The Weakest Link in Internet Privacy: Security and Compliance Risks in Third-Party Vendor Data Handling

Dr. Motunrayo Adebayo

ABSTRACT

The new internet economy relies on third-party sellers, such as cloud computing service providers, SaaS and services, payment processing services, and marketing services. On the one hand, such sellers make scaling and innovativeness possible, and, on the other hand, such sellers endanger the safety of personal data and the sanctity of the law. This paper discusses the vulnerabilities inherent to vendor ecosystems using case studies of the Target and SolarWinds breaches to provide examples of the weaknesses present in systems. It also talks about the regulatory frameworks such as GDPR, CCPA, HIPAA, and PCI DSS, and outlines the impediments to implementation and lapses in responsibility. This empirical study proposal of the best internet company practices on vendor risk is provided to contribute to benchmarking in this under-researched field. Lastly, there are technical safeguards, organizational measures and policy recommendations, and finally a call to a global Vendor Privacy Assurance Standard. The results show that vendors are the least strong link in privacy protection, and that there is a need for concerted efforts across the industry, regulators, and academia.

Keywords: internet privacy, third-party vendors, data breaches, GDPR, CCPA, HIPAA, PCI DSS, vendor risk management, compliance, supply chain security.

Classification: LCC Code: KF1263.C65

Language: English

Great Britain Journals Press

LJP Copyright ID: 975842
Print ISSN: 2514-863X
Online ISSN: 2514-8648

London Journal of Research in Computer Science & Technology

Volume 25 | Issue 4 | Compilation 1.0

The Weakest Link in Internet Privacy: Security and Compliance Risks in Third-Party Vendor Data Handling

Dr. Motunrayo Adebayo

ABSTRACT

The new internet economy relies on third-party sellers, such as cloud computing service providers, SaaS and services, payment processing services, and marketing services. On the one hand, such sellers make scaling and innovativeness possible, and, on the other hand, such sellers endanger the safety of personal data and the sanctity of the law. This paper discusses the vulnerabilities inherent to vendor ecosystems using case studies of the Target and SolarWinds breaches to provide examples of the weaknesses present in systems. It also talks about the regulatory frameworks such as GDPR, CCPA, HIPAA, and PCI DSS, and outlines the impediments to implementation and lapses in responsibility. This empirical study proposal of the best internet company practices on vendor risk is provided to contribute to benchmarking in this under-researched field. Lastly, there are technical safeguards, organizational measures and policy recommendations, and finally a call to a global Vendor Privacy Assurance Standard. The results show that vendors are the least strong link in privacy protection, and that there is a need for concerted efforts across the industry, regulators, and academia.

Keywords: internet privacy, third-party vendors, data breaches, GDPR, CCPA, HIPAA, PCI DSS, vendor risk management, compliance, supply chain security.

I. INTRODUCTION

The current digital economy relies on a sophisticated network of third-party vendors to deliver valuable functionality to the internet services. Companies have been turning to external providers to perform their tasks more and more, be it cloud-hosting service providers or payment processors, analytics software, etc. Not only has this dependency been accompanied by a healthy share of advantages, including convenience in the innovation process, scalability, and cost-effectiveness, but it has also resulted in threats to privacy and data security that are widely spread. This is particularly worrisome because vendors often require direct or indirect access to sensitive personal information in order to finish their work, and are therefore of great interest to the malicious actors (IBM Security, 2023).

The fact that major data breaches tend to occur in the most vulnerable area of privacy and security defence means that vendor ecosystems tend to be the weakest. One of the best-known instances of a hacked vendor account that leaked the personal and financial data of over 40 million consumers was the notorious 2013 hack at Target (Centre for Strategic and International Studies [CSIS], 2014). But most recently, the SolarWinds breach showed that attackers can leverage a very trusted vendor to breach thousands of organizations along the supply chain (Cybersecurity and Infrastructure Security Agency [CISA], 2020). These examples underscore the structural nature of privacy risk in relation to vendors and raise urgent concerns of accountability, compliance, and mitigation.

The authors of this research paper examine the security and compliance risk of third-party vendor data processing of internet services. Specifically, it addresses three research questions that guide the study: (1) What categories of third-party vendors are the most threatening to the privacy of personal data? (2) Are there signs of systemic weaknesses in practice demonstrated by actual

breaches by vendors? (3) What do regulatory regimes and practices in the industry do to mitigate or fail to mitigate these risks? To answer these questions, this paper identifies gaps in vendor oversight, evaluates the regulatory environment, and offers both technical and policy recommendations on how information privacy risks that are vendor-driven can be mitigated.

1.1 The Vendor Ecosystem in Internet Services

The internet services also have a huge and intricate vendor ecosystem comprising both direct service providers and sub-processors. In its simplest form, this ecosystem comprises cloud hosting vendors, Software-as-a-Service (SaaS) vendors, marketing and analytics vendors, payment processors, and specialized infrastructure vendors (such as content delivery networks (CDNs), and vendors of cybersecurity solutions) (National Institute of Standards and Technology [NIST], 2022). All of these types of vendors have privacy risks depending on the nature and amount of data that they process.

The most elementary type of vendor is perhaps cloud providers, since an organization is able to grow without necessarily possessing a huge on-premise infrastructure. This, however, is at the cost of the dependency of the security practice on the vendors to be out-of-conformity with the compliance requirement of the data controller (Pearson and Benameur, 2010). Similarly, SaaS vendors usually deal with sensitive user data, including health records in telemedicine products or financial data in enterprise resource planning applications, and would, therefore, be exceptionally weak in the event of abuse or breach.

The other risk vector is marketing and analytics vendors, where they require aggregation of vast quantities of data and profiling. These services may be defined by processing and distributing personally identifiable information (PII) and behavioural data with third parties without explicit user consent to do so. As it was stated above, this confidentiality (first of all, due to the European Union, General Data Protection Regulation (GDPR) is one of the reasons why the regulation review has been extended to data-sharing deals (European Union, 2016). Payment processors accept and process financial transactions, and should be based on the Payment Card Industry Data Security Standard (PCI DSS), which also introduces an additional component of compliance-based vendor risk management (PCI Security Standards Council, 2022).

The whole vendor ecosystem is a lifeblood of digital innovation and a potential Achilles heel of privacy protection. Organisations failing to chart and trace their vendor relationship risk the failure to spot the weakest links in their data supply chain that would undermine consumer trust and regulation.

1.2 Privacy Risks in Vendor Relationships

Privacy threats of the third-party vendor relationships do not exist only within the traditional conceptual framework of cybersecurity risks. Unauthorized access to sensitive information via the loosely secured vendor accounts or integrations is one of the largest risks. Vendors have a high likelihood of privileged access to systems and databases and are therefore an ideal victim of credential theft and insider abuse (Kshetri, 2021). The problem is also exacerbated by the fact that insecure application programming interfaces (APIs) are extremely popular and, when configured poorly, huge datasets can be made accessible to unauthorized parties as well.

The other risk is sub-processing without full consent or due supervision. A large number of vendors are utilizing their own subcontractors to finish the services, and this has led to a messy web of data processors; this may cut across more than a single jurisdiction. This impact generates an ambiguity about the data storage/transfer location of personal data, which is concerning in the context of cross-border data transfer regulations, such as the GDPR (GDPR, Art. 28). Without good contractual and technical controls, organizations may unwittingly expose their users to vendors that are in high-risk areas with low privacy practices.

Jurisdictional risks also occur where vendors are based in or are accessing information in a country that lacks adequate privacy protection. Using the example of the disqualification of the EU-U.S. Privacy Shield in 2020, the data reveals not only the instability of the transatlantic system of data transfer but also the ability of one company to reconsider a contract with a vendor (Court of Justice of the European Union [CJEU], 2020). Failure to comply in this aspect may result in regulatory penalties and reputational devastation as customers become increasingly aware of where and how their data is stored and utilized.

The last weakness, which is the insecure integrations, is also an issue. Client systems can be connected to vendors via plug-in, single sign-on, or embedded scripts. Failure to design such integrations well means that attackers can use them as entry points into a bigger system to violate it. The latter threat was operational at the time of the 2021 Codecov attack, when criminals used an automated software updating mechanism of one of the suppliers to install an executable that compromised hundreds of downstream organizations (CISA, 2021).

This is because of the risks involved that ensure the relationship between vendors is more than a passive entity; they are active participants in privacy erosion. Protecting under contracts and providing basic technical inspection of the vendors to ensure that the data is processed carefully and securely are part of the existing proper control.

1.3 Case Studies of Vendor-Originated Breaches

There is strong evidence in the history of breaches being initiated by vendors that they are systematic in their vulnerability to vendor risk management. The most popular example is the Target breach that occurred in 2013, where attackers gained access to the company network by using a hacked account of its HVAC vendor. Not only did this attack cost the company more than 200 million dollars and remediation, but 40 million payment card records were stolen, and 70 million customer profiles were posted (CSIS, 2014). This episode raised the unbalanced flow of an isolated weak vendor relationship.

The other landmark case is the 2020 SolarWinds supply chain attack. This allowed attackers to install malicious code into the software update system of the vendor, creating a method through which they could compromise the system and infect a popular IT monitoring tool, Orion. This attack has affected thousands of companies, including government agencies and Fortune 500 companies, and demonstrates how vendor-created breaches can become the national news of the day and impact national security (CISA, 2020). The SolarWinds incident not only underscored the technical weaknesses of vendor ecosystems but also why it is difficult to identify advanced attacks in the supply chain.

The 2018 Facebook-Cambridge Analytica scandal taught us that in the context of API-based services, a supplier can abuse access to consumer data to perform unauthorized profiling and political targeting (Isaak and Hanna, 2018). Though it was not a classic breach, the event demonstrated how ineffective the contractual protection was and how challenging it is to enforce compliance on vendors regarding privacy matters.

In more recent times, cloud environment data breaches, including the Capital One breach of 2019, have demonstrated how vendor misconfigurations can result in huge data breaches. It was even called the consequence of a misconfigured AWS environment, but it was the first indicator of the so-called shared responsibility notion of cloud security, according to which a vendor and a customer have a responsibility that the data is safe (U.S. Department of Justice, 2020).

As demonstrated in these case studies, breaches by vendors are not one-off events but an ongoing phenomenon that exposes weaknesses in the internet service system. They also highlight how stronger regulatory and industry-based reactions to vendor risk are urgently required.

1.4 Regulatory Landscape

The regulatory frameworks like the GDPR, the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), and PCI DSS put major responsibilities on an organization to handle vendor risk. The data controllers must also make sure that processors adopt relevant technical and organizational safeguards, codified in the data processing agreements (DPA) under the GDPR (GDPR, Art. 28). Notably, vendor failure is frequently the responsibility of the controller, which can provide a strong incentive to exercise strict control over vendors.

In a comparable manner, the CCPA provides businesses with responsibilities that require them to make sure that service providers process consumer data in accordance with the statute. That the law between the business, service providers and third parties and that the business must also incorporate in the terms of the contract between vendors that no vendor who is not capable of signing a services agreement on the basis of the agreement may retain, use or disclose personal information beyond the restriction of the agreement (California Office of the Attorney General, 2020).

HIPAA also mandates covered entities in the healthcare industry to sign a business associate agreement (BAA) with vendors who access protected health information (PHI). BAAs likewise present privacy and security credentials of suppliers as well as breach notification credentials (HIPAA Journal, 2022). Complaints that have been made against failure to undertake compliant BAAs have resulted in substantial fines with enforcement measures frequently referring to ineffective vendor oversight as a source of violations.

The PCI DSS also applies to payment processors and merchants and specifies technical and operational standards that companies that have access to payment card data should meet. Vendor due diligence, periodic audit, certification is a compliance factor because compliance also assumes the awareness that the impact of a vendor with incompetent management on financial safety is deadly (PCI Security Standards Council, 2022).

The existence of these regulatory structures still has enforcement issues. In cases of breach, regulators are usually not able to see the intricate web of vendors to know who to hold accountable. In addition, vendor ecosystems are globally distributed, making compliance more difficult because they create conflicting legally binding requirements in different jurisdictions. These holes are an indicator that current regulation policies are inadequate to respond to the systemic risk of vendor data processing.

1.5 Empirical Vendor Assessment Study Proposal

In an effort to learn more about the practice of vendor risk management within the internet services industry, the proposed paper will present an empirical analysis of the 50 largest internet companies based on market capitalization. The research would be based on three aspects: (1) vendor risk evaluation procedures, (2) contractual protection, and (3) compliance reporting.

First, it was possible to perform vendor risk assessment procedures through the analysis of publicly offered security documentation, including vendor management policies and due diligence reports. They can be, but not necessarily include, access to the available vendor inventories in the organizations, periodic security audits, and mandate the vendors to prepare their own audit reports, i.e. SOC 2 or ISO 27001 certificate (Shared Assessments, 2022).

Second, the contractual protections might be evaluated through the analysis of standard contractual provisions in published data processing contracts. Among others, these considerations would include the breach notification requirements, sub-processing requirements, and cross-border data transfer requirements. These clauses would be compared between companies and would give an idea of what is standard in the industry and what is lacking in the management of the vendors.

Third, reviewing transparency reports and regulatory filings could be used to analyse

compliance disclosures. The disclosures usually tell the way companies organize their vendor relations, handle transfers across borders, and answer the questions of regulators. The study would provide a comparative framework to measure the maturity of vendor risk management in the internet sector by benchmarking practices in the 50 leading companies.

This type of empirical measurement would be a valuable addition to the academic and business field as it would measure how much the top internet businesses meet regulatory concepts and best practices. It might also inform policymakers who want to standardize vendor oversight requirements.

1.6 Technical and Organizational Mitigation

A mix of organizational and technical controls is necessary to reduce the privacy risks associated with vendors. Technically, it is important to realize that API design and implementation that helps avoid the unauthorized access to data. The issue with strong authentication and rate limiting, input validation control (OWASP, 2021) are problematic perhaps. Vendors also need to ensure that they are encrypting data when sending it over and when not using it, reducing the likelihood of data exposure during breaches.

Another important protective principle is the principle of least privilege. Access to data and systems should be provided to the vendors only in line with what is required to meet their contractual obligations. Just-in-time provisioning of access and role-based access controls (RBAC) can contribute to reducing the attack surface caused by the restriction of unnecessary privileges (ISO/IEC, 2017).

Vendor audits and certifications also play another important role. Independent assurance provisions, such as SOC 2 Type II and ISO/IEC 27001, that a vendor meets established standards of security are also available. These certifications should not merely be mandated by organizations, they should also be checked with their scope and relevance to the services they are relevant to. Constant monitoring systems (security scorecards, automated vulnerability scanners, etc.) can also provide periodic audit data on the current state of security of the vendor (ENISA, 2021).

On the organizational dimension, good governance means that vendor risk management must be incorporated into wider enterprise risk frameworks. This involves ensuring that there are clear lines of responsibility in terms of vendor management, having current vendor inventories, and training employees involved in vendor interaction. Breaches which are caused by vendors must also be explicitly considered in incident response plans, so that they can be detected, contained, and reported promptly.

These technical and organizational controls combined form a multi-layered defense against vendor breaches and improve the results of regulatory compliance. However, successful implementation is an investment and effort over the long-term, and that is why cross-functional interdependence and executive support are important.

1.7 Policy Recommendations

Since the privacy risks related to vendors are systemic in nature, organizational efforts have to be supplemented by regulatory and policy initiatives. One such suggestion is the creation of compulsory transparency portals through which organizations publicly reveal their current relationship with vendors. It would enable consumers and regulators to track how much data was leaked, and how many high-risk vendors there are in each industry (ENISA, 2021).

The other suggestion is the standardization of vendor risk scoring systems. Regulators and industry consortia could allow organizations to make better decisions when choosing vendors by creating a shared framework used to assess vendors in terms of security, privacy, and compliance metrics. The approach is similar to credit rating procedures in the financial industry, which provides a convenient measure of the reliability of the suppliers.

The economic incentive could also be reflective of the stricter penalties imposed on regulators

regarding insufficient supervision of the vendor; thus, the economic factors are directed to active risk management. Fines are now being used regularly because violations have already occurred, and this creates a reactive model of enforcement. Regulators can promote preventative action by imposing sanctions on not carrying out due diligence on vendors.

Lastly, international coordination is required to deal with cross-border aspects of vendor risk. It may be possible to align requirements internationally through the development of an international "Vendor Privacy Assurance Standard" to mitigate fragmentation in compliance and increase mutual resilience. This standard can be developed by multilateral institutions, on the basis of the available standards such as ISO/IEC 27036 on supplier relationship (ISO/IEC, 2017).

These policy suggestions represent the understanding that the risk posed by vendors is not just a technical problem, but a structural one that must be addressed through a coordinated effort by regulators, industry, and civil society.

II. CONCLUSION

The reliance on internet services on third-party vendors has transformed the digital economy and has also raised serious concerns about data privacy and data security. The weakest point of the privacy chain is often vendors, and breaches in vendor ecosystems have contributed to some of the largest historical events in recent history. The Target and SolarWinds breaches are case studies that demonstrate how the entire system of vendor relationships has been vulnerable, and regulatory frameworks like GDPR, CCPA, HIPAA, and PCI DSS are trying not perfectly but successfully, in some ways, to hold vendors responsible.

This paper has suggested that the vendor risks have not received adequate attention in the literature and policy debate, especially when compared with the direct attack on organizational systems. It suggested an empirical research on the vendor risk management processes by major internet companies, where cross-sector benchmarking may be possible. It also described technical, organizational, and policy interventions that would enhance vendor control.

Finally, internet privacy protection in the vendor age demands a shift in paradigm: companies should abandon their compliance-oriented strategies in favour of active, ongoing, and open vendor risk management. On the policy level, vendor ecosystems are inherently cross-border and hence require global coordination and standardization. Quantitative systems to evaluate vendor risks, the impact of new technologies like artificial intelligence in vendor oversight, and the socio-ethical aspects of outsourcing privacy control to a third party, all should be developed in future studies.

This paper is a contribution to a continuing discussion around the future of internet privacy by pre-empting the possibilities of data management by third-party vendors. The weakest link (i.e., vendors) should be strengthened in both the industry and the regulators.

REFERENCES

1. California Office of the Attorney General. (2020). *California Consumer Privacy Act (CCPA)*. https://oag.ca.gov/privacy/ccpa
2. Center for Strategic and International Studies. (2014). *The Target data breach*. https://www.csis.org/analysis/target-data-breach
3. Court of Justice of the European Union. (2020). *Schrems II judgment (C-311/18)*. https://curia.europa.eu
4. Cybersecurity and Infrastructure Security Agency. (2020). *AA20-352A: SolarWinds compromise*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a
5. Cybersecurity and Infrastructure Security Agency. (2021). *Alert: Compromise of Codecov*. https://www.cisa.gov
6. ENISA. (2021). *Good practices for supply chain cybersecurity*. https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
7. European Union. (2016). *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu

8. HIPAA Journal. (2022). *Business associate agreements*. https://www.hipaajournal.com/business-associate-agreements
9. IBM Security. (2023). *Cost of a data breach report 2023*. https://www.ibm.com/reports/data-breach
10. International Organization for Standardization/ International Electrotechnical Commission. (2017). *ISO/IEC 27036: Information security for supplier relationships*. ISO.
11. Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer, 51*(8), 56–59. https ://doi.org/10.1109/MC.2018.3191268
12. Kshetri, N. (2021). The economics of third-party cyber risks. *IT Professional, 23*(5), 45–51. https://doi.org/10.1109/MITP.2021.3103798
13. National Institute of Standards and Technology. (2022). *Cyber supply chain risk management practices for systems and organizations (SP 800-161 Rev. 1)*. NIST.
14. OWASP. (2021). *API security top 10*. https://owasp.org/API-Security
15. PCI Security Standards Council. (2022). *PCI DSS standards*. https://www.pcisecuritystandards.org
16. Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702. https://doi.org/10.1109/CloudCom.2010.66
17. Shared Assessments. (2022). *Vendor risk management maturity model (VRMMM)*. https://sharedassessments.org/store/vrmmm
18. U.S. Department of Justice. (2020). *Former Seattle technology company software engineer indicted for computer fraud and abuse, wire fraud, and access device fraud*. https://www.justice.gov