CORPORATE ROLE IN PROTECTING CONSUMERS FROM THE RISK OF IDENTITY THEFT

Omondi John Opala, PhD[1] and Syed (Shawon) M. Rahman, PhD[2, *]
[1]Advanced Services, Cisco Systems, Inc., RTP, USA
jopallah@cisco.com

[2]Associate Professor of Computer Science at the University of Hawaii-Hilo, Hawaii, USA and Part-time Faculty at Capella University, Minneapolis, USA
[*]SRahman@Hawaii.edu

ABSTRACT

The Internet has made it possible for users to be robbed of their reputation, money and credit worthiness by the click of a mouse. The impact of identity theft severely limits victims' ability to participate in commerce, education and normal societal functions. This paper evaluates resurgence in syndicated cyber attacks, which includes but not limited to identity theft, corporate espionage and cyber warfare taking advantage of the Internet as a medium of operations. The paper highlights the increase of cyber related attacks in the past ten years due to lack of transatlantic international corporation between participating countries, coherent information security policies, data aggregation and sound international laws to facilitate prosecution of perpetrators. The cyber space coupled with availability of free hacking tools has contributed to resurgence in syndicated identity theft, corporate espionage and identity theft by organized crime elements taking advantage of the Internet as a medium of operations. This paper presents conclusive solution that users, organizations and consumers can enact to protect themselves from the threat of cyber attacks culminating into identity theft, financial loss or both.

KEYWORDS

Identity Theft, Cyber Attacks, Internet Vulnerabilities and Medical Identity Theft, Network Protocols, Wireless Network, Mobile Network, Virus, Worms &Trojon

1. INTRODUCTION

Information security attacks and vulnerabilities began in the 1980s with boot viruses transferred through infected floppy diskettes but with no service impact and prohibitive repair cost of today's network attacks [1]. Most of the attacks of the 1980s were just nuisances by computer technicians trying to show off their programming skills with no system interruption but the attacks have gradually evolved into criminal enterprises. The complexity and anonymity vulnerability exploitation poses the gravest risk to information technology (IT) infrastructure because they inflict maximum peril [2].

The explosive growth of the Internet has been greatly beneficial for society at large in terms of trade, commerce, social networking, online education and created new opportunities across the globe. The great success of the Internet and internetworking has also brought with it uncontrollable vulnerabilities in the cyber space giving rise to a new generation of criminals, identity thieves, cyber spies and warriors [3]. The cyber space is a domain with no boundaries ideal medium for organized clandestine operations and complicated to govern with existing national policies.

DOI : 10.5121/ijcnc.2013.5502

This paper however argues that the lawlessness of the cyber world is just but one of the many reasons of increase in cyber theft. The lack of Trans-Atlantic Legislative Corporation between participating countries, coherent information security policies, data aggregation and sound international laws to facilitate prosecution of perpetrators are the main reasons for the rise. This paper highlight the rising risk of cyber related attacks such as identity theft executed by acquisition of compromised personal data. The tools employed include dumpster diving, hacking, social engineering and spyware attacks by well organized crime organizations. The paper concludes by presenting different ways through which users, consumers and enterprise organizations can protect themselves from the threat of identity criminals. The following sections are organized as follows background of the study, identity theft, medical identity theft, cyber threat tools, data security tools, recommendations and conclusion.

2. BACKGROUND OF THE STUDY ON CYBER CRIMES AND IDENTITY THEFT

Identity theft, espionage and other related cyber crimes has been prevalent before the explosion of the Internet however the ease of access to free spyware tools for hacking, phishing, Trojan horses and data aggregation centers have made attacks un avoidable. The explosive growth of the Internet in the last 15 years has been greatly beneficial for society at large in terms of trade, commerce, social networking, online education and created new opportunities across the globe. However the great success of the Internet-working has also brought with it uncontrollable vulnerabilities in the cyber space giving rise to a new generation of criminals, identity thieves, cyber spies and warriors. The cyber space with all its glamour is a domain with no boundaries making it an ideal medium for organized clandestine operations, which were harder in the past to operate in conventional warfare method. General Wesley Clark is quoted as saying that, "*There is no form of military combat more irregular than an electronic attack: it is extremely cheap, is very fast, can be carried out anonymously, and can disrupt or deny critical services precisely at the moment of maximum peril*" [4].

According to Abdul, identity theft and identity fraud are terms used interchangeably to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain [5]. It is a felony crime to assume another person's identity to acquire credit cards, jobs or any other form of benefits derived from using that identity in the US. Ehud Tenenbaum of Israel who went with a nickname of "The Analyzer" was indicted for masterminding the largest bankcard and identity theft fraud in 2009 according to Horn [5]. He ran a sophisticated computer hacking scheme, which stole over $ 10 million from US banks in Texas. He used software vulnerability tools to compromise American banks and then orchestrated large bank transfers to multiple financial institutions. Most recently in the US, the Federal jury in Los Angeles convicted a person for orchestrating $ 7.7 M Medicare fraud scheme that included identity theft, forging unnecessary prescriptions and diagnostics tests under the supervision of a medical doctor as part of an elaborate electronic scam in 2010 [6].

2.1. Identity Theft

There is a reported rise in identity theft in the US and across the world but it estimated that every day one in four US citizens have their identity stolen [7]. Identity theft however is propagated by criminals who would want to use that information to open new bank accounts, credit cards, and purchase expensive articles online using the stolen information. Identity theft begins with access to personal data such as social security cards, driver's license, and credit card information is compromised. The thief then calls the creditors to change the address on those cards then they either increase the amount on the cards or apply for new cards altogether. In certain cases data is solicited or found through lost documentation, dumpster diving to find non shredded information such as bank records, pre-approved credit card offers which are considered a public domain when it leaves the curb of any street. The most persistent thieves use credit card swipes at businesses to gather information, other use Trojan horses masquerading as legitimate banks on emails sent to send to unsuspecting clients to change passwords but when they open the link it is sent to the thieves' server where he can capture all the information.

Medical information theft is not considered a criminal offense and as such there are no specific laws to prevent victims of such losses. However the vulnerability exists in system access, database and medical organization infrastructures. US Department of Health and Human Services (HHS) began developing a Nationwide Health Information Network to meet the mandate from President Bush to have all medical information online in 10 years. The availability medical information online creates a potential vulnerability for exploitation in the infrastructure. The exploitation of medical information could have grave consequences when accidental disclosure, corruption and loss of health information can cause bodily harm especially when doctors cannot have access during medical emergencies [8]. The organizations would suffer reputation loss, lack of revenue as a result of the breach as well as federal and state fines as provided the corresponding laws.

The individual cost of repairing a stolen identity has been estimated to range from $80 to $800 with over 175 hours of personal time invested in the repair process which makes it an absolute necessity to protect critical data from unwanted access [9]. To the victim there is no real difference because the end result is the same as in identity theft. Anyone who has his or her medical information stolen will suffer loss of services related to medical benefits which can range from being denied service if someone else has used all the benefits for that year, putting the victim in to higher medical risk of pre-existence so they are denied coverage, financial loss and even death especially when the victim cannot be treated in emergency. The perpetrators of the crimes are the same people seeking to use ones information for their own benefit or assuming someone else's information to achieve medical treatment as in the case of medical theft [10].
Those who have fallen victim to identity theft suffer a lot of losses ranging from lost money in bank accounts, huge amounts of credit card debts, loss of credit value, some are arrested especially if the thief used the identity to commit other crimes, evictions from property and the amount of time it takes to clear ones name which in itself is a monumental task [12].

Table 1. Data Breaches

2008 Data Breaches By Category of Source		
Category	**Incidents**	**Records Lost**
Financial Institution	78	18,731,947
Business	240	5,886,960
Education	131	806,142
Gov/Military	110	2,954,373
Medical/HealthCare	97	7,311,833
Total	656	35,961,255
Source: Identity Theft Resource Center		

3. SECURITY VULNERABILITIES

Existing literature suggests that security policy and compliance are necessary to limit what kind of personal identifying information (PII) can be collected and stored by data aggregating companies such as medical data hubs or financial data hubs [12]. In the US social security, credit cards and debit card numbers are considered PII should not be shared unnecessarily. It is estimated that about 32 % of identity theft cases are as a result of stolen social security cards. The failure to secure PII will has lead to an increase in identity theft related cases due in part to security vulnerability exploitations and lack of security awareness by consumers in in some cases. A consumer survey on security risks and vulnerabilities for online purchases showed that the lack of security awareness was among reasons for the rise in cyber based attacks as summarized in table below [13]. The table presents the respondents selection of their perceived security risks based on a scale of 1 – 10.

Table 2. Summary of security perceived risks on a scale of 1 – 10

Belief or Practice	Number
Security Technology	
Worms and viruses are the same	7
Worm is a more destructive type of virus	3
Not aware of having a virus scanner	3
Security Practices	
Keep passwords private/secure	6
Change passwords without prompting	2
Change passwords with prompting	3
Lock computer when away	6
Lock physical files when away	7
Would contact IT staff	4
Reuse passwords	2
Would phone to verify potential phishing	7
Conflate security and functionality	7
Sensitive Information Awareness	
Aware of sensitive information	10
Have access to SSN's	9
Aware of some form of social engineering	12
Received phishing email	10
Security Responsibility	
IT staff are responsible for security	7
Organization is responsible for security	3
Security is a shared responsibility	2
Views of IT Staff	
Trust IT staff technical abilities	9
Believe IT staff to be responsible	6

The rise of cyber warfare turning into cyber crime has made it possible to be robbed of reputation, monetary value, identity and ability to purchase anything in future simple by a click of a button. There are multiple ways that personal data can be compromised but the most commonly used are dumpster diving, social engineering, root kit, malware, botnets, Trojan horse just to mention a few such security vulnerabilities. The reason for the increase in identity fraud is as a result of availability of web tools for hacking and system of purchase of such documents on the Internet through a system referred to as “carding”, which refers to websites that allows for ease sale of personal identifying data (PII) data quickly on the Internet [14]. These Internet forums provide for online bazaars full of stolen personal data and financial information.

This research paper maintains that the availability of cheap software for breaking into networks readily available on the internet and the lack of uniform US policy and international law to prosecute against perpetrators of data theft culminating into identity theft is the reason for the surge in such criminal activities. Some of the most commonly used tools by criminals or hackers to compromise personal data, which culminates into identity theft, are: social engineering, rootkit, malware, botnets, viruses, Trojans and hacking.

3.1 Social Engineering

Social engineering is a form of deceit to access secure data by someone posing as network employee calling employees to let them know they should reset their password [15]. In many cases those practicing social engineering could also shadow someone and look over their shoulders to get the passwords. Information security awareness training to employees and customers concerning personal identifying data is the best antidote to social engineering form of attack.

3.2 Email Attack Tools

Email trapdoors are spam emails, which appear harmless advertising sales items, but the attachments have embedded logic bombs that execute upon clicking on the links. The attachment therefore gives the attacker remote access to the system if antivirus and antimalware are not up to date.

3.3 RootKit

The rook kit phenomenon in network infrastructure has had a lot of attention in the recent studies because of its service denial impacts and potential for denial of service attacks. A root kit is a combination software attack tools rolled into one, they include viruses, malware, and spyware and tear drops. Rootkits are groups of malicious codes accessible on the Internet that can seamlessly operates on an infected systems process without showing signs of infestation to the computer user and the operating system [16]. The impact of rootkit is that they violate access restrictions and execute at operating system level to collect personal data and can be used to foster denial of service attacks. The most recognized reported mass scale of rootkit impacted millions of Sony users through legitimate music disks sold to customers.

3.4 Malware

The most well known source for stealth operations on networks is the use of malware. Malware is software that has legitimate use and can be downloaded on the Internet but in the background is a code that gathers and logs all keyboard functions for the purposes of stealth transmission to the attacker. The attacker therefore has access to the compromised computer without the owner of the computer knowing that something is wrong. These malwares also have a defense mechanism that reduces the likelihood of detection and subsequent removal by usual malware removal software. Malware can either run in armour which detects against intrusion prevention systems such as antivirus scan and stealth mode which masquerades as a legitimate software in the systems while intercepting request and returning false data to debugs or scans [17]. Some form of malware use oligomorphic encryption and polymorphic self defense mechanism to prevent removal from the affected computers. Oligomorphic simply uses encryption as a defense mechanism by acting as a virus generating two or more types of decryption routines. Whereas polymorphic simply encrypts the malware itself and provides a different decryption key for each mutation of the virus.

Malwares are the most well known source for worm stealth operations on networks to cause havoc while remaining undetected [18]. Malware are forms of executable worms integrated in legitimate software to monitor the users transactional activities and report to the attacker through an open backdoor [19]. The attacker therefore has access to the compromised computer without the legitimate users knowledge. These malwares are designed to avoid detection and removal by running in either run armor or stealth mode. The armor mode is designed to stop detection software such as antiviruses whereas stealth appears as antivirus or spyware removal software in order to intercept computer communications. The attack software at times encrypts itself to stop removal or acts at antivirus by encrypting antivirus functions also known as polymorphic malware. Oligomorphic malware generates cryptographic keys to stop legitimate antivirus from removing it. Polymorphic on the other hand encrypts the malware itself and creates different versions ever time making it extremely difficult for antispyware removal.

The US needs national policy regarding the existence of malicious software such as malware as a deterrent to the criminals who use malware for identity theft and other cyber crime. Finally all malware and virus related vulnerabilities can be solved by updating operating software patches, installing antivirus software, installing antispyware, managing patches for enterprise networks, limiting access to servers, restricting use of removable drives, filtering email spam and internet content filtering.

3.5 Botnets

Computer bots are systems infested with worms, spyware and other forms of executable on demand software by hackers. Botnets are logical networks of computers compromised computers used by hackers to launch multiple attacks. The computers can be enterprise network devices or home computers infected with computer code to collect personal identifier (PII) data [20]. Botnets are common attack tools for launching dynamic denial of services and data reconnaissance for cyber warfare. The systems owners and operating systems of exploited computers are oblivious to the zombie attacks sent from those machines. Hackers harden the operating systems by upgrading patches of compromised computer to stop other hackers from their conquest after creating backdoors.

3.6 Viruses

Originally viruses were technical nuisance with limited impact on systems but have morphed into systems process disruptions. The impact of viruses in enterprise network includes TCP/IP session hijacking, lost productivity and loss of proprietary data. The operation cost of removing viruses from infested networks has risen exponentially and the frequency of new types of viruses has grown with noticeable service impact on infrastructures [21]. The fix to virus problem requires enterprise policy with standardized antivirus software. The mandatory process automates antivirus scans through group policy on any network device. The fix though useful to enterprise infrastructures could be susceptible to eaves dropping especially if the virus encrypts itself as an antivirus.

3.7 Trojans

Trojans appear as legitimate software but have hidden code for later execution by the attacker. The main purpose of Trojan is to provide a security violation of the system for backdoor execution of functions to bypass security requirements. The Trojans like spyware provide reporting functionality to the attacker through predetermined communication means such as memory dump or event viewer dumps sent as text or email [22]. Computer hackers as individuals or collectively poses the greatest risk to network infrastructures and individual Internet users because they are associated with the rising cost of cybercrime [23]. Studies indicate that hackers bypass information security measure to gain access to PII that leads to identity theft. Hackers or crackers are behaviors associated with electronic crime syndicates that manipulate computer systems for unlawful access to resources.

3.8 Hackers

The computer hacking phenomenon has evolved from curious harmless events to organized crime ring sponsored operations and government sponsored counter cyber warfare strategies. The hacking technologies have evolved from sniffing, packet capturing and session hijacks to sophisticated oligomorphic spyware virtually undetectable by network intrusion systems. The Russian military incursion in Georgia was preceded by unprecedented network infrastructure hack attacks that caused widespread outages on banks, presidential office and other civic offices. This being the first reported military hacking attack that brought an entire country on its knees accompanied by simultaneous military attack. The use of encryption of data when traversing the Internet is a solution to stop hackers from gaining access to corporate data.

3.9 Spyware

Spywares are like worms and viruses except they are intended for stealth operation without service interruptions [24]. Spywares are software tools developed to gather information from unsuspecting users as passive attacks but can also be used to execute other forms of attack. Spywares are downloaded as third party cookies from visited website or as email attachment from an attacker. Since spywares are client side application, security update on the desktops and antispyware are optimal solutions for defending against them.

4. EFFECTIVE DATA SECURITY ENFORCEMENT PROCEDURES

It is imperative for data storage to be properly secured because an exploitation of security vulnerability affects both the customers and the shareholders alike. The individual employees or customers may loss their valuable information, financial loss and time it takes to correct the identity theft as a result of fraud. The organizations would suffer reputation loss, lack of revenue as a result of the breach, federal and state fines as provided the corresponding laws. The cost of repairing a stolen identity has been estimated to range from $80 to $800 with over 175 hours of personal time invested in the repair process which makes it an absolute necessity to protect critical data from unwanted access. Data security begins with the implementation of a culture of security as a tiered approach for protecting sensitive data at an organizational level. The consumers have to be vigilant and discard all purchase receipts that have credit card information or sensitive data by shredding to avoid dumpster diving. The data aggregating companies should provide for consumer awareness training regarding risk of identity theft and enterprise companies should train their employees on steps to avoid being victimized by identity fraud.

To protect critical infrastructures it is incumbent on organizations to use multi-faceted approach such vulnerability detection policy, technical detective solutions, intrusion prevention systems and firewall solutions instead of waiting for attack to occur to trigger reaction [25]. The overwhelming number of vulnerabilities complicates the process of securing network infrastructure by security managers. The use of security tools and password policies provide control mechanisms required for multi-faceted defence. The traditional technical defence mechanisms against vulnerability exploitations are intrusion detection systems, intrusion prevention systems, firewalls, honey pots and vulnerability scanners. It is imperative for data storage to be properly secured to avoid exploitation of security vulnerability.

The type of controls that can be implemented to limit exploitation varies from the type of industry but common practices such as biometric authentication can be used instead of password method, one time password to deter password hacking and grid authentication for the energy industry [26]. The different ways to secure data requires approaching security as an end to end solution by considering information security policies, physical security, network firewalls, host firewalls, IPS, information security training to create an awareness against social engineering. For any solution to work there has to be security awareness and better policies in place coupled with the technology to protect from outside intrusion.

4.1 User Awareness Training

Data security begins with the implementation of a culture of security as a tiered approach for protecting sensitive data at an organizational level. The internal users should keep up to date of security policies and maintain required security best practice recommendations.

4.2 Vulnerability Analysis

The challenges to securing network infrastructures against attacks range from software design, implementation, and configuration and other Internet related vulnerabilities. This is possible because most network resources are interconnected through the Internet, which increases infrastructure vulnerability because of inherent weaknesses of the Internet [27]. To protect against such attacks vulnerability scanning and audit logs are necessary to report potential malicious traffic. Vulnerability assessment and analysis identifies and tracks network attacks and automates threat assessment. The assessment alone cannot provide comprehensive security in the absence of policy, technical controls and incidence remediation process [28]. The commonly used vulnerability assessment tools are intrusion detection systems (IDS) and intrusion prevention systems (IPS) used to detect attacks and network anomalies. They can be installed as network based scanners or on individual host as hot devices.

The second type of vulnerability scanners is honey pots, which are systems, used to simulate network infrastructure so as to monitor the attackers behavior on the systems. The lack of coherent vulnerability assessment policy limits the enterprise's ability to effectively assess and create a vulnerability profile based on findings, which leads to false sense of security. However vulnerability assessment only provided reports but cannot stop a potential attack. An effective vulnerability policy should include updates from authoritative source such as CERT for evaluation. The use of credential caching can be a great deterrence against DOS type of attacks because it allows network devices to maintain a directory of valid login or access credentials which reduces the verification, improves performance delays the flooding process of vulnerability exploitation.

4.2 Firewall

Firewalls are packet filter devices operating based on access control list for access. The role of the firewall system is recognizes and proxy traffic. Enterprise infrastructure compromise of data and VoIP network each representing some form of vulnerability. VoIP traffic has inherent call set up protocols such as SIP and H.323. The development of a security baseline is required for assessment remediation plan to highlight the areas affected by vulnerability scanners for the entire enterprise. Base lining allows for the creation risk levels based on the type of vulnerability detected per system or department.

Developing of security patch delivery policy with available automated resources for audit and exaction of tested updates upon release by software vendors in compliance with ISO 17799 compliance requirements can reduce the number of attacks significantly. System update policy is required to keep antiviruses up to date and system software security fixes to protect against known vulnerabilities.

4.3 Incident Response Team

The exploitation of vulnerabilities are bound to occur irrespective of the controls put in place however organized response policy to such attacks reduces the down time and impact of such exploitation. Information security incident response teams are charged with the responsibility of analyzing attack and identifying diagnostic approach and mitigation response [28]. The response team evaluates attack data against policies, determine that type and nature of attack and formulate a response within the acceptable reaction time [29]. Effective response to DOS and DDOS are early detection, coordinated cooperation between network domains to exchange information without impacting network support payload [30].

4.4 Anti-Malware

The US government lacks national deterrence policy regarding malicious software such as malware exploitation however infrastructure can report attack for acts cyber attack for investigation. Malware and virus related vulnerabilities can be solved by updating operating software patches, installing antivirus software, installing antispyware, managing patches for enterprise networks, limiting access to servers, restricting use of removable drives, filtering email spam and internet content filtering.

4.5 Outsourcing

The recommendation is not to outsource security functions in its entirety however the cloud’s software as a service creates controls for the many moving parts such as proper planning, design coordination, implementation, operation and continuous optimization. Outsourcing information security and risk management for any company is a daunting task that must be entered into very clearly with written expectations for both parties. The security policies have to involve executives participation for budgetary needs, policy regarding encryptions, data media, IPSec designs for remote access on any other medium that private data will be traversing between the host company and the data owner.

5. Data Protection Laws and Policies

This paper discovered that it is absolutely necessary to have a regulation that limits what kind of PII can be collected and stored by data aggregating companies such as medical data hubs or financial data hubs. However the most valuable of all the PII data in the USA is the social security number and should not be shared unnecessarily because about 32 % of identity theft cases are as a result of stolen social security cards. The failure to secure personal data will still lead to an increase in identity theft related to as a result of such vulnerability exploitations.

In 1996, Congress passed and President Clinton signed into law the Economic Espionage Act (EEA). The law was passed to counter increasing domestic and international espionage threats to the U.S. and American corporations with bipartisan support. Acknowledging concern for this growing threat, the House of Representatives passed the EEA with 399 members in support, 3 members against and 31 members abstaining. The intent of the EEA law is to provide a *"federal remedy targeting the theft of trade secrets and theft of proprietary data"* to help protect economic and military sectors of the U.S. economy. However according to Vatis [30], there still exist a failure in enforcement of existing laws and the policy of reporting incidences of attack are purely based on volunteer basis with no corresponding national taskforce for dealing with identity theft or cyber attacks. The financial sectors are however required to report on suspicion of cyber attack. As a matter of policy the US deals with cyber attacks on two fronts namely investigations by the FBI and intelligence gathering to determine if espionage was the intent.

In recent years the US government have enacted Federal Laws that would hold enterprise companies responsible for the mishandling of personal identifying information. The personal identifying information includes but not limited to social security, drivers license, financial account numbers, mother's maiden name, birth date, home alarm codes, wedding anniversaries and any other similar but private information in nature. Also, different states have adopted laws against identity theft like the Florida Statutes 817.568, which criminalizes identity theft making it a criminal felony. At the federal level there is also the Federal Identity Theft and Assumption Deterrence Act (Act) that also considers it a criminal act to unlawfully have access to a person's data or assume the person's identity for personal gain. The identity theft program law includes the core initiatives of assisting victims, educating consumers, law enforcement, and businesses, and established an identity theft data clearinghouse for the maintenance and dissemination.

US Department of Health and Human Services (HHS) began developing a Nationwide Health Information Network to meet the mandate from President Bush to have all medical information online in 10 years. The danger is that once all the medical information is available online then any one can have access to it for purchase without any way of expunging it, accidental disclosure, corruption, loss of health information which can cause bodily harm especially when doctors cannot have access to it in an accident or some sort of medical emergency.

The HIPAA Privacy Rule, including the Security Rule, provides for administrative enforcement of the regulations but not for litigation by private parties. Aggrieved individuals may file complaints with the Secretary of HHS, and HHS may also conduct compliance reviews on its own initiative. CMS, which administers and enforces the Security Rule, enjoys discretion as to which complaints it will choose to investigate. The secretary of Health and Services has the authority to enforce penalties against non complaints ranging from $100 per violation to $25000 during the calendar year. The only part of HIPAA that has merit is the fact that violators can be prosecuted for criminal offence and be sentenced to jail for 10 years or $250,000 or both. The problem however is that an individual cannot sue based on HIPAA violations only the CMS can sue making it very weak because of the lack of private clause because those who have been injured cannot get personal remedies.

The vulnerability and risk of large scale IT outsourcing exposes the infrastructure to internal security and assurance weaknesses. The leadership of internal control oversight required by executives and board of directors are abdicated contrary to Sarbanes-Oxley (SOX) compliance requirement. The lack of internal security policy controls leads to erroneous financial reports and misleading conclusions however the impact of outsourcing can be mitigated by competent business models. The competent business model creates parallel leadership structure to foster controls with the third party vendor. The consistent overseeing of operations, internal controls, procedures and close working relationship with the board reduces risk and internal diminish vulnerabilities.

Negligent entrustment allows for corporations to be legally liable for security breaches in their outsourced data hubs to low wage countries most of which do not have any privacy protection laws. The research paper contends that any such outsourcing company cannot inherently outsource their security responsibilities as well which may complicate the outsourcing to cheap low wage nations. The negligent entrustment law suit the data handler is legally liable for enable cybercrime by failing to have security policies and procedures in place to deter such a crime. Any US company that outsource data processing to any low wage country still have a duty to confirm that the back office has reasonable data security standard, they are also required to do independent audits prior to transmitting private customer data to India and other countries.

Outsourcing security as a service is a pipe dream that cannot be achieved in reality, for the most part the outsourcer do not report vulnerabilities and the partner who manages security does very little nor do they disclose any flaws like in the case of Northup-Grumman and the Virginia department of Health Professionals. Companies should not outsource security in its entirety but can outsource security operations and monitoring while leaving design and policy to the internal staff. Outsourcing security can never be treated as software as a service because there are many moving parts that require proper planning, design coordination, implementation, operation and continuous optimization making it a nightmare when fully outsourced. Outsourcing information security and risk management for any company is a daunting task that must be entered into very clearly with written expectations for both the outsourcer and outsource-e. The said functions have to be clearly defined with monetary penalties should any tenets of the contract be broken by either side, next the security in depth principle has to be deployed so that it is very clear that the hosting company approaches security from the desktop to the data centers. The security policies have to involve executives buy in for budgetary needs, policy regarding encryptions, data media, VPN or any other medium that private data will be traversing between the host company and the owner of the data being secured.

6. RECOMMENDATIONS

Existing literature agree that it is imperative for data storage to be properly secured because an exploitation of security vulnerability affects both the customers and the shareholders alike. The individual employees or customers may loss their valuable information, financial loss and time it takes to correct the identity theft as a result of fraud. The organizations would suffer reputation loss, lack of revenue as a result of the breach, federal and state fines as provided the corresponding laws. The cost of repairing a stolen identity has been estimated to range from $80 to $800 with over 175 hours of personal time invested in the repair process, which makes it an absolute necessity to protect critical data from unwanted access.

There different ways to secure data which requires approaching security as an end to end solution by considering information security policies, physical security, network firewalls, host firewalls, IPS, information security training to create an awareness against social engineering. For any solution to work there has to be security awareness and better policies in place coupled with the technology to protect from outside intrusion. Data security begins with the implementation of a culture of security as a tiered approach for protecting sensitive data at an organizational level. The consumers have to be vigilant and discard all purchase receipts that have credit card information or sensitive data by shredding to avoid dumpster diving. The data aggregating companies should provide for consumer awareness training regarding risk of identity theft and enterprise companies should train their employees on steps to avoid being victimized by identity fraud.

Data inventory of sensitive or personal identifying data collected and maintained by the company need to be done so as to evaluate what level of security is required to protect such. Some steps to take towards protecting personal identifying information is to institute some form of data security project team which involves representative from all the departments within the organization to respond to cases of lost or stolen personal data.

There is still need for future research on the psychology of identity thieves, their enablers and their economic contributions to the organized crimes infrastructures that foster their success under the radar.

7. CONCLUSION

The challenges of securing network infrastructure is continually changing in complexity of attack tools however strategic installation of firewalls, security best practice configuration requirements, strong password policy, implement physical security, cryptographic use for secure remote access, security lock down of devices with up to date patches are first steps in vulnerability mitigation. The increase in identity compromise is due in part to the lack transatlantic international corporation between participating countries or relevant coherent international laws to facilitate prosecution of perpetrators. Identity theft has a crime has been prevalent before the explosion of the internet however the ease of software tools for hacking, phishing, Trojan horses and data aggregation centers have made the access to millions of personal data more easier. Also, the increase of multiple companies storing millions of PII with third party companies such as financial mortgage brokerage companies, medical insurance companies, outsourced service data centers and cloud computing have increased the surge of identity theft.

The information security vulnerabilities will continue to exist as long as new technologies are developed to bypass security limitations however companies can institute coherent information security governance the includes steps to keep their networks secure. The steps could include enterprise security policy, security awareness programs, user security training and deterrent solutions. Individual consumers have to keep antiviruses up to date; install antispyware and practice secure online transactions just to mention a few such steps. Information security governance is critical for management involvement, compliance requirements and to create an enterprise culture of security because employees are the first line on defense against cyber related attacks.

REFERENCES

[1] Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). “Information security threats and practices in small businesses”. Information Systems Management, 22(2), 7-19

[2] Clark, W., & Levin, P. (2009). Securing the information highway. Foreign Affairs, 88(6), 2-10.

[3] Becker, R., Volinsky, C., & Wilks, A. (2010). Fraud detection in telecommunications: History and lessons learned. Technometrics, 52(1), 20-33. Vol. 52, No. 1.

[4] Abdullah, A. (2006). Protecting your good name: Identity theft and its prevention. Paper presented at the First annual conference on information technology, Jacksonville, FL.

[5] Horn, R. (2009). Top 5 emerging cyber threats. Texas Banking, 98(11), 8-11.

[6] Solow, B. (2010). Your good name: Protecting yourself from physician identity theft. Physician Executive, 36(3), 30-33

[7] Agarwal, S., Budetti, P. (2012). Phyisician medical identity theft. The Journal of the American Medical Association, 307(5), 459-460. doi: 10.1001/jama.2012.78.

[8] Gatzlaff, K., & McCullough, K. (2010). The effect of data breaches on shareholder wealth. Risk Management and Insurance Review, 13(1), 61-83.

[9] Krause, J. (2006). Stolen Lives: Victims of identity theft start looking for damages from companies that hold their personal financial information. ABA Journal, 92(3), 36-64.

[10] Wagner, C. (2009). Internet fraud on the rise. The Futurist, 43(4), 15., 43(4), 15-20.

[11] Agarwal, A. K., & Wang, W. (2010). An experimental study of the performance impact of path-based DoS attacks in wireless mesh networks. Mobile Networks and Applications, 15(5), 693-693-709.

[12] Holmes,T. (2010). "Who Should Have Your Social Security Number? " Black Enterprise, Vol. 40, No. 11, pp. 46-47,

[13] Gross, J. R., M. (2007). Looking for trouble: understanding end-user security management. Computers & Security, 25(1), 27-35.

[14] Peretti, K. "Data breaches: What the underground world of Carding reveals". Santa Clara Computer and High - Technology Law Journal, Vol. 25, No. 2, pp. 375-413, September, 2009.

[15] Sharma, J. & Gupta, J. N. (2002). "Securing information infrastructure from information warfare." Journal of Enterprise Information Management, Vol. 15, No. 15, pp. 414-422, December, 2002.

[16] Bamberger, A. K & Mulligan,K.D. (2011). "Privacy on the books and on the ground". Stanford Law Review, Vol. 63, No. 2, pp. 247-315

[17] Mensch, S.& Wilkie, L. (2011). "Information security activities of college students: An exploratory study". Academy of Information and Management Sciences Journal, Vol. 14, No. 2, pp. 100-112.

[18] Vlachos, V. & Spinellis, D. (2007). "A proactive malware identification system based on the computer hygiene principles." Information Management & Computer Security, Vol. 15, No. 4, pp. 295-312.

[19] Maughan, D. (2009). "Inside risks the need for a national cyber security research and development agenda." Communications of the ACM, Vol. 53, No. 2, pp. 29-31

[20] Easton, G. & Easton, A. (2011). "Bot herding with RSS." International Journal of Management and Information Systems, Vol. 15, No.3, pp. 83-90.

[21] Lee, D., Larose, L. & Rifon, N. (2008). "Keeping our network safe: A model of online protection behavior." Behavior & Information Technology, Vol. 27, No. 5, pp. 445-454.

[22] Chen, C., Shaw, R., & Yang,S. (2006). "Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system." Information Technology, Learning & Performance Journal, Vol. 24, No. 1, pp. 1-14.

[23] Castelluccio, M. (2004). "Spyware! Who put that on my machine? " Strategic Finance, Vol. 85, No. 9, pp. 57-58.

[24] Liu, L., Holt, S., & B. Cheng, (2007). "A Practical vulnerability assessment program." IT Proffesional Magazine, Vol. 9, No. 6, pp. 33-42, February, 2007.

[25] Yang, S. & Choi, H. (2010). "Vulnerability analysis and the practical implications of a server-challenge-based one-time password system." Information Management & Computer Security, 18(2), pp. 86-100.

[26] Noel, S. & Jajodia, S. (2008). " Optimal IDS sensor placement and alert prioritization using attack graphs." Journal of Network and Systems Management, Vol. 16, No. 3, pp. 259-275.

[27] Dawkins, J., Clark, K., Manes, G. & Papa, M. (2005). "A framework for unified network security management: Identifying and tracking security threats on converged networks". Journal of Network and Systems Management, Vol. 13, No. 3, pp. 253-267.

[28] Nasheri, H. (2005). "Economic espionage and industrial spying", Vol. 1. Cambridge University Press, New York.

[29] Vatis, Michael. (2004). "Assurance: Trends in vulnerabilities, threats, and countermeasures", Vol. 1, Cambridge University Publishers, New York.

[30] Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). "Preparation, detection, and analysis: The diagnostic work of IT security incident response". Information Management & Computer Security, 18(1), 26-42.

[31] Gross, J. R., M. (2007). "Looking for trouble: Understanding end-user security management." Computers & Security, 25(1), 27-35.

[32] Henderson, James and Rahman, Syed (Shawon);(2010). "Working Virtually and Challenges that must be overcome in today’s Economic Downturn"; International Jyournal of Managing Information Technology (IJMIT); ISSN : 0975-5586 (Online) ;0975-5926 (Print)

[33] Dreelin, S., Gregory and Rahman, Syed (Shawon);“ Enterprise Security Risk Plan for Small Business”; International Jyournal of Computer Networks & Communications (IJCNC), ISSN : 0974 – 9322 [Online] ; 0975- 2293 [Print])

[34] Donahue, Kimmarie and Rahman, Syed (Shawon); (2012).“Healthcare IT: Is yyour Information at Risk?”; International Jyournal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012, ISSN:0974-9330(online); 0975-

[35] Rice, Lee and Rahman, Syed (Shawon); (2012).“Non-Profit Organizations’ need to Address Security for Effective Government Contracting”; International Jyournal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July 2012

[36] Neal, David and Rahman, Syed (Shawon); (2012).“Video Surveillance in the Cloud?”; The International Journal of Cryptography and Information Security (IJCIS), Vol.2, No.3, September 2012

[37] Halton, Michael and Rahman, Syed (Shawon); (2012). "The Top 10 Best Cloud-Security Practices in Next-Generation Networking"; International Jyournal of Communication Networks and Distributed Systems (IJCNDS); Special Issue on: "Recent Advances in Next-Generation and Resyource-Constrained Converged Networks", Vol. 8, Nos. ½, 2012, Pages:70-84, ISSN: 1754-3916

[38] Amin, Syed; Pathan, Al-Sakib, and Rahman, Syed (Shawon);(2011)." Special Issue on Recent Advances in Next-Generation and Resyource-Constrained Converged Networks" , International Jyournal of Communication Networks and Distributed Systems (IJCNDS)

[39] Mohr, Stephen and Rahman, Syed (Shawon); (2011).“IT Security Issues within the Video Game Industry”; International Jyournal of Computer Science & Information Technology (IJCSIT), Vol 3, No 5, Oct 2011, ISSN:0975-3826

[40] Dees, Kyle and Rahman, Syed (Shawon);(2011).“Enhancing Infrastructure Security in Real Estate”; International Jyournal of Computer Networks & Communications (IJCNC), Vol.3, No.6, Nov. 2011

[41] Hood, David and Rahman, Syed (Shawon);(2011).“IT Security Plan for Flight Simulation Program”; International Jyournal of Computer Science, Engineering and Applications (IJCSEA), Vol.1, No.5, October 2011

[42] Schuett, Maria and Rahman, Syed (Shawon); (2011).“Information Security Synthesis in Online Universities”; International Jyournal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011

[43] Jungck, Kathleen and Rahman, Syed (Shawon); (2011)." Cloud Computing Avoids Downfall of Application Service Providers"; International Jyournal of Information Technology Convergence and services (IJITCS), Vol.1, No.3, June 2011

[44] Slaughter, Jason and Rahman, Syed (Shawon); (2011). " Information Security Plan for Flight Simulator Applications"; International Jyournal of Computer Science & Information Technology (IJCSIT), Vol. 3, No 3, June 2011

[45] Benson, Karen and Rahman, Syed (Shawon); (2011). "Security Risks in Mechanical Engineering Industries", International Jyournal of Computer Science and Engineering Survey (IJCSES), Vol.2, No.3, August 2011

[46] Bisong, Anthony and Rahman, Syed (Shawon);(2011). "An Overview of the Security Concerns in Enterprise Cloud Computing "; International jyournal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011

[47] Mullikin, Aryoun and Rahman, Syed (Shawon); (2010). "The Ethical Dilemma of the USA Government Wiretapping"; International Jyournal of Managing Information Technology (IJMIT); Vol.2, No.4, November 2010

[48] Rahman, Syed (Shawon) and Donahue, Shannon; (2010). “Convergence of Corporate and Information Security”; International Jyournal of Computer Science and Information Security (IJCSIS), Vol. 7, No. 1, 2010

[49] Hailu, Alemayehu and Rahman, Syed (Shawon); (2012). “Protection, Motivation, and Deterrence: Key Drivers and Barriers of Organizational Adoption of Security Practices” ; IEEE the 7th International Conference on Electrical and Computer Engineering (ICECE) December 20-22, 2012, Dhaka, Bangladesh

[50] Hailu, Alemayehu and Rahman, Syed (Shawon); (2012). “Security Concerns for Youb-based Research Survey” IEEE the 7th International Conference on Electrical and Computer Engineering (ICECE), December 20-22, 2012, Dhaka, Bangladesh

[51] Neal, David and Rahman, Syed (Shawon); (2012). “Consider video surveillance in the cloud-computing”; IEEE the 7th International Conference on Electrical and Computer Engineering (ICECE), December 20-22, 2012, Dhaka, Bangladesh

[52] Neal, David and Rahman, Syed (Shawon); “Securing Systems after Deployment”; The Third International Conference on Communications Security & Information Assurance (CSIA 2012), May 25-27, 2012, Delhi, India

[53] Johnson, Mazie and Rahman, Syed (Shawon); “Healthcare System's Operational Security”; IEEE 2011 14th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, December 22-24, 2011

[54] Rahman, Syed (Shawon) "System Security Specifications for a Multi-disciplinary Research Project",7th International Workshop on Software Engineering for Secure Systems conjunction with The 33rd IEEE/ACM International Conference on Software Engineering (ICSE 2011), May 21-28, 2011, Honolulu, Hawaii.

[55] Rahman, Syed (Shawon) and Donahue, Shannon; "Converging Physical and Information Security Risk Management", Executive Action Series, The Conference Board, Inc. 845 Third Avenue, New York, New York 10022-6679, United States

[56] Rahman, Syed (Shawon) and Peterson, Mike; "Security Specifications for a Multi-disciplinary Research Project"; The 2011 International Conference on Software Engineering Research and Practice (SERP'11), Las Vegas, Nevada, USA July 18-21, 2011

[57] Jungck, Kathleen and Rahman, Syed (Shawon); " Information Security Policy Concerns as Case Law Shifts toward Balance betyouen Employer Security and Employee Privacy"; The 2011 International Conference on Security and Management (SAM 2011), Las Vegas, Nevada, USA July 18-21, 2011

Authors Bio:

Dr. Omondi John Opala is an associate professor at the Department of Informati on Technology at Devry’s University’s Keller Graduate School and Technical Lead at Cisco Systems, RTP, NC. Dr. Opala’s research interests include systems architecture, information security governance, big data and software defined networks (SDN)

Dr. Syed (Shawon) M. Rahman is an Associate professor in the Department of Computer Science and Engineering at the University of Hawaii-Hilo, Hawaii, USA and a part-time faculty of School of Business and Information Technology at the Capella University, Minneapolis, MN. Dr. Rahman’s research interests include software engineering education, data visualization, information assurance and security, digital forensics, cloud computing security, web accessibility, software testing and quality assurance. He has published more than 95 peer-reviewed articles. He is a member of many professional organizations including IEEE, ACM, ASEE, ASQ, ISACA, and UPE.