**The Effect of Security Threats on Workplace Productivity**

**Abstract**

As technology becomes increasingly integrated into our society, security threats are becoming much more present. Producers and consumers of software are at risk of many different forms of attacks from malicious users. These attacks can be inflicted by unknowing employees and users, or by malicious users and hackers. The existence of security threats cause an effect on workplace productivity because technology companies must plan, analyze, and develop code that prevents malicious users from gaining access to sensitive data. Workplace productivity can also be greatly affected if an attack were to actually occur, such as a data breach. In these scenarios companies must take extensive measures to ensure security can be brought back to their product. There are many techniques that technology companies can implement to increase the efficiency of developing security measures for their products. It is important for these companies to take every measure possible in order to protect their users from malicious attacks. This paper will analyze the types of attacks companies may be faced with, the effect of these attacks, and how to plan and account for these types of attacks.

**Introduction and Research Guidelines**

In the world of technology, security threats are ever-present. Today, most technology is developed virtually, hosted on servers, and used through connectections over the internet. With these new developments, security has become more of a priority for many technology companies. The changing of priorities has caused an impact in the workplace productivity of these companies, because special attention needs to be given to areas of development that were previously not considered. Depending on the type of technology a company produces, thoughtful consideration is necessary to develop a deep understanding of the potential security risks that surround their product. Many companies have developed cyber-security roles within their employee hierarchy in order to address the potential security risks. While these types of roles can increase the productivity of the workplace, non-security related developers can still become held-back by security measures. The existence of these potential security threats forces developers to take more time to produce their technologies, because they need to consider the potential security risks that could harm their technology. Besides taking extra time to develop well-rounded code, security threats that actually break into the technology, whether they are stealing data or injecting malicious code, can also affect the productivity of the work environment. The research of this paper involved finding sources that informed about the types of security threats that pose risks to software development companies, how these threats can slow productivity in the workplace, and what these companies and their developers can do to avoid these threats. This paper will analyze the total effect of security risks that pose threats to software development companies, including the slowing of workplace productivity due to these security risks.

**Potential Security Risks**

Technology companies face a wide variety of security threats every day. Not only is the technology product at risk, but the actual employees, and the data of users is oftentimes at risk. Malicious users are people who abuse their trusted privileges for the technology product. These users are not always consumers of the product, but they can also take the form of internal employees, or anyone who has access to the developmental material of the product. Malicious consumers can impose a wide variety of security threats. A major issue for companies is Phishing Attacks [2]. This type of attack accounts for 90% of the threats that a technology company may face [2]. A Phishing attack happens when a malicious consumer poses as a trusted user, employee, or contracter. The malicious consumer will attempt to persuade an employee or user to click on a link or download a file that will ultimately give the malicious user access to data or security credentials. An internal example could be a malicious user sending an email to an employee for a technology company. This email could say something like “update login information” with a link to a look-alike sign-in website. If the employee were to fall into this trap, they could potentially be giving out login information to a malicious user that can then get access to sensitive information. An external example could be very similar to an internal example, where an attacker sends an email to a user of the product, but instead of capturing employee resources, the attacker could be gaining access to a specific user's data. Both of these pose risks to the company, and should be taken into account in the developmental process. Another major risk that poses a threat to software companies is malware attacks. This type of attack occurs when a malicious software infects a company owned device. Similar to phishing attacks, this type of attack can affect consumers and internal employees. A common example of this is when an employee uses a personal device while at work. For example, an employee may use a personal USB storage drive while at work. Their storage drive may contain some form of malware and when used at work, the malware infects the work computer. Once on a computer, the malware can cause systems to break down, or allow an attacker to obtain access to data or code. While this type of attack involves a physical aspect, this is still a risk that technology companies must consider in order to provide a safe product for end-users. There are many other forms of attacks that could expose sensitive material besides these two major types, although all of the attacks pose threats in the form of exposing user data, company data, or developmental materials.

**Effect on Workplace Productivity**

Workplace productivity can be slowed down in many ways by security threats. More recently, many technology companies have been adopting styles of development such as Agile or DevOps. These forms of development seek to increase efficiency and timing of production. As a result of this, an increased amount of security risks form because developers can not take the appropriate amount of time to consider all security risks. Eventually, companies need to access the security risks of their product in order to create a secure software. This involves completing an entire analysis of their product to find potential security risks, which creates a slowdown in productivity because it is an inefficient developmental process [1]. This type of slowdown occurs before a security risk occurs. Many productivity slowdowns can occur when an actual security threat occurs. A common threat that occurs for technology companies is a breach of data. When this happens, the company must take time to solve the issue. A typical response of a company that experiences a breach involves assembling a team of experts including a data forensics team and a legal counsel, securing the areas that allowed the breach, and stopping the current data loss [4]. All of the aspects of a typical response take significant time to complete. When a breach occurs, the workplace productivity is significantly affected in a negative way because the company pauses all other operations in order to mend the current emergency. Developers must look back at code that has already been written, and try to access where security risks could be possible. Taking the extra time to analyze code for a second time causes developers to stop production on any new projects because their time needs to be focused on the security breach. Developing code and then accessing for security risks, as well as responding to an emergency significantly impacts workplace productivity, although there are developmental processes that can improve the efficiency of accounting for security risks.

**Accounting for Security Risks**

In recent years, 53% of technology companies have increased their cybersecurity budgets, with 65% of companies expecting to spend more funds on cyber security in the coming years [1]. Creating dedicated cybersecurity related roles allows for developers to focus on creating a product, while the security employees focus on creating a safe product. Security by design is a technique that aids productivity when accounting for security risks. This technique helps to plan for security risks early in the developmental process. When using this technique, the architecture of the product is taken into account in the design phase so that all potential risks can be accessed before extensive development has taken place. Similar to the security by design technique, risk-first and risk-last are also development techniques that allow for considering security threats. The risk-last technique is when the security risk is analyzed after the threat has been analyzed. This means that time could be spent by the developers analyzing risks that will never happen [1]. The rist-first technique is the more time efficient method of taking security into account because only the threats that actually occur are accessed. Most of the methods for accounting for security risks for a product involve considering potential risks in the design phase. This allows companies to release a product that is secure and able to defend and prevent attacks from malicious users. The techniques previously described are measures to protect a product from attacks, although companies must also create policies to protect from other types of attacks. Many companies do not allow employees to use their own devices while at work. This can aid in avoiding introducing malware onto a company's systems. Most companies also likely have policies regarding emails so that employees can be protected from phishing attacks. Many companies also have different levels of security clearances so that low level employees such as interns cannot access sensitive materials. All of these measures are important for companies to consider, because oftentimes these technology companies store user data that could be very sensitive, and it is their obligation to protect their users from data breaches.

**Conclusion**

As technology becomes increasingly integrated into our society, it is important for the companies that produce the technology to take every measure possible to protect the consumers of their product. While taking these measures into account while developing a product can affect the workplace productivity by slowing down production time, there are many techniques that are able to mitigate this inefficiency. Many technology companies have the ideology of quick turn around times when developing a product, although these companies have the obligation to their users to protect their sensitive data from all forms of malicious intent.

**References**

[1] Tuma, Katja, et al. “Finding Security Threats That Matter: An Industrial Case Study.” *ArXiv*, 8 Oct. 2019.

[2] Das, Sanchari, et al. “All About Phishing: Exploring User Research through a Systematic Literature Review.” *ArXiv*, 16 Aug. 2019.

[3] Faily, Shamal. *Designing Usable and Secure Software with IRIS and CAIRIS*. Springer International Publishing, 2018.

[4] “Data Breach Response: A Guide for Business,” *Federal Trade Commission*, 29-Apr-2019. [Online]. Available: https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business. [Accessed: 12-Apr-2020].