A Study of Third-Party Software Compliance and the Associated Cybersecurity Risks

Rashel Dibi, Brandon Gilchrist, Kristen Hodge, Annicia Woods, Samuel Olatunbosun, and Taiwo Ajani

1 Introduction

Third-party software (TPS) are a great investment for companies. They help companies better manage their day-to-day processes and, in some cases, create a better user interface for their customers to use. The idea behind acquiring third-party cloud management tools is to offset what native tools cannot manage or do not see [1]. Customers expect certain capabilities and accessibility to a company and its' products; however, companies may not have the time or ability to support such customer needs especially with continuing evolution of the Internet and technology.

1.1 Third-Party Software in the Cloud

Most purchased TPS are in the cloud. The biggest benefit of third-party tools is visibility into a distributed cloud environment [1]. This is a plus and one of the main reasons why companies decide to purchase cloud-based TPS. Cloud-residing data provides a measure of stability to clients, especially in situations where natural and man-made disasters are present risks. Having a TPS also makes it easier on the administrator because they do not have to focus on things such as systems upgrades

R. Dibi · B. Gilchrist · K. Hodge · A. Woods · S. Olatunbosun (✉)
Department of Computer Science, Norfolk State University, Norfolk, VA, USA
e-mail: r.s.dibi@spartans.nsu.edu; bjgilchrist@nsu.edu; k.hodge102989@spartans.nsu.edu; a.woods77749@spartans.nsu.edu; sbolatunbosun@nsu.edu

T. Ajani
Department of Computer Information Systems, Ferrum College, Ferrum, VA, USA
e-mail: tajani@ferrum.edu

H. R. Arabnia et al. (eds.), *Advances in Software Engineering, Education, and e-Learning*, Transactions on Computational Science and Computational Intelligence, https://doi.org/10.1007/978-3-030-70873-3_54

and other maintenance issues. This leaves ample time to focus on other needs and issues at the company.

General Compliance Issues and Cybersecurity Risk

When it comes to compliance management, the ability to maintain and protect information, remediate problems, and provide adequate compliance reports is essential [2]. Companies have generally overlooked Information Technology Compliance and cybersecurity until recent years. In 2019, the total number of reported third-party breaches was 368. This number increased from 328 in 2018. In addition, the number of records exposed in these breaches skyrocketed to 273% last year, from just over 1.7 billion in 2018 to 4.8 billion in 2019 [3].

Problem Motivation and Importance

(i) Problem: TPS companies are a continuous cybersecurity threat. Because of this, their data and the companies that they provide a service to are in jeopardy of being hacked. Moreover, regarding compliance, companies do not always have the correct measures to ensure that they are legally protected when hacking occurs.
(ii) Motivation: Hackers are always looking for new ways and new products to retrieve data from. Companies with TPS provide more incentive to hackers.
(iii) Importance: Cybersecurity and compliance protocols are needed for TPS. Providers may have companies' data from several countries within their network. No matter what kind of service that the company provides, any given company that they work with are liable to have sensitive personal information that could potentially end up in the wrong hands.

2 Literature

Security is an integral part of functional socioeconomic systems especially considering that people want their personal information protected from hackers and breaches. Security professionals are working diligently to ensure the safety of all people, especially during this time of the coronavirus pandemic when hacking is at the highest rate. The status of security risks is at a peak during the pandemic because of increased online activities and traffic. People are doing a fairly good job of selecting the TPS, but third parties need to be reviewed on a more regular basis to make sure that they keep up with standards, company requirements, as well as local and federal statutes [4]. When one thinks about security and the many attending risks, completing annual checks with the security can improve overall security functions in the security systems. Additionally, ensuring that the TPS are

adhering to the guidelines that are set out in the contract is just as important. It is not just about preventing breaches, but also making sure that the proper protocols are set in place when it happens. Risks are inevitable when addressing cybersecurity for TPS, but how one prepares for potential threats and work to improve the company computer systems can impact the chances of hackers gaining access to the system. Hackers work tirelessly to hack into systems, and there is no guarantee that they will be successfully apprehended. The number of fugitives residing in the United States is difficult to pinpoint because arrest warrants may be issued for minor offenses, such as a failure to appear for a traffic violation, or for more serious matters, such as when criminal suspects are on the run [5]. This information shows how easily criminals can get away with committing crimes such as hacking systems online specifically. One study estimates that two million criminal warrants may be active at any time [5]. Therefore, one cannot rely on the law being able to catch up with perpetrators of online crimes.

Compliance is an integral piece to the puzzle and information security is paramount at the industry level. It must be understood that IT security regulations exist for companies to not only be held accountable, but to also maintain proper data security, prevent data breaches, and minimize the financial burden when there is a data leak or loss. Cybershark, a cybersecurity outfit, states that IT regulations improve corporate security measures by setting baseline requirements [6]. It is important to note that consumers place their trust in any organization whose services they subscribe to. Maintaining compliance with these regulations is comforting to consumers. According to Cybershark, a number of US security compliance laws currently exist. While these laws may not be applicable to every industry, the most common of these regulations include the General Data Protection Regulation, Health Insurance Portability and Accountability Act, Sarbanes-Oxley Act, and Federal Information and Security Management Act of 2002 [6]. The security risks associated with outsourcing to third parties add to the overall complexity of being in compliance. While it may be difficult to maintain and know what laws or regulations apply to the services provided, they must be a priority.

3 Methodology

This project reviews compliance issues and mitigations surrounding the use of TPS applications by organizations, companies, and consumers. It is difficult to find any entity that does not rely on third parties to support its operations [7]. Compliance is considered one of the highest concerns for companies when it comes to the data they maintain or use. Compliance is defined as the set of processes, in a way that is required by a rule or law [8]. The ultimate goal of this study was to have a better understanding of the risks associated with and worth accepting when using third-party software applications and how to mitigate compliance-related issues. In addition, it is the intent to emphasize the importance of enforcing compliance– in

an effort to detect and prevent violations of procedures, which could protect major companies/organizations from litigation.

The use of literature reviews is beneficial in assessing what other entities have been observed and how to use those findings as applicable to risk management. This involves understanding the risk management process as applicable to information technology, systems, and cybersecurity.

There are a multitude of security incidents or data breaches on the rise due to the use of TPS applications. This study helps in understanding why outsourcing to a third party could pose an extreme risk and what the impacts of those risks could be. The purpose of this study is not in support of or against the use of any one particular third-party software application nor is it for or against any particular organization/entity.

4 Results

The study of compliance as it relates to security management can be defined as obedience or an agreement of the parties involved. Hackers are constantly seeking new ways to hack software systems. During the coronavirus pandemic, many Americans have resulted to doing business online, which gives hackers more opportunities to take advantage of vulnerable systems. Many Americans are considering TPS compliance being one that is equally as good as the other parties. TPS is specifically invented for businesses and other security agencies are leaning toward using it as well. The TPS has its risks—just as any security program—and can be a source of concern to security professionals who would try to improve systems daily to eliminate any confusion. The TPS has added risks especially during the pandemic period.

A few other things were revealed during this investigation regarding TPS compliance, associated with cybersecurity risks. In addition, findings confirmed that the risks associated with TPS are specifically unique to the company. This affords the opportunity to conduct trend analysis over time and determine workable steps and solutions to prevent hacking. When systems are breached, there can be panic. Panic occurs when every system is working effectively one day and then a major problem occurs the next day due to hackers. The study revealed that being prepared for the unexpected—such as the coronavirus pandemic—is important in evaluating elevated security risks. Policies, agreements, IT regulations, and requirements are implemented to ensure companies and their consumers are held to a security-focused standard. It is historically documented that organizations dedicate immense man-hours to work diligently to provide a safe and secure cloud computing/TPS environment.

5 Recommendations

The TPS compliance and its associated security risks are discussed more often since there has been an increase in services regarding third parties rendering their expertise to manage company programs [9].

When dealing with TPS, at times, companies do not handle their system with the same level of security as their own—this can expose their internal infrastructure with the vulnerabilities being exploited within that third-party application [9]. In result, this could lead to hackers accessing sensitive data within the organization or even installing ransomware—making their system inaccessible until the company pays a certain amount.

Mitigation to implement handling these risks with TPS is to conduct an analysis of the third-party software that is intended to be utilized evaluating the information security risk already identified [9]. The analysis can reveal how aligned their policies are for their customers and to ensure that the regulations are able to accurately hold the third-party companies responsible for protecting the customer's information within the software application. Additionally, the analysis also reveals the number of incidents and information security breaches that have occurred, successful and unsuccessful attempts, and the history of partnerships the third party had, which displays the outcome of those relationships. If companies pursue use of TPS with known vulnerabilities, they can implement additional controls to ensure that their company's network infrastructure is also protected [9].

In addition, companies should test the software before installing the application onto their network [10]. The software should meet security compliance requirements associated with the company's security policy and should pass all criteria listed. Anyone utilizing TPS applications should always ensure use of the latest version with the latest patch and set the requirement to automatically receive updates [10].

6 Conclusion

In conclusion, since there has been an increase in security vulnerabilities within TPS applications, a company must always be on the alert. When a company partners with a third party who offers application services, the company must have open communication of what expectations are to be met during the contract. They should sit down and go over both party's security policies to ensure they are aligned, and both agree. This prevents any disagreements in the future and allows the company to maintain their security posture to their standards. The company should always ensure that they are in compliance with their own regulations to prevent any vulnerabilities within their network but also should treat the third-party application software just as important. This ensures parties, employees, and customers are protected from cyberattacks.

References

1. Things to know about using third party cloud management ... [Online]. Available: https://www.datacenterknowledge.com/archives/2015/10/09/things-to-know-about-using-third-party-cloud-management-tools/. Accessed: 24-Apr-2020
2. Maintain, protect, and diminish risk with a comprehensive IT compliance strategy, Smartsheet. [Online]. Available: https://www.smartsheet.com/understanding-it-compliance. Accessed: 29-Apr-2020
3. J. Vijayan, Third-party breaches - and the number of records exposed – increased sharply in 2019, Dark Reading, 12-Feb-2020. [Online]. Available: https://www.darkreading.com/attacks-breaches/third-party-breaches%2D%2D-and-the-number-of- records-exposed%2D%2D-increased-sharply-in-2019/d/d-id/1337037. Accessed: 24-Apr-2020
4. E. Holbrook, Ensuring compliance among third parties. Risk Manage. **58**(4), 16–17 (2011). Accessed 27 Apr 2020
5. M.A. Rothstein, C.N. Coughlin, Ensuring compliance with quarantine by undocumented immigrants and other vulnerable groups: Public health versus politics. Am. J. Public Health **109**(9), 1179–1183 (2019). Accessed 27 Apr 2020
6. IT compliance: IT security regulations & compliance management, BlackStratus, 06-Sep-2019. [Online]. Available: https://www.blackstratus.com/compliance/. Accessed: 28-Apr-2020
7. R. Putrus, A risk-based management approach to third- party data security, risk and compliance, (2017). [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/a-riskbased-management-approach-to-thirdparty-data-security-risk-and-compliance. Accessed: 26-Apr-2020
8. "In compliance with," Merriam-Webster. [Online]. Available: https://www.merriam-webster.com/dictionary/incompliancewith. Accessed: 26-Apr-2020
9. P. Paganimi, Third-party application security risks in modern companies, VERACODE, Oct. 15, 2015. [Online]. Available: https://www.veracode.com/blog/2015/10/third-party-application-security-risks-modern-companies-sw. Accessed 25 Apr 2020
10. D. Kaplan, 5 security tips for using third-party applications, Trustwave, Aug. 20, 2014. [Online]. Available: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/5-security-tips-for-using-third-party-applications/. Accessed 29 Apr 2020