EasyChair Preprint

№ 7321

Effect of a Cyberattack on a Company's Economic Performance

Lokesh Kumar, Nikhil Singhal, Mudit Agarwal, Mukul Kumar and Jaivardhan Bhardwaj

January 10, 2022

Effect of a cyber attack on a company's economic performance

Lokesh Kumar
Computer Science and Engineering
Poornima College of Engineering
Jaipur, India
2020pcecslokesh98@poornima.org

Nikhil Singhal
Computer Science and Engineering
Poornima College of Engineering
Jaipur, India
2020pcecsnikhil132@poornima.org

Mudit Agarwal
Computer Science and Engineering
Poornima College of Engineering
Jaipur, India
2020pcecsmudit124@poornima.org

Mukul Kumar
Computer Science and Engineering
Poornima College of Engineering
Jaipur, India
2020pcecsmukul125@poornima.org

Jaivardhan Bhardwaj
Computer Science and Engineering
Poornima College of Engineering
Jaipur, India
2020pcecsjaivardhan125@poornima.org

Abstract - Globally, the cyberattack headlines keep getting grimmer and grimmer: Hackers Steal Bank's Valuable Data. Big Box Store Says Millions of Credit Card Records May Have Been Snatched. US Indicts Chinese Army Officers for Hacking Industry Trade Secrets and most recent of all Wannacry Ransomware infiltrates windows platform. Cyberattacks of the past year have been rattling the IT world, making executives and IT managers wonder how vulnerable their own networks might be. And the incidents are increasing. A recent global survey PwC conducted with CIO Magazine and CSO Magazine shows that the number of attacks reported by midsize companies has jumped 64% since a year ago. Today's hackers are farsighted and more tenacious now when it comes to midsize and smaller companies. To avoid these losses, companies need to take a hard look at their defenses up front. Yet a big reason companies often fail to invest in cybersecurity is that they see it as discretionary spending, not a business imperative. With profitability being top of mind, businesses tend to be more inclined to invest in growth activities than defensive measures. This paper employs an exploratory research design on existing literature with a focus to generate a workable hypothesis to be tested in future empirical studies. The objective of the study is to create awareness of cyber-attacks and to explore the impacts of cyber-attacks on company's economic performance. This will be followed by identification of cyberattack techniques that can be used against company's economic performance.

1. **Introduction** : Increased customer access to services has driven businesses to move operations to e-business. With this move to a new method of doing business, businesses have adapted operating procedures to capitalize on this new distribution channel. (Harris, 2016) In addition to business to consumer (B2C) channels, business to business (B2B) channels have changed as well. Internal business operations have also become enhanced through the communication channels provided by company. (Anderson, 2014). Company economic come in many sizes, shapes and markets. Whereas Amazon can be viewed as a reinvention of normal business, e-Bay, Yahoo, and Google can be seen as entirely new creations. Each of these firms has had its business troubles, yet has ridden out the tough times and joined the ranks of profitable firms in the business landscape. Regardless of the industry, the basic business model is one of firms interfacing with suppliers and customers. The number of relationships is bounded in type, but not in quantity. (Anderson, 2014) For a firm to double its ability to service its customer base the driver is mostly just one of capital – just add servers.

   Cyber security can simply be defined as security measures being applied to computers to provide a desired level of protection. (Anderson, 2014). The issue of protection can be defined using the acronym CIA for Confidentiality, Integrity, and Availability. (Bicknell, 2015) Confidentiality refers to the property that data should only be viewable by authorized parties. Integrity refers to the principle that only authorized users are allowed to change data, and that these changes will be reflected uniformly across all aspects of the data.

   Availability refers to the principle that data and computer resources will always be available to authorized users. Using the word simple to describe computer security is misleading however, much as it can be said to be simple to play golf. Just it the ball in the hole in as few strokes as possible. (Burns & Fiftheen 2013). The current lack of Government support for security on the Internet is forcing businesses to rely on their own personal security measures to protect themselves from cybercrimes, however this is not sufficient in ensuring that cyberspace is a safe haven.

2. **Research Methods** This paper employs an exploratory research design on existing literature with a focus to generate a workable hypothesis to be tested in future empirical studies. The objective of the study is to create awareness of cyberattacks and to explore the impacts of cyberattacks on company economic performance. This will be followed by identification of cyberattack techniques that can be used against company economic performance. This will be followed by recommendation of preventive mechanisms that should counter cyberattack attempts since most company are focused more on reactive rather than proactive measures. The results of this paper will be used to advice company economic stakeholders on how to improve cyber security and how to prevent a cyber-attack.

The security threats in E-Business environment are as follows:

Virus: A virus is a malevolent program which is anticipated to affect the system with severe loss. The virus may get fix itself to the separate file or a group of files leading to severe loss by acquiring more space, modifying files, folders, slow response of the system.

Adware: Adware is considered to be a malevolent which are embedded into the advertisement if the customer unknowingly clicks on it leads to fraudulent activity by seizing customer credentials.

Spyware: Spyware that performs like an application but its main motive is to gather the credentials of the individuals after gathering the credentials it will send this to the malicious attacker which are connected in the network.

Ransomware: Ransomware is a type of malicious software that threatens to publish the victim's data or block access to it until a ransom is paid. On June 2017, one of the worst ransomware attacks in history was carried out by attackers.

The cyber-attack that are possible at customer side are as follows:-

Phishing: Phishing is an attempt to seize customer's identifications such as PIN number, account details. The malicious attacker may add the forged E-commerce login page to the legitimate website if the website is vulnerable to attack. Normally, the forged company websites are widely spread by emails. If the customer has an awareness of this type of cyber-attack he/she will be protective from this attack otherwise it leads to an identity theft by grabbing the user credentials. Seized credentials may leads to threatening the customer by fulfilling the attacker needs.

Pharming: Pharming is similar to phishing attack. The main motive of this attack is to steal customer information by redirecting them to the spurious website. When the domain name of the website is typed in the web browser it first converted into the Numerical address that is IP address which are done using DNS Server. If the IP address is redirected to spurious website it will lead to Pharming attack. This can be done by compromising the DNS Server also it is not a usual attack like phishing.

Log Forgery: The un-sanitized input from the user to access the log files may leads to log forgery or inserting malevolent things to the log. By altering the log file information may leads to a severe impact.

Password attacks: To crack the customer login id and password there are many password cracking tools by cracking the password the attacker may steal the customer's online credentials. Also it leads to cancelation of ordered products by the customer or ordering the new product.

Cross side scripting Attack: The other name for cross side scripting attack is XSS Attack. It is the most common type of attack that occur on the website. In this attack, the legitimate company site is inserted with malevolent code which is done by the attacker. The attacker may vandalize the company site by exploiting this attack.

Brute force attack: It is a type of password guessing attack by using the trial and error method. If the attacker knows about the target customer this type of attack can be performed easily by guessing the password.

Man in the middle attack: It is a common type of attack on the internet. The attacker may silently listen the communication that has been taken place between the customer and the server.

3. **Conclusion:** There is a lack of knowledge throughout as to what cybercrime and its threats are. The Government's efforts to encourage company economic performance and discourage cybercrime are virtually unknown and the majority feels that it would have little impact on their company. Many company do not perceive themselves to be in any great danger and so do not take it as seriously as they should. Their thought process is based on reactive measures rather than proactive measures. The Government should support security on the Internet is so as to protect company from cybercrimes thus ensuring that cyberspace is a safe haven. From the above foregoing, the following two hypotheses are derived: the involvement of the government in supporting security on the internet will improve company economic security and focusing more on proactive rather than reactive measures by the e-business stakeholders will lead to a more secure company economic performance.

References:

Business Leaders Warn of cybercrime Threat to Internet Development, 2010

Burns, R.2013, Introduction to Research Methods

Sage Publications, London, Internet Denial of Service Attacks and the Federal Response,

www.cdt.org/security/000229judiciary.shtml

Franklin, I. 2011, A Can of Worms, Science Direct

Gengler, B. 2017, PayPal's anti-fraud team, ScienceDirect, vol.2002, issue3,.