ietf.org/search/rfc4270

Seifried, K. (2010). Attacks against SSL.Retrievedfromwww.linuxpromagazine.com/content/download/.../060-061_kurt.pdf

Shamir, A. (2002). SecureClick: A web payment system with disposable credit card numbers.*Lecture Notes in Computer Science, 2339*, 232-242. Retrieved from http://link.springer.com/chapter/10.1007%2F3-540-46088-8_20?LI=true

Smith, J. (2009). Mcrypt. Retrieved from http://mcrypt.sourceforge.net

Singh, N. P. (2007). Online frauds in banks with phishing.*Journal of Internet Banking and Commerce, 2*,1-27.

Symantec. (2011). Norton study calculates cost of global cybercrime: $114 Billion Annually.

Retrieved from http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

Symantec.(2012). 2012 Norton cybercrime report. Retrieved from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Thomas, T. L. (2008). Cyberskepticism: The minds firewall. *I-Sphere*. 4-8. Retrieved fromhttp://fmso.leavenworth.army.mil/documents/cyberskepticism.pdf

Tucker, S. (2008). E-commerce standard user interface: An E-menu system.*Industrial Management & Data Systems, 108*, 1009-1028.

Udo-Akang, D. (2012).*Cyber attacks: Contemporary warfare*. Israel Homeland Security.Retrieved from http://i-hls.com/2013/02/cyber-attacks-contemporary-warfare/

Van Der Molen, H. (2013). Forecasting malware conditions: Worsening conditions, some bright spots.*Information Security Journal: A Global Perspectives, 21,* 269-279. doi: 10.1080/19393555.2012.694980

Vasilogambros, M. (2013).*America's 3 biggest cyber security vulnerabilities*.National Journal. Retrieved from http://www.nationaljournal.com/whitehouse/america-s-3-biggest-cybersecurity-vunerabilities20130313

Wang, F., & Head, M. (2007). How can the web help build customer relationships? An empirical study on E-tailing.*Information& Management, 44*, 115-129.

Wyld, D. C. (2008).Management 2.0: A primer on blogging for executives. Management Research News,31, 448-483. doi 10.1108/01409170810876044