International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 9 (2014), pp. 937-940
© International Research Publications House
http://www. irphouse.com

"Cyber Attacks: An impact on Economy to an organization"

Hetram yadav[1] and Shashant Gour[2]

*MS Cyber Security, Sardar Patel University of Police,
Security & Criminal Justice, Jodhpur[1,2]*

Abstract

This paper shows that the Cybercrime is a world scale issue regarding economy because businesses that operate online have to deal with cyber-crime one way or another. The cost to the economy loss, can estimated, is significant and likely to be growing. Cyber-attacks are not only affecting modern computing industries but also government economy, its infrastructure and conventional business also. It emphasisonrequisite of cyber security in an organization. Cyber-attacks causes billions of $ and reputational loss to an organization.Cyber-attacks have several forms of attacks like DoS, information theft, database destruction and many other forms that adversely affect the economy differently.The systematic study of the cost of cybercrime recommends that society should spend less on antivirus software and more on policing the internet.We have suggested some solutions by applyingthosean organization can reduce economic impact due to cyber-attacks.The results of this study suggest that businesses need to look again at their defenses to determine whether their information is indeed well protected.

Keywords: Cyber-attack, DDoS, Phishing, Virtual, ISO27000, BS7799

1. Introduction

Cyber refers to the characteristics of the culture of computers, Information technology (IT) and virtual reality. It includes electronics, digital, internet, web, communication networks, online services etc. Today in the world of computers it has become essential to corporate sectors and government organizations to move from conventional computing system to cyber system. Thus we can say that we all are surrounded and dependent on continued availability, confidentiality and accuracy of Information and Communication Technologies. But there are many vulnerabilities to penetrate, attack in cyber systems due to lack of awareness and knowledge in this new emerging era. Attackers may use different technique to harm a particular organization in different ways. It impacts an organization in different ways like economically, business disruptions etc. Cyber-crime losses about $300 billion to 1 trillion to world's economy which is 0.4% to 1.4% of total GDP[1]. There is no specific solution to attacks but the awareness and implementation of policies is the best suggestion to this growing era.

2. Mostly used Attacking Techniques to Organizations

1.1. *DDoS:* In distributed denial of service attacks the attackers makes the resources unavailable to the legitimate users. The attacker create botnets and malware in the networks and create zombie machines that are remotely controlled by the attacker and constantly send request to the server then the server gets so busy to avail the services or resources to the intended users.

According to Neustar survey over 300 businesses were targeted by DDoS attacks. Mostly web based industries such as financial services, telecom services, retail, travel,IT were victimized often. When a website goes down it costs upto $10K per hour[2].

Business uses web for customer service, direct sales and brand awareness but intense competitor, angry customers or social and political motivated protestors can easily takedown a website lacking adequate protection.

2.2 *Phishing:*Phishing is an attempt to acquire vital information such as username, password, credit card details, pin code, account no, unique id through deceiving as trust worthy entity. It can be done by SMS, e-mail, telecommunication etc.

As RSA Anti-Fraud Command Center reported the total no of fishing attacks was 59% higher than 2011 in 2012.The global losses estimated at $ 1.5 billion 2012 that was 22% higher than 2011.

2.3 Social Engineering:It is a method to get the critical information of authentication and identity by social interaction with the intended person. An outside hacker uses socio-psychological tricks on important employee in context to an organization to gain access their system. So in this technique the needed information is obtained directly from the person rather than breaking into the system without even realizing that they have been manipulated.

2.4 *Data Breach or information loss:*It is essential for an organization to store the data for fast manipulation, analysis, research, login in electronic form in the system. Many times this data is so important to their organization if once it is obtained by unauthorized user may loss huge amount. Data can be breached either by negligence, malicious attack or system glitch. Attacker can manipulate this data, sell this data or can publish in any way it will harm to organization reputation image, trust and revenue.

The largest breach that was reported in December actually occurred during November, where 40 million identities were exposed [4].

2.5 *Malware:*The malicious software installed in a system is a malware. It has dramatical abilities and it can communicate to its originator in background without the knowledge of system administrator. It is the most powerful tool to harm an organization. It can installed by e-mail, downloading attachment and sometime by USB or other external devices.

In public sector 1 e-mail out of 72 in public sector, 163 in education, 218 in finance,235 in marketing, 236 in accommodation industry contains a malware [3].

2.6 *Insider Attacks:*An organization has a threat from its own employees also. The employees share the sensitive information to outsiders to gain some financial benefits or to make the organization in loss. Low level management persons have least knowledge about the importance so unintentionally they share the confidential and sensitive data with attackers. Middle level management has full knowledge of the importance of data so it is very simple for them to misuse the data. Top level management also involved in data share but comparatively lesser than mid-level due to more responsibility.

2.7 *Social Sites:*Through online social media many other competitive organizations attempt to decrease the reputation, brand. They post or tweets negative propagations against an organization so that it reduce the trust among the people.

3. Impacts on Organization due to attacks

1. Economic: All types of attacks results into loss to the economy of an organization.
2. Reputational: when a company faces a cyber-attack, it decrease the trust and faith among the people and people afraid to invest further in the organization.
3. Loss of IP: Sometimes the Intellectual Property of an organization like patent, copyright trade secret is theft which causes a huge loss.
4. Loss of sensitive business information: The data that has value in worth of money should be preserve but loss of such data harm to the organization as it can be used by the competitors.
5. Lack of Trust: Once a organization faces an cyber-attack then customers does not feel safe with that organization. It compel its customers to move on other services.

6. Business Disruption/ Lost Sales: Due do different types of attacks business or sales also affected. In denial of service attack customers cannot get the services so it makes loss to the organization in a very short period of time.
7. Equipment Loss: Sometimes the malwares destroy whole the networking equipments so organization have to spend a lot of money to reinstall them.
8. Stock Prices: Attacker may interpret the stock prices of the organization to reduce the value and image of the particular organization by using malwares.

4. Recommendation to reduce the economic impacts on an organization due to cyber -attacks

1. Human Resource of an organization should be trained time to time to make awareness about the latest attacking technique.
2. An organization should implement cyber security standards like ISO 27001, BS 7799 etc to confirm the security.
3. Data Loss Prevention (DLP) tools also be used to monitor the data flow.
4. At the time of recruitment background and the reason for joining should be interviewed.
5. To prevent the DDoS attacks the session time should be as small as possible.
6. There is a myth that a small organization need not to implement cyber security standards due to cost factors but eventually it losses them higher than the cost to implement the security.
7. All the hardware and software used in the organization should be standardized and according to own parameters.

References

[1] The Economic Impacts of Cyber Crime and Cyber Espionage report by McAfee.

[2] Nuestar-insights DDoS attacks survey q1-2012.

[3] Symantec intelligence report 2013.

[4] Internet Security Threat Report- Symantec 2013.

[5] Cyber Crime Protecting against the growing threat PwC's sixth global surveyMarch 2012 Vol. 256.