JISSec
Journal of Information System Security

A CASE STUDY OF THE CAPITAL ONE DATA BREACH: WHY DIDN'T COMPLIANCE REQUIREMENTS HELP PREVENT IT?

Journal of Information System Security is a publication of the Information Institute. The JISSec mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

ISSN: 1551-0123
Volume 17, Issue 1

www.jissec.org

Nelson Novaes Neto[1], Stuart Madnick[2], Anchises Moraes G. de Paula[3], and Natasha Malara Borges[3].

[1] MIT Sloan School of Management, USA, [2] MIT Sloan School of Management and MIT School of Engineering, USA, [3] C6 Bank, Brazil

Abstract

In an increasingly regulated world, with companies prioritizing a big part of their budget for cyber security protections, why have all of these protection initiatives and compliance standards not been enough to anticipate the leak of billions of data points in recent years? New data protection and privacy laws and recent cyber security regulations demonstrate a strong trend and growing concern on protecting businesses and customers from cyberattacks. The purpose of this research was to understand if compliance requirements would help prevent a major data breach incident at Capital One, one of the largest financial institutions in the U.S. This case study aims to understand the technical modus operandi of the cyberattack, map out exploited vulnerabilities, and identify the related compliance requirements that existed, based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, an agnostic security framework widely adopted by the global industry to provide cyber threat mitigation guidelines. The results of this research and the case study will help government entities, regulatory agencies, and companies to improve their cyber security controls for the protection of organizations and individuals.

Keywords: Data Breach, Cybersecurity, Cyberattack, Data Protection, Privacy Laws, Technology.

JISSec
Journal of Information System Security

Introduction

Technology is one of the main enablers of digital transformation worldwide. The use of information technologies increases each year and directly impact changes in consumer behavior, development of new business models, and creation of new relationships supported by all the information underlying these interactions.

Based on numerous cyberattacks reported by the media (Kammel, Pogkas, and al., 2019), organizations are facing an increasing urgency to understand the threats that can expose their data as well as the need to understand and to comply with the emerging regulations and laws involving data protection within their business.

As privacy has emerged as a priority concern, governments are constantly planning and approving new regulations that companies need to comply with to protect consumer information and privacy (Gesser, Forester, et al., 2019), while the regulatory authorities throughout the world are seeking to improve transparency and responsibility involving data breach. Regulatory agencies are imposing stricter rules, e.g. they are demanding disclosure of data breaches, imposing bigger penalties for violating privacy laws, as well as using regulations to promote public policies to protect information and consumers.

Despite all efforts made by regulatory agencies and organizations to establish investments and proper protection of their operations and information (Dimon, 2018), cases of data leak in large institutions are becoming more frequent and involving higher volumes of data. According to our research, the number of data records breached increased from 4.3 billion in 2018 to over 11.5 billion in 2019 (Neto, Madnick, de Paula, and Borges, 2021).

There are a number of frameworks, standards and best practices in the industry to help organizations meet their regulatory obligations and establish robust security programs. For the purpose of this research, an agnostic security framework was adopted to help mapping industry's best practices for mitigatory security controls. The Cybersecurity Framework (CSF) version 1.1, published by the U.S. National Institute of Standards and Technology (NIST), represents a well-know and widely accepted framework organizing and expressing compliance and mitigatory controls. [1]

1 NIST published a Cybersecurity Framework in 2014 that consists of standards, guidelines and best practices to manage cybersecurity risks and to protect critical infrastructure from cyberattacks, represented by a large set of technical and/or management activities (known as "subcategories") organized in five core domains (the so-called Functions: Identify, Protect, Detect, Respond, and Recover). NIST Cybersecurity Framework is widely adopted by organizations from different industries and geographies, including financial institutions in the U.S., to guide the information security strategy and it is formally recommended by various governance agencies, such as the Federal Financial Institutions Examination Council (FFIEC).

Moreover, an extensive literature exists to help mapping NIST CSF to the majority of most relevant cyber security standards and regulations.

Since NIST CSF is widely adopted by U.S. financial institutions, it will be considered as a basis for understanding the set of security controls that should be in place to help mitigating a cyberattack. Ultimately, while NIST CSF refrains from labelling its use as one of a strict compliance-orientation, adherence to the framework's guidelines requires a company to own a compliance culture, largely within the open-ended and risk-based handling of adapting the framework for individual organizations.

For the purpose of this paper, we selected U.S. bank Capital One as the object of study due to the severity of the security incident they faced in July 2019 that impacted an estimated 106 million customers (Capital One - 1, 2019).

The main research goals and questions of this study are:

- Analyze the Capital One data breach incident;
- Discuss if compliance controls were sufficient to anticipate and to prevent the Capital One data breach.

The result of this study will be valuable to support executives, governments, regulators, companies and specialists in the technical understanding of what principles, techniques, and procedures are needed for the evolution of the normative standards and company's management in order to reduce the number of data breach cases and security incidents.

Related Articles

The academic literature related to the objective of this research is very limited, since the Capital One data breach incident was very recent, and few cyber security incidents have enough public information available for a detailed technical analysis. Salane (Salane, 2009) describes the great difficulty associated with studies regarding data leaks: *"Unfortunately, the secrecy that typically surrounds a data breach makes answers hard to find. (…) In fact, the details surrounding a breach may not be available for years since large scale breaches usually result in various legal actions. The parties involved typically have no interest in disclosing any more information than the law requires."*

While the use by private sector is voluntary, NIST CSF is mandatory for all United States federal agencies as of 2017, and as consequence, it also applies to organizations and subcontractors that are prompted to work with U.S. federal agencies. While NIST CSF in itself is not a regulatory instrument and it was developed as a general cybersecurity framework, its subsequent mandatory nature for all U.S. federal agencies have elevated its status.

Due to the high relevance of Capital One data leak to US consumers, an extensive news coverage exists, which provided valuable help for this paper. The most extensive report, the indictment at US District Court at Seattle, is available online, including the detailed FBI investigation report (US District Court at Seattle, 2019). Such court records are a rich resource for research, since it provides detailed investigation on the cause of the incidents, including details of the modus operandi of the attack and, eventually, existing compliance controls. In addition, many cyber security consulting companies published blog posts with technical analysis of the incident, such as CloudSploit (CloudSploit, 2019). American journalist Brian Krebs also covered the story, providing some additional technical details about the incident (Krebs, 2019). With such amount of information available, it was possible to identify the technical details that describe how the cyberattack took place.

Procedures, criteria and analysis considerations

One of the greatest difficulties for understanding the modus operandi of the successful attacks that compromised billions of records in the recent years is obtaining detailed information on the attack's vectors, threats, exploited vulnerabilities, technical details of the technological environments and what were the TTPs (Tactics, Techniques, and Procedures) used to compromise the data. Unfortunately, many companies do not disclose the details of the incidents while some will only report and notify clients that their data was compromised, either to comply with regulations, e.g., EU General Data Protection Regulation (GDPR), or involuntarily due to disclosure of details of the incidents by hackers, researchers, the media, or other ways.

To properly understand the chain of events that led to the incident related to this case study, the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework was adopted to help assessing the TTPs behind each technical step that played a significant role in the success of the cyberattack analyzed.[2] Different from NIST Framework, MITRE ATT&CK is not a compliance and control framework; instead, it is a framework for mapping each one of a list of well-known cyberattack techniques, describing their TTPs and related mitigation and detection recommendations. As a result, it helped to determine the security controls that failed or should have been in place to mitigate the attack.

[2] An extensive ATT&CK description is available online at https://attack.mitre.org.

Our background research comprised:

1. A detailed analysis to identify and understand the technical modus operandi of the attack, as well as what conditions allowed a breach and related regulations;
2. Technical assessment of the main regulations related to the case study;
3. Answer to the question: Why didn't compliance requirements help prevent the data breach?
4. Recommendations for regulatory agencies, organizations, and entities.

Criteria for regulations analysis (Compliance)

The regulatory scenario is large and permeates several segments across various industries and geographies. When it comes to cybersecurity, there are strong regulations in different industries, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) for healthcare and the Sarbanes Oxley (SOX) and Payment Card Industry – Data Security Standard (PCI-DSS) for the financial industry. In addition, there are numerous legislations applicable to a particular country or region such as the California Consumer Privacy Act (CCPA), the General Data Protection Regulation (GDPR) in the European Union, the Brazilian General Personal Data Protection Act (LGPD) and an extensive number of laws in other countries.

Due to the diversity of cyber security regulations, legislations and compliance frameworks, it is more productive to select an agnostic, industry-neutral framework that is widely adopted by the industry and offers a strong and comprehensive mitigation guideline to cyber threats. Thus, the NIST Cybersecurity Framework (CSF), version 1.1, was selected.

The NIST CSF provides a common language for understanding, managing, and expressing cybersecurity risks and delivers a large set of both technical and management mitigatory activities to reduce cybersecurity risks. Different types of entities use the NIST CSF to provide a flexible and risk-based implementation of security controls that can be used with a broad array of cybersecurity risk management processes.

Criteria for Case Study Selection

The majority of the public stories about data leak incidents in 2018 and 2019 did not cover technical details about the incident, nor had enough information about compliance information on the targeted organization. For instance, usually press reports only cover superficial information about the type and extent of the incident.

A rare exception was the data breach of U.S. bank Capital One in 2019. The incident, which was the result of an unauthorized access to their cloud-based servers hosted at Amazon Web Service (AWS), took place on March 22 and 23, 2019. However, the company only detected the attack on July 19, four months after the data exfiltration, resulting in a data breach that affected 106 million customers (100 million in the U.S. and 6 million in Canada) (Capital One - 1, 2019). Capital One's shares closed down 5.9% after the bank disclosed the data breach, losing a total of 15% over the next two weeks (Henry, Capital One Shares Fall Nearly 6% After Breach, 2019). A class action lawsuit seeking unspecified damages was filed just days after the breach became public (Dellinger, 2019).

The Capital One case stood out in this research because there is a lot of public information available on the case, including the FBI investigation report (US District Court at Seattle, 2019). In addition, the incident has a strong representation in the cloud computing industry, since Capital One was recognized as a leading use case of cloud computing adoption in the financial services industry. Based on the abundance of details about the incident, as well as the relevant impact to U.S. consumers, the Capital One incident was chosen for the Case Study. In addition, Capital One meets the research criteria since it is an organization working in a highly regulated industry, and the company abides to existing regulations.

Case Study: Capital One

Capital One adoption of technology

Capital One is the fifth largest consumer bank in the U.S. and eighth largest bank overall (Capital One, 2020), with approximately 50 thousand employees and 28 billion US dollars in revenue in 2018 (Capital One - 2, 2019).

Capital One works in a highly regulated industry, and the company is subject to regulations, such as *"the New York Stock Exchange ("NYSE") corporate governance rules, the Sarbanes-Oxley Act of 2002, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, and the implementing rules of the Securities and Exchange Commission (SEC) thereunder (or any other legal or regulatory requirements, as applicable)"* (Capital One - 3, 2019). In addition, Capital One is a member of the Financial Services Sector Coordinating Council (FSSCC), the organization responsible for proposing improvements in the Cybersecurity framework, which was selected for this research. We also found job advertisements at Capital One's Career website available online in December 2019 where Capital One was looking for Managers with experience in the NIST framework, which demonstrates that the company had adopted it (Capital One - 4, 2019) (Capital One - 5, 2019) (Capital One - 6, 2019).

Capital One is an organization that values the use of technology and it is a leading U.S. bank in terms of early adoption of cloud computing technologies. According to its 2018 annual investor report (Capital One - 2, 2019), Capital One claims that *"We're Building a Technology Company that Does Banking."* Within this mindset, the company points out that *"Today, 85% of our technology workforce are engineers. Capital One has embraced advanced technology strategies and modern data environments. We have adopted agile management practices, (…). We harness highly flexible APIs and use microservices to deliver and deploy software."* In addition, the report highlights that *"The vast majority of our operating and customer-facing applications operate in the cloud (…)."*

Capital One was one of the first banks in the world to invest in migrating their on-premises datacenters to a cloud computing environment, which played a key role in the data leak incident in 2019. Indeed, Amazon lists Capital One as a renowned case study (AWS, 2018). The company has been expanding the use of cloud computing for key financial services since 2014 to reduce its datacenter footprint. From 8 physical datacenters in 2014, all were decommissioned before 2021 (du Preez, 2021), moving all Capital One's applications and systems to the cloud computing infrastructure hosted at AWS. In addition, Capital One worked closely with AWS to develop a security model to enable operating more securely in the cloud. According to George Brady, executive vice president at Capital One, *"Before we moved a single workload, we engaged groups from across the company to build a risk framework for the cloud that met the same high bar for security and compliance that we meet in our on-premises environments."* (AWS, 2018).

Technical Assessment of the Capital One Incident

Despite the strong investments on IT infrastructure, in July 2019 Capital One disclosed that the company had sensitive customer data assessed by an external individual. According to Capital One's public report released on July 29, 2019 (Capital One - 1, 2019), *"On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information from Capital One credit card customers and individuals (…)."* The company claimed that compromised data corresponded to *"personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, e-mail addresses, dates of birth, and self-reported income."* The unauthorized access *"affected approximately 100 million individuals in the United States and approximately 6 million in Canada"*.

According to the FAQ published by Capital One (Capital One - 7, 2019), the company discovered the incident thanks to an e-mail message sent to their Responsible Disclosure Program on July 17, 2019, instead of being discovered by regular cybersecurity operations. The FBI complaint filed with the Seattle court (US District Court at Seattle, 2019) displays an e-mail from an outsider informing that data from Capital One's customers was available on a GitHub page (see screenshot extracted from FBI report).


Capital One

Responsible Disclosure (Shared) <responsiblediscloure@capitalone.com>

[External Sender] Leaked s3 data

[redacted] Wed, Jul 17, 2019 at 1:25 AM

To: "responsiblediscloure@capitalone.com" <responsiblediscloure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

Figure 1: E-mail reporting supposed leaked data belonging to Capital One

Capital One reported via a press release (PRNewswire, 2019) that some of the stolen data had been encrypted but the company did not provide any detail on how it was possible for the attacker to access the information: *"We encrypt our data as a standard. Due to the particular circumstances of this incident, the unauthorized access also enabled the decrypting of data."*

According to the FBI investigations, *"Federal agents have arrested a Seattle woman named Paige A. Thompson for hacking into cloud computing servers rented by Capital One, (…)."* The press soon realized that, according to her LinkedIn profile, Thompson worked previously at Amazon (Sandler, 2019) from 2015 to 2016. In addition, the U.S. Department of Justice accused Paige Thompson of stealing additional data from more than 30 companies, including an unnamed state agency, a telecommunications conglomerate, and a public research university (U.S. Attorney's Office, 2019). Thompson created a scanning software tool that allowed her to identify cloud computing servers with misconfigured firewalls, allowing the execution of commands from outside to penetrate and to access these servers.

The complaint filed with the Seattle court indicates that FBI investigations identified a script hosted on a GitHub repository that was deployed to access the Capital One data stored in their cloud servers, compromising three commands allowing the unauthorized access: the first command was used *"to obtain security credentials (…)*

that, in turn, enabled access to Capital One's folders", a second one *"to list the names of folders or buckets of data in Capital One's storage space"*, and a third command *"to copy data from these folders or buckets (…)."* In addition, *"A firewall misconfiguration allowed commands to reach and to be executed at Capital One's server."* FBI adds that Capital One checked its computer logs to confirm that the commands was in fact executed.

After analyzing the records of the Seattle Court, cloud security company CloudSploit published an analysis of the incident in its corporate blog (CloudSploit, 2019), describing that the access to the vulnerable server was achieved by a Server-Side Request Forgery (SSRF) attack[3] that bypassed the misconfigured Web Application Firewall (WAF) solution deployed by Capital One: *"An SSRF attack tricks a server into executing commands on behalf of a remote user, enabling the user to treat the server as a proxy for his or her requests and get access to non-public endpoints"*. Reports and articles in the industry also assumed that Ms. Paige Thompson performed a SSRF attack at Capital One's AWS servers. American journalist Brian Krebs also concluded that the attacker ran an SSRF attack that exploited a misconfigured WAF tool. Krebs added (Krebs, 2019): *"Known as "ModSecurity,"[4] this WAF is deployed along with the open-source Apache Web server to provide protections against several classes of vulnerabilities that attackers most commonly use to compromise the security of Web-based applications."*

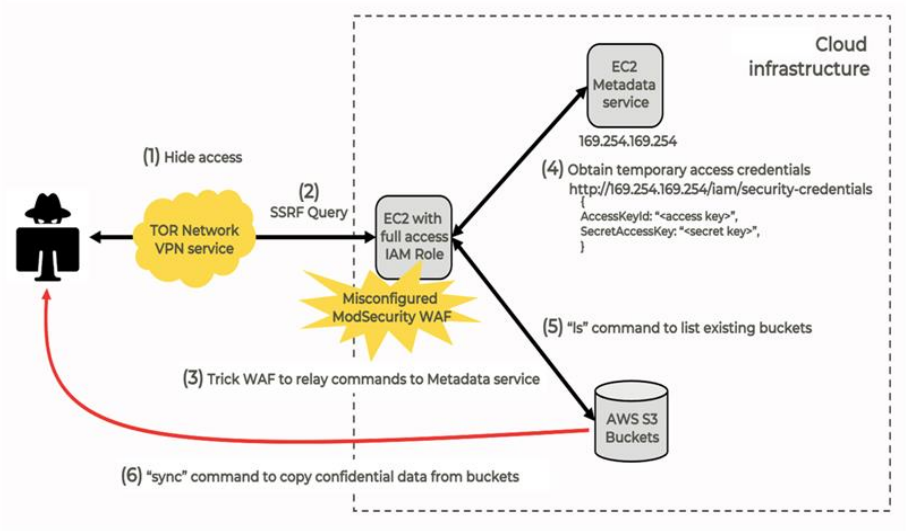


Figure 2: Capital One attack

[3] Server-Side Request Forgery, (SSRF) is a software vulnerability class where servers can be tricked into connecting to another server it did not intend to, then making a request that's under the attacker's control (Abma, 2017), enabling an attacker to send crafted requests from the back-end server of a vulnerable web application (O'Donnell, 2019).

[4] Modsecurity is a popular open-source, host-based Web Application Firewall (WAF) solution.

Figure 2 provides a summary of how the attacker got access to the vulnerable server and executed the commands that led to the access to sensitive data stored in AWS S3 buckets[5].

The reports from FBI, CloudSploit and Mr. Brian Krebs made it possible to figure out the steps taken during the cyberattack, between March 22nd and April 21st, 2019, as presented in Figure 2 and described below:

1. The FBI and Capital One identified several accesses through anonymizing services such as TOR Network and VPN service provider iPredator, both used to hide the source IP address of the malicious accesses;
2. The SSRF attack allowed the criminal to trick the server into executing commands as a remote user, giving the attacker access to a private server;
3. The WAF misconfiguration allowed the intruder to trick the host-based Modsecurity web application firewall (WAF) into relaying commands to a default back-end resource on the AWS platform, known as the metadata service with temporary credentials for such environment (accessed through the URL http://169.254.169.254);
4. By combining the SSRF attack and the WAF misconfiguration, the attacker accessed the URL "http://169.254.169.254/iam/security-credentials" to obtain the AccessKeyId and SecretAccessKey privileged access keys from a role described in the FBI indictment as "*****-WAF-Role" (name was partially redacted by the FBI). The resulting temporary credentials allowed the criminal to run commands in AWS environment via API, CLI or SDK;
5. By using the stolen credentials, the attacker ran the "ls" command6 multiple times, which returned a complete list of all AWS S3 Buckets of the compromised Capital One account ("$ aws s3 ls");
6. Lastly, on March 22nd, 2019, the intruder ran the AWS "sync" command7 to copy nearly 30 GB of Capital One credit application data from these buckets to the local machine of the attacker ("$ aws s3 sync s3://bucketone."). This command gave the attacker access to more than 700 buckets, according to the FBI report.

[5] Amazon launched its Simple Storage Service (S3) in 2006 as a platform for data storage. Since then, S3 buckets have become one of the most commonly used cloud storage tools.
[6] "ls" is a command available at AWS's command-line interface that list objects and common prefixes under a prefix or all Simple Storage Service (S3) buckets.
[7] "sync" is a command available at AWS's command-line interface that recursively copies new and updated files from the source directory to a specific destination.

According to the complaint filed by the FBI, Capital One claimed that some of the information stored in the stolen files were protected by tokenizing or encrypting them (as Social Security Numbers), while other information including customers' names, addresses, date of birth and credit history was kept unprotected in clear text. However, in the incident disclosure statement, Capital One explicitly states that "the unauthorized access also enabled the decrypting of data." Therefore, the attacker managed to access even the data that was previously encrypted.

The steps described above can be mapped within the specific stages of the MITRE ATT&CK framework, as shown in Table 1 below. The ATT&CK framework also describes, for each known attack technique, the main recommendations for mitigation and detection controls that can be used whenever applicable. Therefore, MITRE ATT&CK framework provides a valuable help by identifying the faulty security controls that made the incident possible.

Stage	Step of the attack	ATT&CK
Command and Control	Step 1: Use TOR to hide access	T1188 - Multi-hop Proxy (MITRE, 2018)
Initial Access	Step 2: Use SSRF attack to run commands	T1190 - Exploit Public-Facing Application (MITRE, 2018)
Initial Access	Step 3: Exploit WAF misconfiguration to relay the commands to the AWS metadata service	Classification unavailable[8]
Initial Access	Step 4: Obtain access credentials (AccessKeyId and SecretAccessKey)	T1078 - Valid Accounts (MITRE, 2017)
Execution	Step 5 and 6: Run commands in the AWS command line interface (CLI)	T1059 - Command-Line Interface (MITRE, 2017)
Discovery	Step 5: Run commands to list the AWS S3 Buckets	T1007 - System Service Discovery (MITRE, 2017)
Exfiltration	Step 6: Use the sync command to copy the AWS bucket data to a local machine	T1048 - Exfiltration Over Alternative Protocol (MITRE, 2017)

Table 1: List of attack steps mapped to MITRE ATT&CK Framework

[8] MITRE ATT&CK has no specific category that represents the exploitation of a misconfigured cyber security control or tool.

Technical Assessment of the Regulations Applied to Capital One

To support this article and the selection of the NIST Cybersecurity Framework both regulatory aspects required by US government agencies and the best practices were studied.

Based on the analysis regarding the regulatory framework applied to Capital One, it was possible to understand the security guidelines provided by Federal Financial Institutions Examination Council (FFIEC), which is a mandatory cybersecurity-related banking regulation in the United States (Miller, 2015). The FFIEC assumes that the COSO structure (ISACA Control Objectives for Enterprise IT Governance) is the framework elected to support the information security strategy of the financial institutions, associated with the NIST Cybersecurity Framework.

According to information made available by Capital One in their investors' webpage (Capital One - 8, 2019), in the scope of Corporate Governance Capital One states that *"The Board of Directors has adopted Corporate Governance Guidelines to formalize the Board's governance practices and to provide its view of effective governance. (…) The Board reviews and periodically updates these principles and practices as legal, regulatory, and best practice developments evolve."*

Capital One follows governance practices regarding cyber security and applied normative frameworks. Indeed, to map the best-practices that Capital One's professionals follow, we investigated the job descriptions for Capital One's open positions (Capital One, n.d.) to confirm that the abilities and knowledge related to the NIST Cybersecurity Framework are required for those positions.

While there are numerous regulatory requirements and global standards and best practices covering cybersecurity, some of them apply to Capital One, this research focused on NIST framework since it provides a common organizing structure for multiple regulatory requirements to cybersecurity.

Assessment of Technical Controls versus Normative Standards Applied to the Capital One Incident

This assessment focused on management and technical controls that could anticipate the Capital One data leak incident, according to the incident details published in the U.S. Department of Justice report (US District Court at Seattle, 2019), as described in session 0. In addition, the MITRE ATT&CK framework was used to help understand the attack progress and to infer the mitigatory controls based on the NIST CSF subcategories.

For each step performed by the attacker, Table 2 lists the related technical controls and NIST CSF subcategories to mitigate the attack, compromising a total of 61 potential NIST subcategories representing security controls that could have been in place to help prevent the cyberattack to Capital One in a given step of the attack.

Since some NIST CSF subcategories apply to more than one attack stage, the number of unique subcategories presented in Table 2: NIST CSF Failed Subcategories is less than 61. For example, NIST CSF subcategory DE.CM-7 ("Monitoring for unauthorized personnel, connections, devices, and software is performed") is mentioned as a mitigatory control to help anticipating all steps in the attack against Capital One, and PR.PT-3 ("The principle of least functionality is incorporated by configuring systems to provide only essential capabilities") appears in six out of the seven stages of Capital One attack. The following NIST CSF subcategories are the ones that apply to at least two different cyberattack stages at Capital One data breach incident:

- Seven stages: DE.CM-7, DE.DP-2
- Six stages: DE.AE-3, PR.PT-1, PR.PT-3
- Four stages: DE.CM-6
- Three stages: PR.AC-4, DE.CM-1, PR.IP-1
- Two stages: DE.CM-8, PR.IP-12

While the same NIST CSF subcategory can be applied to different attack steps, usually it represents a different scenario where a specific technical or management control should be implemented to mitigate the associated risk.

As detailed in Table 2: NIST CSF Failed Subcategories, most of CSF subcategories failures were related to the lack of vulnerability management (compromising controls DE.CM-8 and PR.IP-12), least privilege (controls PR.AC-4, PR.AC-1, PR.AC-3, and PR.AC-7), security event monitoring (DE.AE-3, DE.CM-1, DE.CM-6, DE.CM-7, DE.DP-2, and PR.PT-1), and security principles (PR.IP-1 and PR.PT-3).

The table supports the conclusion that it is likely that if some of the controls listed here were implemented effectively and operated consistently, the incident would not have materialized. We will discuss in detail, as example, two of the attack stages and related security control failures in sections 4.5.1 and 4.5.2.

Stage	Step of the attack	Technical Controls	NIST CSF Failed Subcategories
Command And Control	Use TOR Network to hide the origin of the attack	Block at Firewall and hosts access from IP addresses from TOR network exit nodes and from malicious proxy server Alert on IDS/IPS successful access from malicious IP addresses	**ID.AM-4:** External information systems are catalogued **PR.DS-5:** Protections against data leaks are implemented **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed **DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.DP-2:** Detection activities comply with all applicable requirements
Initial Access	Use SSRF attack to run commands on vulnerable server	Such attack could be mitigated by a well configured WAF and preventive controls, such as periodic vulnerability scanners	**PR.IP-12:** A vulnerability management plan is developed and implemented **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events **DE.CM-7**: Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.CM-8:** Vulnerability scans are performed **DE.DP-2:** Detection activities comply with all applicable requirements
Initial Access	Explore WAF misconfiguration to send commands to AWS Metadata Service	WAF configuration error could be identified by using preventive vulnerability scan	**PR.IP-12:** A vulnerability management plan is developed and implemented **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.CM-8:** Vulnerability scans are performed **DE.DP-2:** Detection activities comply with all applicable requirements

Stage	Step of the attack	Technical Controls	NIST CSF Failed Subcategories
Initial Access	Get the access credentials (AccessKeyId and SecretAccess Key)	Monitor and audit the use of administrative accounts	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions **PR.AC-7:** Users, devices, and other assets are authenticated commensurate with the risk of the transaction **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.DP-2:** Detection activities comply with all applicable requirements
Execution	Run commands in the AWS' command line interface (CLI)	Tracking commands on the AWS account	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.DP-2:** Detection activities comply with all applicable requirements

Stage	Step of the attack	Technical Controls	NIST CSF Failed Subcategories
Discovery	Run commands to list buckets in AWS S3	Tracking commands on the AWS account	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties **PR.DS-5:** Protections against data leaks are implemented **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.DP-2:** Detection activities comply with all applicable requirements
Exfiltration	Use the sync command to copy data from AWS buckets to local computer	Outbound traffic monitoring	**ID.AM-3:** Organizational communication and data flows are mapped **PR.AC-3:** Remote access is managed **PR.DS-1:** Data-at-rest is protected **PR.DS-5:** Protections against data leaks are implemented **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.DP-2:** Detection activities comply with all applicable requirements

Table 2: NIST CSF Failed Subcategories

Discussion on the Failed NIST CSF Framework

Due to the extent of Capital One's data leak incident and the numerous NIST CSF subcategories cyber security controls that supposedly failed across the attack flow, two relevant attack steps and related security controls were selected to provide a closer analysis of the security controls whose applicability failed during the chain of events that led to the Capital One data breach incident: the privilege escalation that granted the intruders' access to Capital One's server and the data exfiltration conduct.

The existence of technical controls to monitor and to audit the use of administrative accounts and to monitor outbound traffic could have prevented the privilege escalation and the data exfiltration activities, respectively. An extensive analysis of the entire set of mitigation controls is not in the scope of the current paper.

– ***Discussion on restricting access to privileged credentials***

During the initial access to compromise Capital One infrastructure, Ms. Paige Thompson managed to trick the metadata service to request access credentials AccessKeyId and SecretAccessKey (similar to "root access"), as described as "Step 4" in Table 1 ("Obtain access credentials (AccessKeyId and SecretAccessKey)"). Such trick allowed her to gain the necessary permissions to run commands in the servers hosted at AWS environment, as explained in section 0.

As listed in Table 2, it is expected that the mitigatory controls represented by a total of 11 NIST CSF subcategories would be able to prevent the attacker to have access to temporary credentials by the implementation of proper provisioning controls, as well as by monitoring and auditing the access and use of administrative roles.

To prevent an attacker from getting the access credentials (AccessKeyId and SecretAccessKey) to perform an exploitation, a set of technical controls are required to restrict the use of user accounts with administrative privileges, as the ones represented by NIST CSF subcategories PR.AC-1, PR.AC-4, PR.AC-6, PR.AC-7, PR.IP-1, and PR.PT-3. Monitoring and alerting subcategories described by PR.PT-1, DE.AE-3, DE.CM-6, DE.CM-7 and DE.DP-2 would raise alarms of any unauthorized access to administrative credentials.

Therefore, it is very likely that Capital One had insufficient Identity and Access Management (IAM) controls for the environment that was hacked. The periodic review of user and group configuration, in particular the Security Groups, can help ensure that services are not inadvertently exposed, and that the necessary access controls are applied correctly using the principle of least privilege.

– ***Discussion on data exfiltration prevention and detection***

In the last step of the cyberattack at Capital One, Ms. Paige Thompson ran a sync command on Capital One's server hosted at AWS cloud infrastructure to exfiltrate a large volume of sensitive information by copying data from AWS buckets to her local computer. Unfortunately, the incident and the leak of nearly 30 GB of sensitive data went unnoticed by Capital One's regular cybersecurity operations.

Table 2 lists 12 NIST CSF subcategories that are expected to help anticipating the data exfiltration by restricting remote access and by monitoring inbound and outbound traffic at Capital One servers hosted in AWS cloud infrastructure, as well as unauthorized access to critical data stored at Capital One servers.

The data exfiltration could be anticipated by the presence of technical controls to block unauthorized outbound traffic and to monitor outbound traffic from the AWS environment, as represented by subcategories PR.DS-5, PR.PT-1, DE.AE-1, DE.AE-3, DE.CM-1, DE.CM-6, DE.CM-7 and DE-DP-2. Mitigatory technical controls include, but are not limited to the use of well-known security technologies such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Data Loss Prevention (DLP). Such tools could generate alerts that would be subject to specific monitoring.

In addition, Capital One had insufficient controls to detect and to alert them when Paige Thompson ran the specific command line instructions to list and to copy the existing S3 buckets. FBI report shows that Capital One have all the logs regarding the malicious accesses, however the company was unable to detect and to block the access at the time the logs were generated, or even raise an alert afterwards, as recommended by NIST CSF subcategories listed in Table 2. For instance, AWS has the CloudTrail auditing service, which provides log and monitoring of the commands ran within the AWS infrastructure.[9] A proper monitor and alerting capabilities associated with the command history would allow the detection of suspicious actions, such as the copying of a high number of data repositories.

Discussion and Recommendations

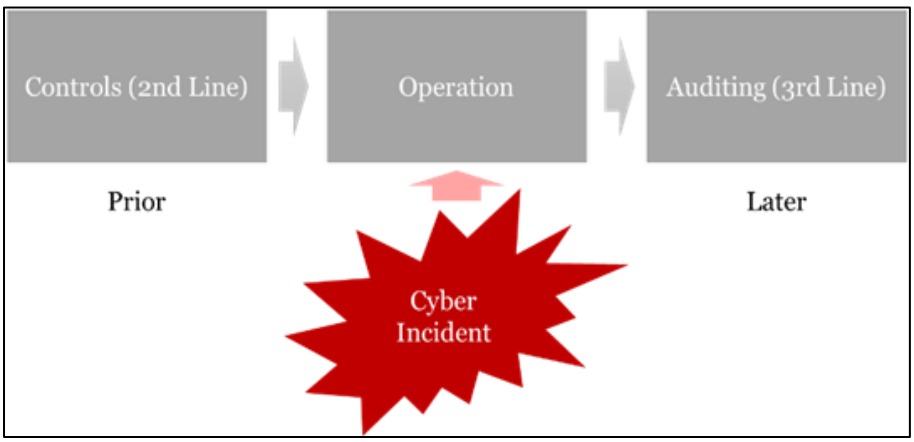
The Compliance impact on cyber security readiness

Throughout the development of this article, the modus operandi of the Capital One attack was understood, as well as the scope of the disciplines contemplated in a mature security framework adopted by the bank. By analyzing the context of the compliance and regulation requirements, one must consider that organizations have the freedom to apply best practice and regulatory controls according to their own interpretation, as well as technical requirements and business decisions appropriate to their risk appetite. In addition, there is a desire on the part of regulatory bodies to allow companies to have the necessary flexibility to adjust the guidelines and controls to fit their particularities, once it follows the proper risk management practices.

[9] CloudTrail provides a history of events for the AWS account activity, including commands ran via the AWS Management Console, SDKs, and the command line tool. (AWS, n.d.)

The potential risk for the materialization of cyber incidents lies precisely in this window of opportunity, where an organization is free to interpret the applicability of a compliance control, but the operationalization of such control may not be enough to anticipate an incident. In the Capital One case, access management control according to NIST requirement PR.AC-1 was applied, but without considering the premise of least privilege (PR.AC-4), which allowed the attacker to gain the necessary access to exfiltrate the sensitive data.

Organizations in general have the challenge to properly establish consistent compliance management across the different teams involved in handling compliance controls, usually organized as "defense lines" across large companies such as Capital One.[10] The management and assurance activities performed by the Risk, Compliance, Internal Controls, and both Internal and External Audit teams, have by definition their role in a different time and space where cyber incidents can materialize (see Figure 3: Cyber Incident window of opportunity).



Note: Three lines of defense model has different time and space between each other, which can be a window of opportunity to a cyber incident to take place without being detected.

Figure 3: Cyber Incident window of opportunity

Whereas the Capital One's Technology team (first line of defense) failed to establish proper access controls with least privilege, the time window between identifying and correcting this technical control, either by the second or third line of defense, represents a timeframe where the attacker might exploit. In such scenario, any of

[10] The Institute of Internal Auditors (IAA) adopts the "Three Lines of Defense Model" to explain the relationship between the teams involved in the ownership and responsibility for operating risk management and control (Chartered Institute of Internal Auditors, 2019).

the teams (lines of defense) would be able to identify (Brady, 2019) and to demand the correction of the weak control prior to exploration. Based on the public information available regarding this incident, it was unable to corroborate the position of the Capital One auditor team. Continuous audits through online compliance monitoring can assist with timely decision making and mitigate the risk of this kind of incident occurrences.

The cyber security gap between Governance, Management and IT

Capital One's digital transformation journey to migrate its entire technology platform to the cloud represented a well-planned strategy. They hired talent engineers, invested financially on multiple fronts, hired a renowned CISO, and even supported AWS developing a series of tools like Cloud Custodian to have a portal to monitor compliance in their entire complex, multi-account AWS environment.

However, all of these actions were not sufficient to anticipate the data breach incident. Regarding the Capital One incident, AWS said its cloud unit that stored the data was not compromised in any way. Instead, it attributed the breach to a "misconfiguration" outside of the cloud. Capital One attributed the problem to an error in its own infrastructure (Henry, Capital One customer data breach rattles investors, 2019).

The misconfiguration issues had not been detected and avoided by the security controls that Capital One claims to implement, which led to a discussion where a human error might be part of the cause. Indeed, even before the incident, some Capital One staff raised concerns about employees' morale: *"employees raised concerns within the company about what they saw as high turnover in its cybersecurity unit and a failure to promptly install some software to help spot and defend against hacks (…). While the bank was generous with cybersecurity funding, the unit struggled to stay within its budget last year.... This year (2019), budget issues have continued and possible money-saving measures, including staff cuts, have been discussed… Routine cybersecurity measures to help protect the company sometimes fell by the wayside.... the bank around late 2017 bought software from a company called Endgame to improve its ability to detect hacks... More than a year after buying the software, Capital One still hadn't finished installing it… The issue was flagged to Mr. Johnson (CISO), the bank's internal auditors and others, according to one of the people. It couldn't be determined how they responded…".* The report adds *"Sometimes the broader tech-centric culture of the firm could complicate security... Technology employees had at times been given free rein to write in many coding languages — so many that it made it harder for the cybersecurity unit to spot problems."* (Andriotis and Ensign, 2019).

While cybersecurity skills are in high demand and companies are ready to hire top talent, weak leadership and a toxic culture can quickly lead to employee morale and retention issues. This is not a technological risk, but a management risk that can impact critical actions of an organization.

In addition to the many negative consequences for the image and stock after the incident, Capital One also changed its chief information security officer out of the role. No other consequences could be identified for other compliance, audit or technology employees.

Even with these misconfiguration and management issues, Richard Fairbank, CEO at Capital One said: "We remain absolutely committed to our digital strategy and our technology transformation, and the public cloud is an essential element of that strategy." (S&P Global, 2019).

Recommendations to mitigate and strengthen cybersecurity standards based on Capital One case study

This analysis provides a set of general recommendations to help government entities, regulatory agencies, and companies to improve their cybersecurity protection strategies.

– ***To avoid the improper adoption of compliance controls***

Highly regulated industries, such as health and financial institutions, make an effort to refine their compliance guidelines and to limit the companies' autonomy in pursuit of an increasingly uniform and collaborative environment. As an example, the Federal Financial Institutions Examination Council (FFIEC) in the United States published a detailed set of controls, the so-called Technology and Security Booklets. This posture can be beneficial for companies as the regulators will have more ability to enforce controls, and auditors will have a more assertive audit criteria to achieve the objective.

– ***To keep the controls relevant as the technology evolves***

Compliance standards, legislations and regulations demand a long-term effort from the industry and regulatory bodies to be developed and updated on a regular basis. As a consequence, keeping up with the constant technological changes is a major challenge for the applicability of compliance controls. In the Capital One case, and most of other data leak cases, existing security controls applied to Cloud Computing storage properties were not properly configured to avoid the access and exfiltration of sensitive information.

As shown in Table 2: NIST CSF Failed Subcategories, the controls proposed could prevent the security incident from materializing if properly applied. A stronger governance practices, including continuous monitoring and auditing, would help Capital One to maintain a clear system of security controls. Along with compliance governance over NIST controls, keeping strong security principles, as the defense-in-depth and least privilege, would have helped with Capital One's ability to avoid and/or detect the incident.

– ***Multidisciplinary Skills***

The technical qualification of IT and Compliance professionals is an important point to consider. By working with modern and advanced technologies, in an interconnected online business, employees require multidisciplinary skills and frequent training. Even professionals with extremely technical roles as web developers and IT architects, need to improve their security and governance skills to properly apply such controls to their context, just as governance professionals must be able to understand the technological requirements applied to their IT environments. In addition, companies have to establish a governance structure that establishes the approval and action mandates, so that decisions are made timely.

– ***How to protect a Storage (S3) Cloud Environment***

Our research shows that many recent incidents are related to misconfiguration in cloud storage, for example, AWS S3 buckets. Some security controls to mitigate this type of vulnerability in AWS include:

- Know the infrastructure and know which users can access what and why;
- Apply a Principle of Least Privilege. Use AWS Identity and Access Management (IAM); user policies to specify users that can access specific buckets and objects;
- Separate resources and do not mix private and public data within a S3 bucket;
- Manage all entities and enable blocking public access;

- Keep the infrastructure up to date;
- Amazon offers a WAF solution which integrates with CloudFront and blocks suspicious requests before they reach the servers;
- Monitor the S3 buckets using AWS Config, AWS Cloudtrail and Lambda tools. Enable email notifications from AWS Trusted Advisor to notify unintended changes to bucket policies and ACLs. Run Amazon S3 Bucket Permissions check;
- Follow all the best practices as NIST CSF and the vendors' recommendations (AWS, 2019).

– ***The need to manage the compliance window***

The time lapse between a compliance control being evaluated, implemented and audited represents an important element to be considered by organizations wishing to enhance their cyber defense capabilities. Organizations can benefit from filling the gap with ongoing monitoring and auditing activities, by increasing the monitoring of their operation, from technical infrastructure (done by Network Operation Centers – NOC) and security-related incidents and vulnerabilities (managed by the Security Operation Center - SOC), with the regulatory and governance aspects, building a Governance Operation Center (GOC). Such approach would help to continuously measure the efficiency of the existing compliance controls in real time, as well as being fertile ground for analytics initiatives given the amount of multidisciplinary data.

Final considerations

The study of the Capital One incident showed that the company failed to implement proper security controls. It also demonstrated that the mitigatory recommendations detailed by the NIST Framework probably would have been sufficient to mitigate the incident, if there were enough compliance controls in place to identify the malicious activities performed in Capital One's cloud computing infrastructure, including the unauthorized access and data exfiltration during the entire chain of events.

The many cases of information leak incidents show that companies worldwide are not properly adapted to use and to manage the security of new cloud computing environments, even when compliance controls do exist, and vendor guidance is in place to provide support to companies and secure their environments. In addition, the industry has shown the inability to benchmark its desired level of regulatory compliance, keeping companies essentially blind and unable to properly avoid exposing customers to a great level of risk.

From a global perspective, each country has to assure that regulatory agencies establish proper cybersecurity compliance frameworks and regulations to support local companies and to mandate that companies must comply with widely adopted global standards. For example, in Latin America the absence of legislation enforcing the use of well-established standards such as the NIST or ISO frameworks means that companies based in these regions are not required to implement such controls that would anticipate further incidents - except when the organization itself takes the initiative to apply such frameworks on their own. In Brazil, for instance, local financial institutions have to comply with cyber security controls enforced through Central Bank Rule 4658, and also by existing laws such as LGPD[11]. However, these standards lack controls as complete and comprehensive as NIST. That being said and considering that many companies operate globally with customers and suppliers (supply chain) potentially anywhere in the world, such as the new global banks, we recommend that companies adopt global governance frameworks that feature cyber security controls capable of addressing new technologies.

In an increasingly connected world that breaks down continental barriers, weak security standards will be compromised and will, therefore, contribute to the compromise of other organizations even if such organizations follow stronger standards. In other words, a local failure can impact everyone in the industry, which is the reason why we need better global policies for data protection.

Acknowledgments

This work was supported, in part, by the C6 Bank and Cybersecurity at MIT Sloan. We would like to thank all the researchers, students, faculty from Cybersecurity at MIT Sloan and all the reviewers and editors from Journal of Information System Security for providing constructive feedback and comments on earlier versions of this article.

[11] LGPD (Lei Geral de Proteção de Dados Pessoais) is a Brazilian general data protection law.

References

Abma, J. (June de 2017). *How To: Server-Side Request Forgery (SSRF).* Fonte: HackerOne Blog: https://www.hackerone.com/blog-How-To-Server-Side-Request-Forgery-SSRF

Andriotis, A., and Ensign, R. L. (2019, August 15). *C1 Cyber Staff Raised Concerns Before Hack.* Retrieved from The Wall Street Journal: https://www.wsj.com/articles/capital-one-cyber-staff-raised-concerns-before-hack-11565906781

AWS. (2018). "*How to Cloud*" *with Capital One.* Retrieved from AWS: https://aws.amazon.com/pt/solutions/case-studies/capital-one-enterprise/

AWS. (2018). *Capital One on AWS.* Retrieved from AWS: https://aws.amazon.com/solutions/case-studies/capital-one/

AWS. (2019, May 2017). *How can I secure the files in my Amazon S3 bucket?* Retrieved from AWS: https://aws.amazon.com/pt/premiumsupport/knowledge-center/secure-s3-resources/

AWS. (n.d.). *AWS CloudTrail.* Retrieved from AWS: https://aws.amazon.com/cloudtrail/

Brady, J. (2019, August 08). *Governance in a DevOps Environment*. Retrieved from Capital One: https://www.capitalone.com/tech/culture/governance-in-a-devops-environment/

Capital One - 1. (2019, September 23). *Information on the Capital One Cyber Incident.* Retrieved from Capital One: https://www.capitalone.com/facts2019/

Capital One - 2. (2019, February 20). *2018 Annual Report.* Retrieved from Capital One: https://ir-capitalone.gcs-web.com/static-files/04c57bd9-b351-418c-9f18-ed91d4bfad23

Capital One - 3. (2019, November 1). *Corporate governance guidelines.* Retrieved from Capital One: https://ir-capitalone.gcs-web.com/static-files/2c9fe450-b8e9-4ab7-ab47-1a6e77e4d629

Capital One - 4. (2019, November 8). *Manager - Cyber Risk Management.* Retrieved from Capital One Careers: https://www.capitalonecareers.com/job/mclean/manager-cyber-controls-validation-cyber-risk-management/1732/14063087

Capital One - 5. (2019, December 16). *Sr. Manager - Cybersecurity & Tech Oversight.* Retrieved from Capital One Career: https://www.capitalonecareers.com/job/mclean/manager-or-sr-manager-cybersecurity-and-technology-oversight-cyber-risk-management/1732/14514806

Capital One - 6. (2019, November 26). *Sr. Manager - Cybersecurity Legal Business Counsel.* Retrieved from Capital One Careers: https://www.capitalonecareers.com/job/mclean/sr-manager-sr-counsel-cybersecurity-legal-business-counsel-3-positions-operations-and-intelligence-/1732/14299426

Capital One - 7. (2019, September 23). *Capital One.* Retrieved from Frequently Asked Questions: https://www.capitalone.com/facts2019/2/

Capital One - 8. (2019). *Corporate Governance – Overview*. Retrieved from Capital One - Investor Relations: http://investor.capitalone.com/corporate-governance/governance-overview

Capital One. (2020, January 7). *Our Company.* Retrieved from Capital One: https://www.capitalone.com/about/corporate-information/our-company/

Capital One. (n.d.). *Capital One Careers*. Retrieved from https://www.capitalonecareers.com

Chartered Institute of Internal Auditors. (2019, October 7). *Gov of risk: 3 lines of defence.* Retrieved from Chartered Institute of Internal Auditors: https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/

CloudSploit. (2019, August 02). *A Technical Analysis of the Capital One Hack.* Retrieved from CloudSploit Blog: https://blog.cloudsploit.com/a-technical-analysis-of-the-capital-one-hack-a9b43d7c8aea

Dellinger, A. (30 de July de 2019). *Capital One Hit With Class-Action Lawsuit Following Massive Data Breach.* Fonte: Forbes: https://www.forbes.com/sites/ajdellinger/2019/07/30/capital-one-hit-with-class-action-lawsuit-following-massive-data-breach/?sh=65c3b6f36b1a

Dimon, J. (2018). *JP Morgan & Chase Annual Report 2018.* Retrieved from JPMorgan Chase & Co.: https://reports.jpmorganchase.com/investor-relations/2018/ar-ceo-letters.htm?a=1

du Preez, D. (2021, January 12). *Capital One closes its data centres and goes all in with AWS* . Retrieved from Diginomica: https://diginomica.com/capital-one-closes-its-data-centres-and-goes-all-aws

Einstein, M. (2019, April 17). *Amazing Statistics about Online Data Creation.* Retrieved from Information Overload Research Group: https://iorgforum.org/case-study/some-amazing-statistics-about-online-data-creation-and-growth-rates/

Gesser, A., Forester, D., et al., e. (2019, January 15). *2019 Predictions – Top 10 Cybersecurity/Privacy Trends.* Retrieved from Davis Polk Cyber Blog: https://www.dpwcyberblog.com/2019/01/2019-predictions-top-10-cybersecurity-privacy-trends-to-prepare-for-now/

Hall, A. A., and Wright, C. S. (Volume 6, 2018). Data Security: A review of major security breaches between 2014 and 2018. *Federation of Business Disciplines Journal*, pp. 50 - 63.

Henry, D. (2019, July 30). *Capital One customer data breach rattles investors.* Retrieved from Reuters: https://uk.reuters.com/article/uk-capital-one-fin-cyber-amazon-com/amazon-says-cloud-unit-aws-not-compromised-in-capital-one-hack-idUKKCN1UP1I7

Henry, D. (30 de July de 2019). *Capital One Shares Fall Nearly 6% After Breach.* Fonte: Reuters: https://www.reuters.com/article/us-capital-one-fin-cyber-amazon-com-idUSKCN1UP1LD

Kammel, B., Pogkas, D., et al., e. (2019, march 18). *These Are the Worst Corporate Hacks of All Time.* Retrieved from Bloomberg: https://www.bloomberg.com/graphics/corporate-hacks-cyber-attacks/

Krebs, B. (2019, August 02). *What We Can Learn from the Capital One Hack.* Retrieved from KrebsOnSecurity: https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/

Miller, R. (2015, August 31). *FFIEC and NIST: A Comparison of Two Prevalent New Compliance Frameworks* . Retrieved from West Monroe Partners: https://blog.westmonroepartners.com/ffiec-and-nist-a-comparison-of-two-prevalent-new-compliance-frameworks/

MITRE. (2017, May 31). *Command-Line Interface.* Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1059/

MITRE. (2017, May 31). *Exfiltration Over Alternative Protocol.* Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1048/

MITRE. (2017, May 31). *System Service Discovery.* Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1007/

MITRE. (2017, May 31). *Valid Accounts.* Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1078/

MITRE. (2018, April 18). *Exploit Public-Facing Application*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1190/

MITRE. (2018, January 16). *Multi-hop Proxy*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1188/

Neto, N. N., Madnick, S., de Paula, A. M., and Borges, N. M. (January de 2021). Developing a Global Data Breach Database and the Challenges Encountered. *Journal of Data and Information Quality*.

Newman, D. (2019, July 14). *Top 10 Digital Transformation Trends For 2020.* Retrieved from Forbes: https://www.forbes.com/sites/danielnewman/2019/07/14/top-10-digital-transformation-trends-for-2020/

O'Donnell, L. (25 October 2019). *Is AWS Liable in Capital One Breach?* Fonte: threatpost: https://threatpost.com/capital-one-breach-senators-aws-investigation/149567/

Panetta, K. (2018, October 15). *Top 10 Strategic Technology Trends for 2019*. Retrieved from Gartner: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/

PRNewswire. (2019, July 29). *Capital One Announces Data Security Incident.* Retrieved from Capital One: https://www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident/

Reinsel, D., Gantz, J. and Rydning, J. (2018, November). *The Digitization of the World.* Retrieved from Seagate: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

S&P Global. (2019, October 24). *Capital One CEO (...) data breach*. Retrieved from S&P Global - Market Intelligence: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/55016463

Salane, D. E. (2009, June 5). *Are Large Scale Data Breaches Inevitable?* Retrieved from John Jay College of Criminal Justice: http://johnjay.jjay.cuny.edu/files/centers/cybercrime_studies/D_SalaneLargeScaleDataBreaches.pdf

Sandler, R. (2019, July 29). *C1 Says Hacker Breached Accounts Of 100 Mi People.* Retrieved from Forbes: https://www.forbes.com/sites/rachelsandler/2019/07/29/capital-one-says-hacker-breached-accounts-of-100-million-people-ex-amazon-employee-arrested/

TCDI. (n.d.). *Info Sec Compliance: Which regulations relate to me?* Retrieved from TCDI Blog: https://www.tcdi.com/information-security-compliance-which-regulations/

U.S. Attorney's Office. (2019, August 28). *Former Seattle Tech Worker (...) Computer Data Theft.* Retrieved from U.S. Department of Justice: https://www.justice.gov/usao-wdwa/pr/former-seattle-tech-worker-indicted-federal-charges-wire-fraud-and-computer-data-theft

Unknown. (2017, August 17). *Who Regulates Whom?* Retrieved from EveryCRSReport: https://www.everycrsreport.com/reports/R44918.html

US District Court at Seattle. (2019, August 28). *USA v. Paige A. Thompson Indictment.* Retrieved from The U.S. Department of Justice: https://www.justice.gov/usao-wdwa/press-release/file/1198481/download

Whittaker, Z. (2019, July 29). *Capital One's breach was inevitable.* Retrieved from TechCrunch: https://techcrunch.com/2019/07/29/capital-one-breach-was-inevitable/

Whittaker, Z. (2019, July 22). *FTC slaps Equifax with a fine of up to $700M for 2017 data breach.* Retrieved from TechCrunch: https://techcrunch.com/2019/07/22/equifax-fine-ftc/

Nelson Novaes Neto is a MIT Affiliated Researcher and CTO and Partner, of C6 Bank, where he is the CTO. Nelson Novaes is one of the leading partners in the creation of C6 Bank, a rapidly expanding digital bank. Novaes is a MIT Affiliated Research, engineer, postgraduate in InfoSec, MBA and Master's in Psychology. Novaes has broad experience in the internet industry product development and security. He also has several international certifications. He was CISO at Itaú Unibanco, the largest financial conglomerate in LATAM and present in more than 25 countries. For over a decade, Novaes was CSO of UOL, the biggest ISP in LATAM. He is a member of the PCI-DSS and Board of the (ISC)2 for LATAM. He also developed several projects for the education and protection of the infrastructure in Brazil. In addition, develops social projects with the authorities, Brazilian Internet Steering Committee, NGOs and Government. He is also a climbing passionate who reached the biggest summit in Americas, Europe, Africa and Alps.

Stuart Madnick is the John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management and a Professor of Engineering Systems at the Institute for Data, Systems, and Society, MIT School of Engineering. He is the Founding Director of Cybersecurity at MIT Sloan (CAMS), formerly the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. His involvement in cybersecurity research goes back to 1979, when he co-authored the book *Computer Security*. He holds a Ph.D. in computer science from MIT and has been an MIT faculty member since 1972 and has been the head of MIT's Information Technologies Group at the Sloan School of Management for over 20 years. He is the author/co-author of more than 400 books, articles and reports. Besides cybersecurity, his other research interests include Big Data, semantic connectivity, database technology, software project management and the strategic use of information technology. Dr. Madnick has been active in industry as a developer of IBM's VM/370 operating system and Lockheed's DIALOG system. He has served as a consultant to major corporations and was the co-founder of five high-tech firms. He is currently responsible for operating the 14th century Langley Castle Hotel in England.

Anchises Moraes is a cyber prevenger who uses a hacker mindset to bring unorthodox paradoxes to a hyper-connected world. With over 20 years' experience in the computer security industry he works as a Cyber Evangelist at C6 Bank, having he worked at RSA and VeriSign iDefense as a Threat Intelligence Analyst. A director of the Cloud Security Alliance Brazil and the Supreme Chancellor of the Garoa Hacker Clube hackerspace, he co-founded the Security BSides São Paulo conference.

Natasha M. Borges works as Cyber Engineer at C6 Bank. She has a strong background of working with security and IT governance in highly regulated environments such as financial markets and telecoms.