The Role of Data Fragmentation in Data Breaches

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Andrew Li

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kent A. Wayland, Department of Engineering and Society

Introduction

Detailed and comprehensive data collection has become pervasive in nearly every sector imaginable. Storing and retrieving useful insight from this data is the challenge of "big data" analysis that drives innovation in the digital economy, from artificial intelligence to the internet of things. A central task in maintaining such sheer quantity and diversity of data is organizing and unifying it. The volume and complexity of big data also introduces another problem: securing the data from cyberattacks and data breaches. When data is stored in very disparate systems, called data silos, and protected under inconsistent security standards, this causes data fragmentation. While data fragmentation generally describes the state of the data itself, it is impossible to understand without also investigating the often-corresponding fragmentation of entities that use, store, and protect that data. Data fragmentation can lead directly to severe security vulnerabilities, potentially putting sensitive or private information like health or financial data at risk (Gibbs et al., 2002). Additionally, data fragmentation can lead to inefficient utilization of information that can be used to rapidly detect and mitigate security breaches (ThreatConnect, n.d.). These concerns suggest that as the amount and diversity of data collected increase, data fragmentation can be a growing cybersecurity problem for companies.

This paper seeks to examine the role of data fragmentation in recent cybersecurity breaches of financial data and how data unification could have prevented or mitigated them. Multiple high-profile data breaches of financial companies, including Equifax in 2017 and Capital One in 2019, have affected millions of consumers and cost billions of dollars in settlements alone. These case studies can illuminate ways in which investments in data unification can—or can't—help reverse the surging quantity and severity of data breaches and protect consumers' most private information and assets in an increasingly digital world.

Background

Cyberattacks are estimated to cost the world $8 trillion in the year 2023 alone (Morgan, 2022). Meanwhile, the cybersecurity industry has reached $2 trillion in demand (Aiyer et al., 2022). Updating data infrastructure, including supporting data unification, will be a major segment of the burgeoning market. Data unification refers to the consolidation of different types of data, often stored in separate virtual or physical databases, into a consistent and accessible format. This may involve combining physical data stores into one centralized server or database, or just developing intermediary systems that can provide a single endpoint from which data of different types can be accessed in a uniform manner. As data collection and storage systems have matured in recent years, data unification has become both increasingly difficult and more important to enforce—systems that were designed incrementally and independently become resistant to unification. Redesigning or merging these systems can be expensive and complex—but maintaining fragmented databases is very expensive in itself (Mallikarjuna, 2020). Financial companies in particular have struggled with the costs of data fragmentation, especially as they have become popular targets for cyber attacks. Cyber attacks can be extremely costly with both legal penalties and damage to reputation, costs that are exceptionally high for financial companies (Mallikarjuna, 2020).

Data unification is a complex process that involves and is motivated by numerous institutions, social groups, and technologies. Actor Network Theory, as proposed by Bruno Latour (1992), can be used to clarify these relationships. Actor Network Theory argues that technology is shaped through the interactions between people, institutions, and the technology itself. In the case of data unification, these actors may generate data that others consume as well as consume data that other actors generate, creating a complex network where data of different

types and uses flow between nodes. Between the technical and non-technical actors, tasks and responsibilities can be delegated to technology or prescribed back to the humans, creating a web of information flow between people and computers. Within an institution or company, data may be collected, stored, and retrieved by both human associates and computers. Cybersecurity analysts monitor incoming data regarding cybersecurity-critical actions like logins and access tokens and analyze this information to create new data, like reports and alerts. Non-cyber associates may search for and retrieve information like internal risk reports, news articles, and blog posts. Automated systems process data to detect and remedy abnormalities and potential cyber attacks. Customers and users generate sensitive data and personal information that is stored by financial institutions. As data storage and computing services move to third-party cloud providers, these providers also enter the network of data stored and used by financial institutions. Finally, governments and agencies regulate the ways companies and employees can access and store data as well as the technical systems themselves. The ways in which these actors interact with each other are mediated by the successes and failures of existing technology. The complexity of these relationships is outlined below.

Data unification and fragmentation essentially regards data as an entity of its own—one that naturally tends towards increasing complexity and disorganization with its growing size. This intrinsic tendency can be governed and influenced by a variety of other actors. Thus, while data unification is fundamentally about the state of data itself and can occur independently of any other actors, this is rarely the case in practice. Data is only useful when processed and utilized by other entities, including individuals, organizations, and computing systems. Data unification is important to these other entities because it makes it cheaper and easier to extract value from the data. Thus, attempts to create data unification by human actors often seek to offload the burden

of organizing and maintaining useful data from humans to technology. Well-organized and unified data requires less investment from human analysts inside a company to help store, retrieve, and sort through data, instead relying on automated systems and infrastructure to perform this work independently. Thus, delegation of responsibilities to increase efficiency from specialization is one of the primary draws of data unification.

A key relationship driving the current state of data unification in many companies and organizations involves the accelerating movement of data to cloud storage and computing providers like Amazon Web Services (AWS) and Microsoft Azure. Cloud providers are a new but growing entity involved in the storage and access of data who increasingly take on the responsibility of protecting other organizations' data. This trend can also be described through a delegation of responsibilities; building and maintaining efficient data infrastructure is being increasingly delegated to specialized cloud providers, rather than being the responsibility of the company that owns the data. This delegation is a result of industry specialization to increase efficiency and ease of use (Tak et al., 2011). This phenomenon is key to understanding data unification and fragmentation in modern systems. On one hand, centralization around a few major cloud providers represents some level of data unification. With greater amounts of data from many different organizations held under consistent storage practices by a single third party, there is greater standardization in how data is stored and protected. However, it can also be argued that the addition of another third-party entity causes greater data fragmentation between different entities and opens more endpoints vulnerable to attack (Campos et al., 2016). The increasing prevalence of big data in tandem with cloud computing introduces more potentially insecure endpoints for data access, creating a more complicated data management environment

for cybersecurity. Reliance on cloud computing services was a key cause of Capital One's data breach in 2019.

Governments and regulators are also key actors motivating investment in data security. Regulations stipulate the balance of responsibilities in protecting data between companies and consumers. These regulations are often complex and differ between countries, further complicated by the fact that multiple jurisdictions may have authority over multinational companies. In general, the policies of the United States, European Union, and China all vary significantly in their level of responsibility delegated to the company (Palmieri III, 2019). There often is no universally optimal level of regulation; different methods have different advantages and disadvantages which can depend on the social norms in the country established by law and by custom (Martínez-Martínez, 2020). Regulation is highly dependent on the relationship between government, citizens, and companies. Citizens may pressure the government into enacting regulation to protect consumers. Private companies may resist the regulatory relationship with governments to reduce their liability for cyber attacks and data breaches (Peng, 2018), creating a potentially adversarial relationship between these two actors.

The interplay between these actors suggests that the current and future cybersecurity landscape is dependent on delicate power balances and relationships. Whether or not data unification becomes a common or useful cybersecurity tactic will depend on more than its innate utility; it will also depend on the actors that support or resist it.

Prior Literature

Several papers have investigated the causes and aftermath of Capital One's 2019 data breach. Neto et al. (2020) provide an in-depth analysis of the technical failures and governance issues that contributed to the breach. They find primarily that a number of violations of technical

controls suggested by the National Institute of Standards and Technology (NIST) severely limited Capital One's ability to both prevent and respond to the hack. Many of these controls can be implemented through or rely on data unification. The paper also alludes to complications in data governance caused by high employee turnover in the company's cyber department and inexperience with AWS's S3 cloud storage environment. There has also been some scholarship covering the consequences of the data breach, though mainly limited to monetary losses. Lu (2019) estimates the direct and indirect costs to Capital One as a result of the data breach and places the total costs at around $500 million prior to any costs to reputation, lost business, and regulatory backlash or punishment. Lu also recognizes the delicate balance between regulators and private companies, cautioning that excessive punishment could discourage innovation.

Similar research has been done on Equifax's 2017 breach. Luszcz (2018) investigated the technical failures that allowed hackers to access the personal information of 102 million customers. Among the failures was reliance on third-party software without vetting, creating more openings for vulnerabilities to proliferate. This point of failure is similar, but distinct from data fragmentation; it involves the underlying software and systems that utilize data, rather than the data itself. However, it can be compared to data fragmentation because of the similar roles in which delegation of responsibilities led to more entities involved in the handling of data, ultimately opening more cybersecurity vulnerabilities. In both the Capital One and the Equifax data breaches, a combination of human error and technical failures allowed the breach to happen. In this paper, I will determine the role of data fragmentation in both cases and the potential for data unification to have prevented or mitigated the event.

Methods

I will be performing case studies on the Capital One and Equifax data breaches using a variety of sources. Because both breaches were extremely high-profile events, there are numerous news articles, academic articles, and case studies covering the myriad causes and effects of the two breaches. To perform my own case studies and focus on the role data fragmentation played in the two events, I will identify areas where fragmentation of both data and the entities involved in the storage and access of data led to vulnerabilities that were exploited by the attackers. Case studies are selected as a primary method as it is a particularly effective research method for contemporary events to answer the critical questions of how and why they happened (Yin, 2009).

These cases will be viewed substantially through the lens of Actor Network Theory to understand how complex relationships between public and private entities may have contributed to vulnerabilities or, conversely, helped mitigate risks associated with data fragmentation. Critically, I will focus attention on the actors involved in the storage of data, including cloud providers, regulators, and the companies themselves.

Case Study: Capital One

Capital One's data breach was a failure not only of individual components, but also the linkages between the many entities involved in data storage and security. The primary relationship of interest in this case is that between Capital One and its cloud services provider Amazon Web Services (AWS). Capital One was an early adopter and serious investor in cloud technology. By many accounts, Capital One ran a "state-of-the-art cloud infrastructure" and was touted as an example to follow, including by AWS themselves (Amazon Web Services, 2020). At least since 2014, Capital One has been transitioning data it stored in its own data centers to AWS, a transition it completed in 2020, a year after the 2019 data breach. Thus, by the time of the

breach in 2019, Capital One had shuttered the vast majority of its own servers and had accumulated a heavy reliance on AWS to provide it with data storage and security services. This healthy business relationship was repeatedly featured in press releases by both AWS and Capital One. In July of 2019, however, the relationship took a sour turn.

The technical details of the Capital One data breach have been well documented, though not without debate. The attacker was ex-AWS employee Paige Thompson, who exploited a misconfigured firewall to gain access to cloud server instances owned by Capital One and transferred almost 30 GB of confidential data affecting 102 million of Capital One's credit card customers, leaking highly sensitive information like their social security numbers (Neto et al., 2020). The breach occurred in March 2019, but was not detected by Capital One until July 19, 2019, after an unaffiliated third-party notified Capital One through their Responsible Disclosure Program that Capital One's sensitive data had been published online (Capital One, 2022). In the immediate aftermath, companies, regulators, and the public scrambled to understand exactly how and why such an incident could have occurred and gone unnoticed for so long.

AWS was quick to absolve themselves of blame for the incident. AWS operated under a "shared-responsibility model," where AWS was responsible for the security of cloud infrastructure, such as the physical devices and software, but its clients were responsible for everything else in the cloud. In this case, because the breach exploited a misconfiguration in software rather than a bug, AWS claimed that the breach did not reflect any weaknesses with its product or mistakes on its part. Though AWS may characterize itself as an innocent third-party, this disguises the depth of the relationship and responsibility AWS holds towards Capital One as a steward of their data. Some analysts noted that Capital One did follow the best practices set forward by AWS (Khan et al., 2023). However, AWS's guidance was not sufficiently detailed

and allowed security vulnerabilities like the misconfigured firewall to slip through. On Capital One's part, their assumption that AWS's guidance was sufficient and lack of comprehensive knowledge about cloud security led to the misconfiguration in the first place. Both companies delegated more responsibility to the other party than the other party was prepared for, causing too much room for error.

Data fragmentation played a significant role in defining this deficient relationship. The partnership between Capital One and AWS split the responsibilities towards collecting, storing, and protecting the data between the two companies. Exactly how these responsibilities were split, however, was nebulous. Data fragmentation was a conscious choice for Capital One and an investment of years of time and money. In doing so, Capital One hoped to shed much of the burden of securing and maintaining data onto AWS. Instead, vagueness in the relationship led Capital One to mistakenly assume that security of the data was primarily the responsibility of AWS (Khan et al., 2023). As a result, many of these responsibilities in protecting data were lost, with neither party willing to shoulder them or explicitly delegate them to the other. This led to fragmentation of knowledge resulting in narrow specialization that allowed mistakes from both companies to propagate. Khan et al. (2023) argue that Capital One's misconfiguration of the firewall was, in itself, not enough to cause a significant cyber vulnerability. However, when combined with AWS's lack of understanding of the interaction between the firewall (the client's responsibility) and its infrastructure (AWS's responsibility), it becomes a critical flaw.

The major failures that led to this breach were ultimately human, rather than technical. However, it is still important to understand the interaction between human actors and technologies and how they contributed to the incident. While there were no inherent bugs in the firewall software Capital One deployed, the lack of experience of Capital One's associates with

configuring the technology caused a vulnerability. Capital One also had systems of automated network access logging that could have helped detect the breach sooner, if not prevent it as it was happening, but these logs were not checked frequently by analysts. Thus, most of the technical failures were ultimately failures in the relationship between humans and technology. In addition, data fragmentation also complicates relationships between machines, just as it did between Capital One and AWS. The distributed nature of the cloud means that many different servers store different types of data and must communicate with each other, another case of data fragmentation. AWS's infrastructure established a default assumption of trust between different server instances running on the cloud. Thus, if one instance is compromised, it would easily be able to extract information from other instances, just as was done in Capital One's breach.

Finally, Capital One's data security is governed by a number of federal and state agencies and laws. The Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and Office of the Comptroller of the Currency (OCC) are all federal agencies that oversee Capital One's operations. Federal laws including the Gramm-Leach-Bliley Act (GLB Act) and Fair and Accurate Credit Transactions Act of 2003 (FACT Act) also regulate Capital One's operations and duty to protect consumers' information. The multitude of these laws and agencies serve to ensure strict responsibilities towards ensuring cybersecurity. However, many of these regulations are especially strict or specific to financial institutions. Thus, AWS is not governed to the same degree, despite being just as important as Capital One in storing and securing sensitive data. The imbalance between the amount of oversight for companies like Capital One versus cloud service providers like AWS doesn't reflect the balance of responsibilities created by data fragmentation in the cloud. Cloud service providers will also heavily resist attempts to equalize the amount of oversight over their operations with the clients that it serves.

Case Study: Equifax

The Equifax data breach in 2017 predates Capital One's disaster by two years. Its many similarities to Capital One's breach in 2019 should have been a warning for financial institutions, whose reliance on third-party software and services proliferate vulnerable endpoints and invite human error. Though the Equifax breach does not involve fragmentation of the data itself, the same fragmentation of responsibilities between entities critically involved in the storage and access of data allowed the breach to happen. In many ways, the context behind Equifax's breach mirrors the relationship between Capital One and AWS in which a deficient relationship between two entities opened a crack in the data pipeline that attackers were able to exploit.

On July 29, 2017, Equifax discovered and patched a vulnerability that allowed hackers to access millions of customers' names, birth dates, social security numbers, and even driver's license numbers (Equifax, 2017). By that time, hackers had already been extracting information from Equifax's servers for over two months and ultimately involved more than 143 million people (Kolevski et al., 2021). Equifax would not publicly release information about the incident until September of 2017.

The direct cause of the data breach was a vulnerability in the open-source web server software called Apache. The Apache Software Foundation discovered the bug in March 2017 and issued a patch to fix the update, a patch that Equifax did not apply until after they discovered the data breach (Kolevski et al., 2021). Unlike Capital One, Equifax was not fully invested in the cloud at the time of the data breach, putting all culpability on Equifax for not keeping their infrastructure up-to-date and secure. However, like Capital One, Equifax's breach fundamentally originated from a disconnect between a third-party vendor and Equifax itself. Like many companies, Equifax delegated the responsibility of developing and maintaining web server

software to a third-party. However, a lack of understanding of the third-party software led to an outstanding vulnerability and ultimately to the data breach. While this is not directly a case of data fragmentation like in Capital One's case, it is a fragmentation of knowledge and siloing of expertise. Thus, the unique set of relationships between Equifax, third parties, and technology itself mirror those of Capital One.

Apache is open source software, meaning the source code is freely and publicly available to anyone, and anyone may use the software for personal or commercial purposes without paying the writers of the software or the Apache Software Foundation. In return, the Apache Software Foundation claims no liability or responsibility for the use or misuse of the software. Thus, there is no explicit business relationship between companies that use the Apache software and the Apache Software Foundation. Rather, the lack of responsibility on behalf of the Apache Software Foundation is governed by the open source license contained in the Apache source code. The onus is on the user of the software to stay informed about vulnerabilities in the software and react accordingly. Unlike AWS, the Apache Software Foundation has no explicit responsibility to aid or guide its clients in ensuring their software is configured properly. This may have been one cause of Equifax's failure; their apathy or ignorance about the security vulnerability in their code was aided by the fact that the Apache Software Foundation had no responsibility to proactively notify and fix the error for Equifax's servers. The deficient sharing of responsibility between Equifax and Apache Software Foundation was fully intentional and designed to absolve Apache of culpability. In return, Equifax can utilize Apache's product free of charge.

Despite the *de jure* indifference of Apache to its users, there is an implicit *de facto* responsibility of the software and its writers to serve users of Apache responsibly. Unfortunately, this unenforced relationship does break down sometimes, like it did for Equifax. The gap

between the software writers and users is dangerous for Apache and all open source software (Luszcz, 2018). While the freedom associated with permissive licenses like the Apache license is attractive to many companies, there is a commensurate cost to this freedom. This tradeoff should be considered seriously, and similar tradeoffs exist for companies considering a transition to cloud computing as well.

Conclusion

The fragmentation of resources—both data and software—driven by increasing industry specialization and outsourcing feature prominently in the data breaches of Equifax and Capital One. This data fragmentation is a fact; companies are eschewing owning and running their own data centers in favor of relying on cloud service providers. Equifax is no longer an exception to this trend; following their 2017 data breach, they have begun a full transition to the cloud hosted by AWS and Google Cloud (Amazon Web Services, 2022; Google Cloud, 2021). Capital One hasn't slowed their transition either and completely shifted to the cloud in 2020. This trend, often promoted as an investment in security, is not inherently a bad thing. Besides the concerns about data fragmentation outlined above, there can be valid and compelling benefits of fragmentation (Ciriani et al., 2010). In particular, specialization that is enabled by fragmentation can allow companies to focus on a narrow set of responsibilities, which can benefit companies that don't have the resources or scale to design their own secure systems from scratch. Rather than try to reverse years of effort investing in the cloud, companies and governments should look forward and mitigate the new vulnerabilities associated with fragmentation.

Governance and regulations matter for cybersecurity. Gaglione (2019) argues that these data breaches should be seen as opportunities to improve regulation. It is concerning that rather than learning from these breaches, companies have been repeating the mistakes of the past and

suffering from incidents that reprise each other—not least in the case of Equifax and Capital One. With the development of increasingly complex and decentralized relationships in the provision of financial services, regulators and companies need to clearly define responsibilities and liability between actors. Though reshaping the interactions between these actors will incur friction from entrenched relationships and a general reluctance to accept increased potential liability, they are a necessary change to face increasing fragmentation and cybersecurity risk.

References

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022, October 27). *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Amazon Web Services. (2020). *Capital One Completes Migration from Data Centers to AWS, Becomes First US Bank to Announce Going All In on the Cloud*. Amazon Web Services. https://aws.amazon.com/solutions/case-studies/capital-one-all-in-on-aws/

Amazon Web Services. (2022). *Using the Cloud to Become a Security Leader | AWS Executive Insights*. Amazon Web Services, Inc. https://aws.amazon.com/executive-insights/customers/equifax-ceo-mark-begor/

Campos, J., Sharma, P., Jantunen, E., Baglee, D., & Fumagalli, L. (2016). The Challenges of Cybersecurity Frameworks to Protect Data Required for the Development of Advanced Maintenance. *Procedia CIRP*, *47*, 222–227. https://doi.org/10.1016/j.procir.2016.03.059

Capital One. (2022, April 22). *Information on the Capital One cyber incident*. Capital One. https://www.capitalone.com/digital/facts2019/

Ciriani, V., Vimercati, S. D. C. D., Foresti, S., Jajodia, S., Paraboschi, S., & Samarati, P. (2010). Combining fragmentation and encryption to protect privacy in data storage. *ACM Transactions on Information and System Security*, *13*(3), 1–33. https://doi.org/10.1145/1805974.1805978

Equifax. (2017). *Consumer Notice*. 2017 Cybersecurity Incident & Consumer Information. https://www.equifaxsecurity2017.com/consumer-notice/

Gaglione, G. (2019). The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America. *Buffalo Law Review*, *67*(4).

Gibbs, M. R., Shanks, G., & Lederman, R. (2002). Data Quality, Database Fragmentation and Information Privacy. *Surveillance & Society*, *3*(1). https://doi.org/10.24908/ss.v3i1.3319

Google Cloud. (2021). *Equifax Case Study*. Google Cloud. https://cloud.google.com/customers/equifax

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2023). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. *ACM Transactions on Privacy and Security*, *26*(1), 1–29. https://doi.org/10.1145/3546068

Kolevski, D., Michael, K., Abbas, R., & Freeman, M. (2021). Cloud computing data breaches: A review of U.S. regulation and data breach notification literature. *2021 IEEE International Symposium on Technology and Society (ISTAS)*, 1–7. https://doi.org/10.1109/ISTAS52410.2021.9629173

Latour, B. (1992). Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts. In *Shaping Technology / Building Society: Studies in Sociotechnical Change*. MIT Press.

Lu, J. (2019). *Assessing The Cost, Legal Fallout Of Capital One Data Breach* [SSRN Scholarly Paper]. https://doi.org/10.2139/ssrn.3438816

Luszcz, J. (2018). Apache Struts 2: how technical and development gaps caused the Equifax Breach. *Network Security*, *2018*(1), 5–8. https://doi.org/10.1016/S1353-4858(18)30005-9

Mallikarjuna, J. (2020). *The Relevance of Data Unification*. SG Analytics.

Martínez-Martínez, D.-F. (2018). Unification of personal data protection in the European Union: Challenges and implications. *El Profesional de La Información*, *27*(1), 185. https://doi.org/10.3145/epi.2018.ene.17

Morgan, S. (2022). *2022 Official Cybercrime Report*. Cybersecurity Ventures. https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

Neto, N. N., Madnick, S., Moraes G. de Paula, A., & Malara Borges, N. (2020). *A Case Study of the Capital One Data Breach* [SSRN Scholarly Paper]. https://doi.org/10.2139/ssrn.3570138

Neto, N. N., Madnick, S., Moraes G. de Paula, A., & Malara Borges, N. (2021). A Case Study of the Capital One Data Breach: Why Didn't Compliance Requirements Help Prevent It? *Journal of Information System Security*, *7*(1).

Palmieri III, N. F. (2019). Data Protection in an Increasingly Globalized World. *Indiana Law Journal*, *94*(1), 297–329. https://www.repository.law.indiana.edu/ilj/vol94/iss1/7

Peng, S. (2018). "Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime. *Cornell International Law Journal*, *51*(2), 446–470. https://scholarship.law.cornell.edu/cilj/vol51/iss2/4

Tak, B. C., Urgaonkar, B., & Sivasubramaniam, A. (2011, June). To Move or Not to Move: The Economics of Cloud Computing. *3rd USENIX Workshop on Hot Topics in Cloud Computing*. USENIX.

Teen, M. Y., & Tan, R. (2020). *Capital One: A Breach in the Cloud* [Corporate Governance Case Studies: Financial Services Edition]. CPA Australia. https://governanceforstakeholders.com/wp-content/uploads/2020/07/cg-fs-casestudies.pdf#page=153

ThreatConnect. (n.d.). *Fragmentation: The "Silent Killer" of Your Security Management Program*. ThreatConnect.

https://threatconnect.com/wp-content/uploads/ThreatConnect-whitepaper-fragmentation.pdf

Yin, R. K. (2009). *Case Study Research: Design and Methods* (Fourth edition).