The Increasing Complexity of Hacker Attacks on Personal and Corporate Information Systems: A Proactive Mitigation Response Model

[1]Osuagwu O.E., [2]Ndigwe Chinwe, [3]Ijeoma Agwamba, [4]Okide S, [6]Njoku Obilor A. and Dave [5]Ogbonna

[1]Department of Computer Science, Imo State University, Owerri
profoliverosuagtwu@gmail.com +2348037101792
[2] Department of Computer Science, Anambra State University, Uli, Anambra State
[3]Department of Computer Science, Federal Polytechnic, Nekede, Owerri
[4]Department of Computer Science, Nnamdi Azikiwe University, Awka
[5]Department of Network Engineering Technology, South Eastern College of Computer Engineering And Information Technology, Owerri
[6]Department of Computer Science, Federal University of Technology, Owerri

Abstract

Information Technology and associated tools have brought both blessing and curse to humanity. In spite of awe-inspiring attacks of hackers and malware writers, the immense benefits of this technology have prevented many from withdrawing from its use. Just any one is affected by the services of Information Technology - Transportation Systems, Personal and corporate financial records and systems, Banking and financial institutions, Hospitals and the medical community. The public telephone network, Air Traffic Control, Power systems and other utilities, the government and the military. No body is left out. To prevent the collapse of the Internet, the Internet Workforce and the industry have pooled resources together to provide some mitigation or palliative strategies, but these efforts have been inadequate to prevent continuing massive attacks by hackers. The attacks are becoming daring and more complex by day. The most advisable mitigation approach is to take the proactive route for survival. This paper has provided a modest list of emerging attacks on corporate information systems, a catalogue of the motivators, intension of hackers and sketches out a model of proactive and reactive mitigation response model for individuals and corporations.

1.0 Introduction

When we look at few statistics on Cyber warfare, one would ponder if the ascendance of Information Technology application is a blessing or a curse. For example, in January, Riptech announced it had culled more than 128,000 attempted attacks on 300 Riptech customers over six months. And in March, Predictive Systems amassed more than 12 million malicious-looking events from 54 sensors around the world in just three months equating to 90 attempted attacks per second. The Riptech study found 30 percent of all attacks came from computers in the U.S.; next was South Korea, at 9 percent. In fact, five of the top 10 sources of attacks were computers in Pacific Rim countries. In terms of intensity, i.e. attacks per Internet user, Israel far outdid any other nation [6]. According to [7] Chinese hackers already have unlawfully defaced a number of U.S. web sites, replacing existing content with pro-Chinese or anti-U.S. rhetoric. In addition, an Internet worm named "Lion"

is infecting computers and installing distributed denial of service (DDOS) tools on various systems. In 1999, FBI Computer Crime & Security Survey observed that out of 521 security practitioners in the United States, 30% reported system penetrations from outsiders, an increase for the third year in a row, 55% reported unauthorized access from insiders, also an increase for the third year in a row, Losses due to computer security breaches totalled (for the 163 respondents reporting a loss) $123,779,000 averaging a loss of $759,380 [8]:

There are more than 403 million unique known malware variants, and more than 55,000 known malicious web domains. Symantec software blocked 5.5 billion malicious web-based attacks in 2012 alone, 315 mobile device vulnerabilities were discovered in 2011. At least 232 million identities were maliciously exposed in 2011. The major US government defence agencies reported an average of 10 million cyber-attacks per day, per agency [10]. Recently (2008-2013) Verizon gave an overview of security breaches in Fig. 1 below:

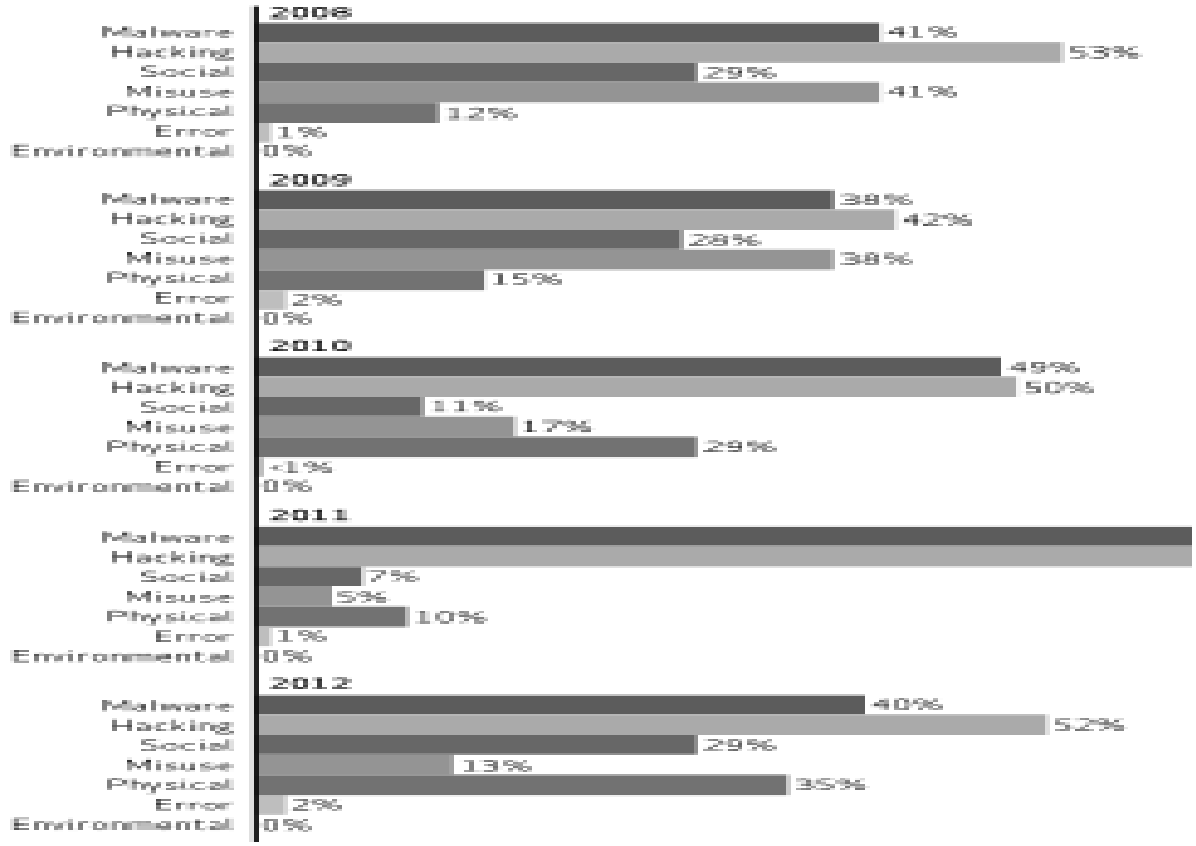

Fig. 1: 2013 Data Breach Report [source: (Verizon)]

Fig 1.8 observes a mixed growth from 2008 to 2013 in all the variables reported – Malware (47% in 2008 was down to 40% in 20012, hacking increased from 52% to 53% in 2012, an increase of only 1%, Social remained static from 29th in 2008 to 29% in 2012, Misuse was down from 41% in 2008 to 13% in 2012. This may be due to some proactive measures taken by management. Physical rose from 12% in 2008 to a whooping 35% in 2012! Error only marginally rose from 1% in 2008 to 2% in 2012. Environmental factors remain no threat as it earned no score in 2008 and 2012. According to ITU [9] Botnets', or as the media calls them, 'Zombie Armies' or 'Drone Armies', and their associated malware have grown over the years into a

multimillion dollar criminal economy, which now constitute huge risk to government, critical infrastructure, industry, civil society and to the broader Internet community. That is what the current situation is! The threat is real!!

Corporate Information is the most valuable asset to all firms. If some trade secrets stored in the organizations data bases are compromised, the firm might be heading to a failure trajectory with its concomitant negative consequences for the national economy. It is therefore imperative that such information systems be protected from the massive attacks of hackers and malware writers. Security is about *regulating access to assets.* Thus, the goals of any corporate security policy are based on the CIA Triad [1]:

- Confidentiality
- Integrity
- Availability
- (authentication)
- (non-repudiation)

The three variables that constitute the Triad include ***confidentiality***, ***Integrity*** and ***Availability***. **Authentication** supports Confidentiality and Integrity while **non-repudiation** adds value to the concept of Integrity during business transactions

Confidentiality refers to the assurance that information is shared only among authorized persons or organizations. Breaches of confidentiality can occur when data is not handled in a manner appropriate to safeguard the confidentiality of the information concerned.

Integrity is the ***assurance*** that data cannot be created, changed, or deleted without proper authorization as such would compromise the confidence placed in such valuable asset.

Availability is the **a**ssurance that the systems responsible for delivering, storing and processing information are available 24/7 and accessible when needed, by those who need them and authorized to use such information. [2]

Webopedia [3] has defined ***authentication*** as the process of identifying an individual, usually based on a username, password, biometrics such as finger print or voice recognition. Thus, in computer security systems, *authentication* is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication ensures that the individual is **who he or she claims to be**, but says nothing about the access privileges of the individual.

Non-repudiation:

Web Dictionary [5] defines Non-repudiation as a state of affairs where the purported maker of a statement will not be able to successfully challenge the validity of the statement or contract. The term is often seen in a legal setting wherein the authenticity of a signature is being challenged. But this specifically refers to online transaction. In digital communication, it specifically refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

The summary of the foregoing discussion is encapsulated in Fig. 1.1 below.

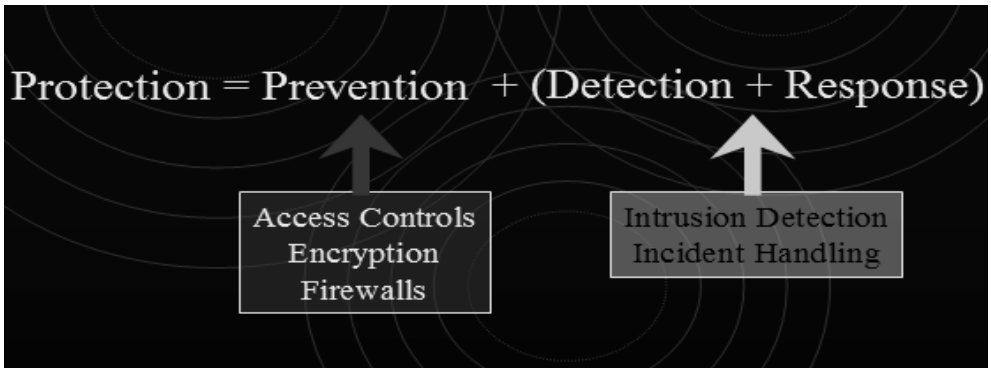

Fig. 2 Corporate Computer Security Operational Model

Fig. 2 is in essence saying that to protect Corporate Information systems require some proactive response model such as providing protection via Access Controls, Encryption and proper setting of Firewalls; Detection and Response which includes Intrusion Detection and Incident handling

Most security problems can be grouped into one of the following categories:

- Network and host misconfigurations
- Lack of qualified people in the field
- Operating system and application Flaws
- Deficiencies in vendor quality assurance efforts
- Lack of qualified people in the field
- Lack of understanding of and concern for security

Organizations may approach attacks proactively or reactively. Most organizations only react to security threats, and, often times, those reactions come after the damage has already been done.

The key to a successful information security program resides in taking a *pro-active* stance towards security threats, and attempting to eliminate vulnerability points before they can be used against the firm. Other threats are created via weak security in TCP/IP, Eavesdropping, Theft of valuable information, Fraud, Authentication and Non-repudiation.

Cyber Warfare

The security challenges facing e-organizations today is analogous to pure combat warfare**.** The description of the following battles confirms this assertion. Some of these treats include Identity spoofing, Denial of service, Loss of privacy, Loss of data integrity, Replay attacks, Viruses, Spyware, Trojans and other Malicious Software such as Botnets, Phishing, Spam, Cyber Stalking, Cyber Bullying and Online Predators etc. One of the worst vulnerabilities that can hit a corporate network is the virus/worm outbreak. Such attacks can tie up networks, cripple mail servers and disable many individual PCs [12].

Some definitions and grouping of illicit activities in the Cyberspace.

- *Hackers*: They enjoy intellectual challenges of overcoming software limitations and how to increase capabilities of systems.
- *Crackers*: These of hackers who illegally break into other people's secure systems and networks.
- *Cyber Terrorists*: This group of attackers threaten and attack other people's computers to further a social or political agenda

Hacker Motivation.

The following factors are part of the intrinsic motivators that let them do what they do:

- *The challenge* – we want to tell the world of our technical prowness.
- *Ego* – placing oneself on top of society

- *Espionage* – act as agent for others for financial gains.
- *Ideology* - a belief system such as secrets should done away with and let the world be transparent (Wiki Leaks).
- *Mischief* – to cause mayhem and disrupt social processes
- *Money (extortion or theft)* – to make money
- *Revenge* – to respond to previous maltreatment say by past employer.

Hacker Characteristics:

They are predominantly male folks. Most are aged from mid-teens to mid-twenties and they lack social skills. Most have fascination or obsession with computers and a good proportion of them are underachievers in order areas of human endeavour and see computing as a means of becoming important and powerful in society [4].

For ***Malware writers***, their motivations include the desire to see how far the virus can spread. The second motivator is to cause damage and destruction to a targeted individual or organisation. Others include the desire to achieve a feeling of superiority/power and to leverage some form of personal gain. Finally, they intend to use their technical prowess to teach some lessons to the Internet communication and to conduct some experiments.

Attack Pattern and Threats

We would like to precede attack patterns with some important definitions**:**

- ***Vulnerability***: A flaw or weakness in system security procedures, design, implementation, or internal controls that may result in a security breach or a violation of the system's security policy.
- ***Threat***: The potential for a specific vulnerability to be exercised either intentionally or accidentally
- ***Control***: measures taken to prevent, detect, minimize, or eliminate risk to protect the Integrity, Confidentiality, and Availability of information.
- ***Vulnerability Assessment***: The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system
- ***Vulnerability remediation*** is the process of fixing vulnerabilities. Remediation choices
- For every vulnerability there are three choices for remediation -Fix - eliminate vulnerability altogether, Accept - the cost of fixing outweighs the risk, Mitigate – do not outright fix but use additional layers of security to lessen the risk presented by the vulnerability
- You should arrange to plan to remedy all vulnerabilities found in the system. This plan must include whether to fix, mitigate or accept vulnerabilities or Whether to use automatic or manual remediation Strategy to mitigate any remaining vulnerabilities and try to justify why a vulnerability should be accepted as it is without spending extra financial resource on the threat..

Malware Writers

These are a group of attackers responsible for the creation of malicious software that infects and destroy information systems**.** Malware is Malicious Software - deliberately created and specifically designed to damage, disrupt or destroy network services, computer data and software. There are several types. It includes viruses that conceal themselves, infect computer systems, replicate themselves and deliver a *payload*. ***Worms*** are Programs that are capable of independently propagating throughout a computer network. They replicate fast and consume large amounts of the host computers memory. ***Trojan Horses*** **are computer programs** that

contain hidden functionality that can harm the host computer and the data it contains. Trojan Horses are not automatic explicators - computer users inadvertently set them off and attacks commence.

Software Bombs are Time Bombs usually triggered by a specific time/date. ***Logic Bombs*** are triggered by a specific event. Both are introduced some time before and will damage the host system.

Samurai

These are hackers hired to legally enter secure computer or network environments for nefarious objectives or to check the vulnerability of the network to various forms of attack**.**

Phreakers

This group of attackers focus on defeating telephone systems and associated communication technologies.

Phishing

This group specialize in sending out 'scam' e-mails with the criminal intent of deceit and extort. Thus, *Phishing* is a technique used by strangers to ***fish*** for information about you, information that you would not normally disclose to a stranger, such as your bank account number, PIN, and other personal identifiers such as your National Insurance number. These messages often contain company/bank logos that look legitimate and use flowery or legalistic language about improving security by confirming your identity details. This is becoming very rampant. You see in your email box your banker's logo and form format requesting you to fill your secret details. If you do, your email will automatically be compromised and the hacker will seize your password and change it to his and take full control of all communications sent to you. The programs are java applets which automatically installs themselves once you open the mail!

Spam

This is the main source of criminality particularly in Nigeria. It involves sending of unsolicited and/or undesired bulk e-mail messages, often 'selling' a product targeting of instant messaging services. The promise of disproportionate benefit to themselves and tries to extort some money deceitfully**.**

Zombie Computers

These are computers dedicated for fraud or systems used by 419 crooks to do illegal activities.

Defacing Websites

Hackers can leave their presence on other people's websites by defacing form example a Catholic Church website with nude women. Many sites have fallen foul of this activity and they include FBI, CIA, NASA, British Labour and Conservative Parties and New York Times as well as Conservative Party Website Hacked and Defaced 1997.

Denial-of-service (DoS)

DoS or ***distributed denial-of-service attack*** is an attempt to make a machine or network resource unavailable to its intended legitimate users through some of the attacking techniques already discussed.

SQL Injection Attacks

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution.

Mitigation and Counter Measures

There are two basic approaches used to deal with security vulnerabilities: These are ***proactive*** and ***reactive***. Proactive approaches include all measures that are taken with the goal of preventing host-based or network-based attacks from

successfully compromising systems. Reactive approaches are those procedures that organizations use once they discover that some of their systems have been compromised by an intruder/hacker or attack program. We shall now discuss these two approaches and mitigation strategies adopted. Both are not opposing forces. There is need to find a balance between how many resources can be devoted to proactive measures designed to deter network attacks, and how much to devote to reacting to intrusions [12]

Proactive measures:

These may include physical security of building, screening of personnel, legal framework to deter criminals and training of employees. Encryption is the strongest link we have for securing data. Everything else is worse: software, networks, and people.

Setting up Security Monitoring Plan

The purpose of this plan is to identify suspected access violations and attempted system intrusions. A sample plan for example is:

- ***Daily review of remote access log-ins*** to identify failed access attempts.
- ***Review of system access logs*** for access to systems during non-work hours.
- ***Review of traffic*** on external gateways
- Review of access to application system utilities and privileged user activities
- ***Review of access*** to sensitive files or data Monitoring licenses registered versus licenses used
- Inventorying of PC software
- Developing and distributing approved software lists
- Developing software usage policies

- **A physical security plan** should check the use of Cipher or key pad locks, Fencing, Guards, Monitoring devices, Maintaining authorized personnel access lists, Limiting access to only essential operations personnel, Maintaining sign-in logs and Badges

- **An environmental security plan** would include Backup power (UPS) Air conditioning, Fire suppression devices (fire extinguishers, halon, other), Fire detection devices (sensors), Heat detection devices, Business continuity plans, Alternate processing facilities and Disaster recovery plans, System and data backups.

Backup and Recovery

Backups are critical and must be performed so that system, program, or information loss or damage can be efficiently restored. Backups should be stored away from the processing facilities. Tape management techniques need be reviewed often.

Risk Assessment

Deployment of IT for corporate information services is a risk. An Information Systems Manager ought to ponder what could happen (threat event)? If it does happen, how bad could it be (threat impact)? How often could it happen (threat frequency, annualized)? And how certain are the answers to the first three questions (recognition of uncertainty)?

Risk Management

This involves questions on what can be done (risk mitigation), how much will it cost (annualized) and is it cost effective (cost/benefit analysis)?

Business Continuity Planning (BCP)

Integrate the following phases into your BCP policies;

- Awareness and discovery
- Risk assessment
- Mitigation
- Preparation
- Testing

- Response and recovery

Risk and Impact Analysis

The firm should attempt to identify her assets, determine vulnerabilities, estimate the likelihood of exploitation, compute expected annual cost, survey applicable controls and their costs and project annual savings attributable to control**.** An estimate of the probable cost may include Estimate of Expected Loss such as Legal obligations for preserving confidentiality and integrity, Business agreements on the expected service, Cost due to public disclosure, Benefit to competitor due to compromise of data, Loss of future business, credibility, Computational cost and outsourcing possibility, Value to other from the data and Cost of data recovery or reconstruction

Impact Analysis of possible attack would include the identification of what the enterprise has at risk, which business processes are most critical, Prioritization of risk management and recovery investments, identifying the enterprise's vulnerability to risks so that they can be mitigated in the project design phase.

Key Management (KM)

KM is a Set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. It involves the initialization of system users within a domain, generation, distribution, and installation of keying material, controlling the use of keying material, update, revocation and destruction of keying material, storage, backup/recovery, and archival of keying material**.**

Configuration of Firewalls is critically important if information systems have to be able to contain the attacks at first level.

Other measures include:

- Update the software on your computer weekly (or more frequently)
- Install anti-virus and anti-spyware software and keep it up-to-date
- Use accounts and strong passwords
- Encrypt sensitive information
- Do not install unknown software from unknown sites
- Do not share your accounts/passwords
- Use password protected screen savers
- Deploy Biometric Authentication Systems such as Finger print, iris of the eyes, voice recognition.
- Deploy Intrusion Detection and Prevention System and effective firewall on your servers
- Do not use the same password for all accounts
- Change passwords frequently
- Use more difficult passwords on more sensitive accounts

- Use a password safe (but do not lose the master password
- Do not open unknown emails and attachments.
- Visit only reputable web sites http://safeweb.norton.com/
- Do not reply to SPAM or Phishing emails
- Only login to servers for the duration needed - disconnect when done
- Do not let others use your computer irresponsibly
- Use a Credit card for online shopping
- Do not Give out your personal information in response to an *unsolicited* email, phone call, or voice mail. If you are in doubt If in doubt, call the company using another legitimate phone number (not the one provided in the email or phone call).
- New scams use social networking sites to get your background personal information
- Be cautious when using open wireless networks. Others using the network maybe be "sniffing" the network. Security Expert Claims Thieves

Can Detect Wi-Fi In Sleeping Computers.

- If you *must* use a public computer, change the password on the account accessed using a secure computer ASAP

For individual Laptops, Implement passwords on the device, Backup your data frequently and test backups. Store backups away from the laptop. Encrypt sensitive information. Watch your laptop at all times. Keep your laptop in your possession at all times and do not leave it out in your hotel room. You can also lock up your laptop with some software. Do not leave your laptops in the car, it could be stolen. Some people have left their Laptops in their cars and came back to see their car windows broken and their laptops taken away.

Reactive Measures

These are measures taken after an attack has succeeded. It includes reporting to the cyber crime committee and EFCC for tracking the culprits and their eventual prosecution and installation of *adhoc* measures to prevent further attacks. However, the damage has been done! Normally when the worse happens, management implements temporary countermeasures, especially when a rampaging worm or virus makes it impossible to wait for thorough testing and careful application of patches. Often, this strategy means following a defined incident-response plan and shutting down ports on firewalls and routers or blocking IP addresses. The ability to put together an incident-response team, notify all necessary parties (internally and externally), and follow clear guidelines for escalation of issues is integral to successful implementation of these countermeasures [11].

Summary and Conclusion

Corporate information Systems attacks are increasing daily with exponential complexity. This threat requires a strategically planned action by firms to put attacks at bay and ensure the CIA tenet of Confidentiality, Integrity and availability. A consolidated Information security unit need be set up in every organization to detect and prevent the growing trend of Denial of Service attacks, phishing, and malware attacks. This unit should be equipped with the right tools. Deployment of mitigation strategy must come after critical risk analysis to avoid economic waste. Paying good attention to security and associated risks is bound to secure the most important asset of organizations and prevent an inclination towards failure trajectory.

References

[1] http://en.wikipedia.org/wiki/Information_security

[2] Ndigwe Chinwe, Osuagwu O.E. et. Al. (2013) ***Understanding Integrity in Networked Data Base Applications,*** **MicroWave International Journal of Science & Technology**, Vol.5 No. 1 December 2013

[3] http://www.webopedia.com/TERM/A/authentication.html

[4] Cybercrime by Steven Furnell (2002) p 47

[5] http://en.wikipedia.org/wiki/Non-repudiation

[6] *Missed Opportunity* By Scott Berinato, www.cio.com, Apr 2002

[7] ***Collateral Damage May Soon Have A New Definition. "China Warns Of Hack Attack"Washington TimesApril 23, 2001, Front Page***