The Economic Effects of Cyber-Attacks in the Tech Industry

David Allen

Thomas Nelson Community College

ITE 119: Information Literacy

Dr. Michael Mann

November 3, 2021

Abstract

Cyber-attacks are far too common in today's world. They can have a huge impact on today's society, from a local level and expanding into an international level. Many things can happen to a business once they become victims of a cyber-attack, which can ultimately ruin their plans for success. Businesses lose a lot of things like their data, time, and money just to recover from these attacks and try to improve their defenses to prevent another attack. The main point of all of this is how well the tech industry deals with these situations and how it affects them, as they are the ones who deal with these situations most of the time whether it be directly or indirectly. This paper will discuss the economic effects of cyber-attacks on the tech industry by using information such as type of attacks and economic effect of type of attack.

Introduction

Before talking about how cyber-attacks effect the tech industry, there needs to be a discussion about the various types of viruses and what they can do in order to steal information from businesses. First, attackers use malware, which is a malicious type of software used to enter someone's computer for the intent of harm or illegal activity (Evans et al., 2016). Attackers use malware to distribute viruses, which can then infect your computer to then do harm to it. Hackers use one type of attack called a worm. Worms have the ability infect on their own through a network without any further interaction from a person. Once a host computer is infected in the network, it then searches for another computer in the same network to attack. A Trojan virus pretends to be a specific program, but users end up clicking on it and it actually ends up being a computer virus. Another type of virus is an encryption virus. Hackers use ransomware to encrypt files by asking for a ransom. The only way that a user can unlock these files is to pay the amount the hackers ask for. Hackers can also use rootkits to take control of a computer without the user even knowing it. As shown, there are many ways that a hacker can maliciously attack a computer using malware, and there are many others out there that I haven't even talked about, like a DDoS and zombies. Hackers have a wide variety of tools to use at their disposal. These types of tools can harm users and steal valuable information from them. An even larger threat would be businesses and larger corporations like Google, Wells Fargo, or any other type of large corporation. These types of attacks can devastate a business by stealing data, money, or any other valuable information that belongs to a company. Businesses need to be on high alert for these kinds of things because it can make or break your success.

Protection Against Viruses

When it comes to the average internet user, they need to make sure they stay protected so that they browse the internet in the safest way possible. The same can go for any business as well, but they have a lot more on the line than just data. With that in mind, there are multiple ways that users can protect themselves on the internet. One way to do that is using a secure firewall (Evans et al., 2016). Windows and MacOS are known to have reliable firewall software to use. There are also multiple anti-virus software packages that come with a secure firewall such as Norton, McAfee, and AVG. The most common way for a user to protect their identity is making sure that they have a secure password. The best way to make sure a password is secure enough is to make sure it has a combination of different letters, numbers, and symbols. Users can also test their passwords using sites such as Password Meter to test its strength. Many people can be under threat of viruses, but they can also protect themselves online as much as there are malware. Doing so can result in an overall safer and improved experience while online.

Making Decisions in IT Related Systems

There is a lot to decide when it comes to making a decision as an IT manager of a business. A study shows the rate of a hacker's success of being able to attack a company (Kshetri, 2018). This study concluded that a hacker has a higher success rate in attacking a smaller company compared to a much larger one. Larger companies tend to spend more money on their defenses compared to the smaller ones that have less valuable information. This shows that the smaller companies need to improve their defenses in order to prevent cyber-attacks and order to stay ahead of the game.

The Impacts of Cyber-Attacks on Businesses

Cyber-attacks have a large impact on businesses and the tech industry of today. Businesses have a lot at stake when it comes to the threat of a cyber-attack. Many of these can include their loss of revenue, loss of data and equipment, loss of intellectual property, cybersecurity improvements, court fees, customer protection, regulatory penalties, and forensics (Pinto et al., 2020). To determine the total impact of a cyber-attack, a company must add up these estimated amounts (Council of Advisors, 2018). These numbers can vary from company to company based on multiple factors. Overall, these elements play a factor in how much an event can affect a single organization. Depending on the amount of damage caused, this could be an eye-opener for many businesses, even for the smaller ones that are trying to make a name for themselves and could use

WannaCry and the Impacts of it on the Tech Industry

An example of a cyber-attack that made an impact on the tech industry is WannaCry. WannaCry is an encryption virus, or ransomware, that was launched on Friday, May 12, 2017 (Castillo & Falzon, 2018). It was launched after a security gap was found in the Microsoft Windows operating system. This attack infected over 300,000 computers in 150 different countries (Lawrence & Robertson, 2017). The people affected by this virus were asked to pay a ransom in order to unlock their files. It was eventually stopped by a cybersecurity expert named Markus Hutchins after finding an exploit in the virus. This attack ended up having a negative effect on the companies that were attacked but ended up having a positive effect on tech companies specializing in cybersecurity. The effect it had on the tech companies was that the

attack had led to a positive rate on stocks. This shows the reliability of cybersecurity companies during a time of crisis and how useful cybersecurity can be for a company.

Conclusion

This paper has discussed the many ways that cyber-attacks can have an effect on businesses and even the tech industry. Businesses have a lot to lose when a cyber-attack happens. Not only does it affect the business affected by the attack, but it also has an impact on the tech industry. Smaller businesses should be aware of changes in the tech industry and follow the business models of the larger ones to have a greater chance of defense from cyber-attacks. Adapting to cyber-threats in the industry can overall improve a businesses success.

References

Council of Economic Advisors. (2018, February). *The Cost of Malicious Cyber Activity to the U.S. Economy*. hsdl.orgland Security Digital Library at NPS. https://www.hsdl.org/?view&did=808776

Daniel Castillo & Joseph Falzon. (2018, February 2). *An analysis of the impact of WannaCry cyberattack on cybersecurity stock returns*. Economics and Finance Research | IDEAS/RePEc. https://ideas.repec.org/a/bap/journl/180308.html

Evans, A., Martin, K., & Poastsy, M. A. (2016). *Securing Your System: Protecting Your Digital Data and Devices*. https://learn.vccs.edu/courses/409279/files/108511137/download?download_frd=1. https://learn.vccs.edu/courses/409279/files/108511137/download?download_frd=1

Kshetri, N. (2018, January). *Introducing the IT economics department.* IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8291803

Lawrence, D., & Robetson, J. (2017). *"The global hack could have been much, much worse"*. Bloomberg. https://www.bloomberg.com/news/articles/2017-05-18/the-wannacry- global-hack-could-have-been-much-much-worse

Pinto, C. A., Keskin, O. F., Kucukkaya, G., Poyraz, O. I., Alfaqiri, A., Tatar, U., & Kucukozyigit, A. C. (2020, December 30). *Defense acquisition innovation repository: Cybersecurity acquisition framework based on risk management:*

Economics perspective. Defense Acquisition Innovation Repository. https://dair.nps.edu/handle/123456789/4504