Capital One Data Breach:

Revised Information Assurance Plan

Jeremy Willett

**Overview of Goals and Objectives**:

In 2019, Capital One was subject to a data breach. This breach was discovered on July 19, 2019. According to Capital One, “we determined that an outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products” (Information on the Capital One Cyber Incident, 2022). In an analysis of the event, Jose Blanco states, “The breach started between the 22nd-23rd March and was discovered almost four months later by Capital One (19th July). The stolen information included credit card numbers, birth dates, addresses, names, phone numbers, transaction history, 140,000 Social Security numbers and 80,000 bank account numbers. After initial speculations that pointed to a zero-day exploit, the culprit, a former employee of Amazon Web Services (AWS), who used an SSRF attack, was arrested. An investigation has been opened that will affect Capital One, AWS and GitHub (the platform that published the stolen data)” (Blanco, 2020). An SSRF attack is a Server-Side Request Forgery attack in which involves an attacker abusing server functionality to access or modify resources.

The goal of this document is to analyze Capital One’s existing information assurance plan and recommend changes to develop a new information assurance plan to work to minimize the effects of this kind of event in the future. It is commonly agreed upon in the field of cybersecurity that data breaches cannot be entirely prevented. These events will happen as would be attackers seek to gain access to sensitive information. The main goal of an information assurance plan is to uphold the confidentiality, integrity, and availability of information at all times. While no plan can prepare for every possible kind of event, developing, implementing, and practicing a good information assurance plan within a company will lead to minimizing the effects that security breach events have and reduce the impact on the company and its clientele.

The common CIA triad (confidentiality, integrity, and availability) has been altered to include two additional pillars to add authentication and non-repudiation. These pillars combine to create the overarching principles of information assurance and describe their purpose in their meaning. “Information security analysts use their knowledge of computer systems and networks to defend organizations from cyber threats. They monitor the networks to keep track of any possible security breaches, and they investigate any that they find. Additionally, they are responsible for setting up protective measures within information systems. To ensure that those measures will comply with the five pillars of information assurance, they also conduct penetration tests that simulate attacks so they can identify vulnerabilities real attackers could exploit” (Norwich University Online, 2018).

By creating a plan around these five principles, a company can work to maintain their information by ensuring it remains confidential and protected. The data stays protected preventing it from be altered or changed by any unauthorized individuals. With the data protected it remains available to be accessed when needed by those authorized to do so. Changes and access to the data is verified and tracked meeting the requirement of non-repudiation and finally, those accessing the information are verified and authenticated ensuring they are authorized to access the information.

**Confidentiality, Integrity, and Availability of Information**:

Regarding the data breach of 2019 at Capital One, only one of the pillars of information assurance was in place. The information was accessed and downloaded however nothing was changed, meaning the integrity of the company information in question was maintained. The issues arise around the other pillars.

First, looking at confidentiality, this was breached by way of the data being decrypted. “Capital One reported via a press release (PRNewswire, 2019) that some of the stolen data was 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” (Neto, Madnick, Paula, & Borges, 2020). While they did not disclose specifics of how this happened, the fact that the encrypted data was decrypted indicates the method of encryption used was not secure.

Availability coincides with authentication. While the information remained available to the company, it was left too available, in a sense, allowing the attacker to gain access to it easily and download from the servers it was stored on. While availability dictates that information be easily available and not hindered for overbearing protections, it needs to be supplemented with proper authentication to ensure only those who are supposed to accessing the data are doing so. Without good authentication in place, as is the case of this data breach, the information becomes free reign to anybody who happens to look for it.

Lastly a system of nonrepudiation being in place is necessary to ensure all access to data is recorded and trackable. Proper implementation of nonrepudiation makes it so that no person can deny accessing a given system. In the case of the breach, the company got lucky in the fact that to the attacker posted the information on GitHub and made social media posts about it. The fact that the attacker was caught had little do with any of the security protocols and protections Capital One had in place.

**Current Protocols and Policies**:

It is unlikely for a company to willingly reveal deficiencies they may have in their policies and protocols at the time of an incident; however, we can look at the evidence used in cases against Capital One at the time for reference. Capital One faced fines from the Office of the Comptroller of the Currency (OCC), and a class action lawsuit from those affected by the data breach. From these cases we can look at the deficiencies of Capital One’s policies at the time.

The OCC levied its fines “based on noncompliance with the Code of Federal Regulations (CFR), specifically, 12 CFR Part 30, Appendix B, Interagency Guidelines Establishing Information Security Standards” (Lalloobhai, 2020). The OCC noted in their findings:

* “Capital One failed to establish effective risk assessment processes in 2015 before migrating its information technology operations to a cloud environment.
* Internal audit did not properly assess the cloud environment, and as a result, did not effectively identify nor report on weaknesses and gaps to the Audit Committee.
* For internal audit findings that were reported, the Board did not take the appropriate action to hold management accountable” (Lalloobhai, 2020).

As a result, when migrating their information over to the Amazon Web Services, Capital One failed to have redundancies in place to ensure obvious vulnerabilities were not in place such as the one used as a vector for the attack.

In the class action suit against Capital One, the plaintiffs alleged, “that Capital One (and AWS) knew their systems were vulnerable to SSRF attacks and described a mitigation called Cloud Custodian that would encrypt all data stored in Capital One S3 buckets. While this would not have prevented the data from leaving Capital One’s control, it would have made it useless to individuals such as Ms. Thompson. Encrypting the data makes it unreadable” (Covert, 2021). This is something that it would appear Capital One had an idea of as used as example in the suit, “In fact, Capital One seemed to predict its own data breach when a senior engineer from the company at a public engineering conference host by AWS stated: “In the cloud, all these resources are just available via URL so those are part of your network boundary. And those resources that have embedded IAM policies need special care and attention because they can be enabled to be accessible outside of your account. I think everyone’s familiar with some of the things around S3 but that extends out to a lot of the other resources I called out a couple here”.” (Covert, 2021).

The company’s policies at the time were lacking and left them vulnerable. “The Open Web Application Security Project (OWASP) is a non-profit organization dedicated to improving software deployed on the Internet. They publish a number of resources for software developers and organizations and make them freely available to download. OWASP calls them “cheat sheets.” They outline controls or mitigations companies can use to prevent a number of vulnerabilities including SSRF” (Covert, 2021). Failure to follow industry recommendations leaves the company directly at fault for the vulnerabilities left in place allowing the data breach to occur. As a result of this, the current information assurance policy needs to be altered to prevent obvious vulnerabilities in the handling of sensitive personal and company information.

There are barriers that may exist to implementing a new information assurance plan. They can include a lack of resistance to training from staff. “It is difficult to get the balance right. If you ‘over-secure’ and enforce some highly rigid controls, you risk creating an unpleasant working culture that leads to attrition. But if you are too lax in implementation, you get ‘passive avoidance’, where people ignore guidance, or mark something as low priority, to make their lives easier” ( Data security: barriers to success, 2017). Another barrier could be that the right people aren’t in the loop such as high-level management. “If you do not have buy-in at the highest level, any enterprise-wide data initiative is likely to fail. This isn’t just because the leadership can provide governance and give the program its due level of importance – it also ensures that those involved in assessing the data are clear about its wider strategic relevance” ( Data security: barriers to success, 2017). A final barrier to consider is inconsistency in applying data security principles. “Despite guidance such as the CIA model, it is difficult for large organizations to achieve consistency in how their people think about data. Exacerbating this problem is the fact that the risk attached to one data set may change over time depending on its relevance to current business priorities” ( Data security: barriers to success, 2017).

**Responsibilities of Key Leaders**:

Capital One employs an entire cyber unit. The main leader of this area is the Chief Information Security Officer (CISO). At the time of the data breach, Michael Johnson was the CISO for Capital One. “Bank management should “evaluate and monitor the cloud service provider’s technical, administrative, and physical security controls that support the financial institution’s systems and information assets that reside in the cloud environment,” the FFIEC said” (Ennis, 2020). The FFIEC is the Federal Financial Institutions Examination Council. They continued to write, “Management’s failure to understand the division of responsibilities for assessing and implementing appropriate controls over operations may result in increased risk of operational failures or security breaches” (Ennis, 2020). The CISO holds primary responsibility for these understandings, assessments, and implementation.

Under the CISO, the cyber security unit employs security analysts and engineers responsible for the day-to-day operations and development and implementation of new software handed down by management. “Employees at Capital One Financial Corp. had raised concerns about problems in the bank’s cybersecurity unit, those concerns included those about high turnover and questions about why software meant to prevent hacks was not installed in a timely matter, according to the report” (Cooper, 2019). The members of the cyber unit at Capital One are under the CISO and answer to them in regard to their assignments and responsibilities. “Some of those sources also pointed to a long delay in Capital One’s deployment of software it purchased to ward off hacks, according to WSJ” (Cooper, 2019). These kinds of reports are an example of the failure of the management responsible for systems protection and implementation and the degree that employees under them have no control in the processes necessary for these to take place.

**Key Ethical and Legal Considerations**:

The main ethical considerations the companies and managers must consider revolve around privacy. As a company that intakes and stores personal sensitive information always must keep customer privacy at the top of the list of priorities.” As a network administrator or security professional, you have rights and privileges that allow you to access most of the data on the systems on your network. You may even be able to access encrypted data if you have access to the recovery agent account. What you do with those abilities depends in part on your particular job duties (for example, if monitoring employee mail is a part of your official job description) and in part on your personal ethical beliefs about these issues” (Schinder, 2005). In the banking industry, the level of sensitive personal data added to the equation is increased substantially as this adds financial information and control. Think of the entire picture. A bank stores all personal information of an individual such as name, address, contact information, and social security number. Add to this the account and routing information for the individuals checking, savings, and credit card accounts and the picture can be seen as having full access to someone’s most personal sensitive information. With this considered, it shows how privacy is the top concern for any financial institution. These are all compounded by a manager needing to direct all the employees under them who all have access to this same information.

The main legal concern for a financial institution and their information security falls under the governance of the Gramm–Leach–Bliley Act (GLBA). This act “requires financial institutions to protect customer data and honestly disclose all data-sharing practices with customers. Under this U.S law, financial entities must establish security controls to protect customer information from any events threatening data integrity and safety. This includes strict financial information access controls to mitigate the chances of unauthorized access and compromise” (Kost, 2022). Financial institutions must also maintain compliance with the Financial Industry Regulatory Authority (FINRA). FINRA is “an organization that has established a set of rules for protecting customer data from compromise. FINRA also promotes controls for detecting cyber threats and mitigating their impact” (Kost, 2022). Compliance with FINRA is required in the United States. These legislative documents guide and direct how information is stored and protected. Maintaining compliance with these regulations is required to uphold proper information security standards.

Failure to comply with legal and ethical standards and regulations in the financial industry can result in legal action. In the case of the 2019 data breach, Capital One faced class action lawsuits from customers affected by the data breach. As evidenced by statements of employees in the cyber unit, the vulnerability that left the door open to this data breach was a fault of Capital One and as a result, the financial burden placed on the company is a direct result of not protecting customer information properly. Financial impact can extend beyond lawsuits resulting from a data breach. The impact of a data breach can affect how customers perceive the organization and a loss of customers can be seen from customers losing confidence in the organizations ability to protect their information. This is something that must be kept in mind when managing risks as public perception can easily impact an organization heavily if the public and their customer base lose confidence in their ability to perform their duties as a financial institution.

**Key Components of Information Assurance**:

Information Assurance is upheld when confidentiality, availability and integrity are maintained. These aspects fall onto every employee in an organization. From the CISO to individual security analysts to customer service representatives, data must be protected and secured. This is done through several avenues. The first line of defense for an organization is training. “Misconfigurations are caused by human error. Therefore, organizations need to prioritize training and education for security teams and system administrators, so they are adequately prepared to perform the job functions expected of them. Admins need to understand more than just what security controls and tools are in place, but why they are implemented and the reasons for existing configurations. Managing attrition, understaffed teams and navigating skill gaps can make seemingly straightforward tasks much more difficult to perform consistently. Whether training is on the job or in a more traditional classroom setting, knowledge transfer and training should be prioritized” (Yakencheck, 2019).

A second component of maintaining information assurance is periodic review of system configurations. “Mistakes are inevitable – no one is perfect. Unfortunately, security teams must be right all the time to effectively defend networks and a bad actor only has to find one slip-up to cause havoc with an exploit. Conducting internal periodic and recurring reviews of configurations, patch levels and security posture is an effective method to detect potential exposures before they are exploited. Each organization should assess if it is performing recurring reviews and implementing the follow-up actions to remediate any findings in a timely manner” (Yakencheck, 2019).

A third component is audit logging and review. “The logs of actions taken within the Capital One environment appear to have been comprehensive enough to reconstruct the events that took place and effectively determine how the intrusion occurred. Enterprises should have robust logging in place and protect those logs to maintain a strong security posture. Active monitoring and efficient investigation of audit log events facilitate quicker discovery of anomalies and help foster a culture of greater cyber-resiliency” (Yakencheck, 2019). Had Capital One performed an audit on a regular interval, the data breach would not have taken months for the company to discover, and the avenue of attack would not have remained open for so long.

Lastly, customer protections need to be in place to help ensure constant monitoring and help protect customer in the event of data breaches. “While more than 100 million people are impacted by this Capital One breach, less than 1 percent of those people had their Social Security or bank account numbers compromised. Still, other data was stolen, such as reported income, addresses, names, and other key information. As always, credit monitoring and basic cyber-hygiene processes are important and should help ensure the average consumer does not have catastrophic disruption to their livelihood” (Yakencheck, 2019).

**Analysis of Environment**:

While Capital One is a financial institution and as such must meet regulations imposed on this industry, the company has made a large push to move to the use of cloud computing for their systems. The company utilizes AWS for this task. To analyze the environment the company operates within, it is necessary to investigate AWS and how it works in conjunction with its customers to secure data and maintain information assurance.

Amazon utilizes what they call “AWS Cloud Compliance”. To maintain this, they put in place a policy they refer to as the “Shared Responsibility Model”. “Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer’s operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security “of” the Cloud versus Security “in” the Cloud” (AWS, 2022). This can model can be visualized in the following chart.

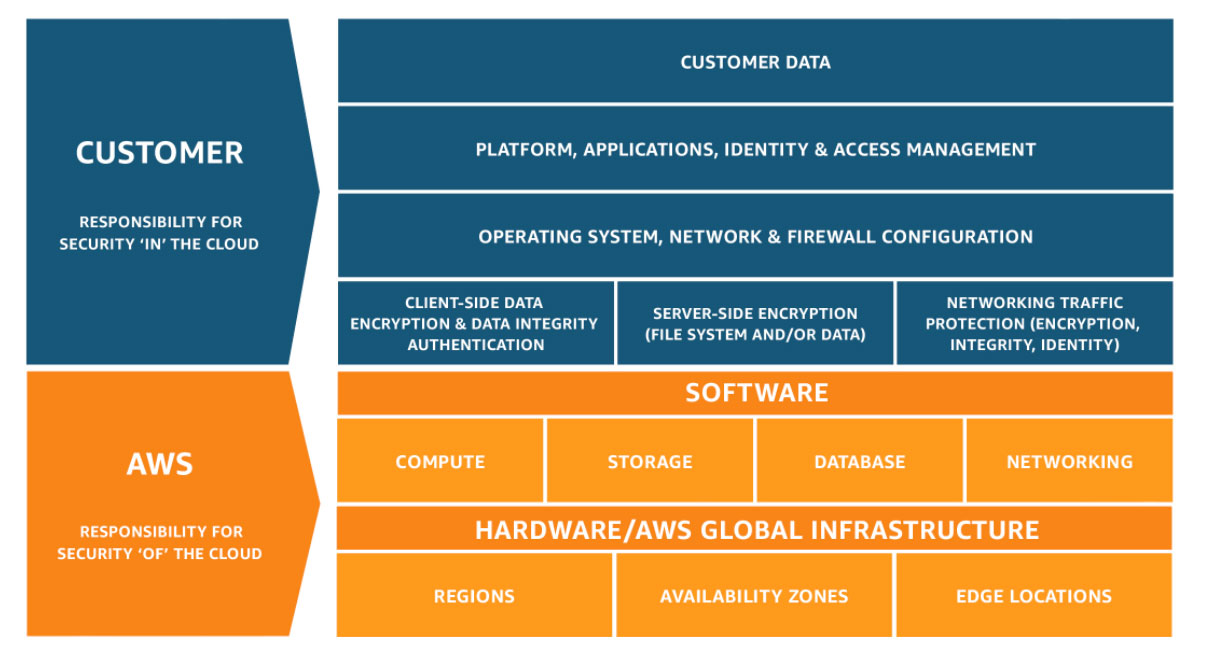


Figure 1 - AWS Shared Responsibility Model (AWS, 2022)

With this model in mind, the responsibility of client data protection falls onto Capital One (as the customer in this situation) and AWS holds responsibility for the infrastructure and base software side. As a result of this, both AWS and Capital One must ensure the system is configured to protect from unauthorized access on their respective sides of the system. By utilizing AWS, Capital One is relying on an external company to ensure the necessary steps are taken to protect the system as well as needing to ensure protection steps are taken on their side of the system.

**Threat Environment**:

The threat environment created by utilizing AWS is unique in the aspect of where the threat can come from. In the case of the 2019 data breach, the breach came from a previous AWS employee. Regardless of who the attacker may be, a system needs to be configured in a way to prevent unauthorized access regardless of where the attempt to access information is made, whether internal or external. We can analyze some of the facts from the data breach to assess the threat environment of the company pre data breach.

The main vulnerability here is the configuration of the web application firewall (WAF) being implemented on the system. ““WAFs are great, but there should be an additional layer of security, and the underlying resources themselves need to be secure,” Hunt says. “For argument’s sake, if this was lack of authentication on a resource, and they were just relying on the WAF to keep people out, then that is a pretty egregious oversight.”” (Kirk, 2019). This firewall was left open to bypassing by having an administrator account set up with privileges that allowed essentially walking right through the firewall. “But the use of the administrator account to access large amounts of data should have been a signal of possible malicious activity for Capital One, Vecci says. Access management is a key part of security, including watching what activities certain accounts undertake, such as copying large amounts of data. “This means there wasn’t the right kind of monitoring in place,” Vecci says. “Privileged accounts accessing data this way should be flagged as abnormal.”” (Kirk, 2019). Failure to have monitoring in place to identify and track accounts accessing and copying data left the company open to attack with very little response. Failure to monitor data access resulted in the four-month gap in discovery of the breach and even then, it was not the company that discovered the unauthorized data access, they were notified from a third party who saw the data listed outside the company.

Another threat comes from the practice of keeping old data and the risk this carries. “Hunt says a more relevant question is why Capital One still needed credit card application data from as long as 14 years ago. The personal data covered 100 million people and was collected between 2005 and early this year. The data includes applicant names, addresses, birth dates, credit histories, balances, and payment histories. The prevailing wisdom these days is that organizations shouldn’t hold onto data that’s unneeded. That is codified in Europe’s General Data Protection Regulation, which says organizations should generally delete personal data when it’s no longer needed for the purpose it was collected, such as if someone closes their account. But Hunt says, “organizations tend to look at data as an asset, and they don’t ever look at it as a liability”” (Kirk, 2019). Holding onto sensitive data needs to be viewed from the perspective of the risk it carries. The data breach was a perfect example of this risk. A vast number of those affected by this breach did not need to be affected had the company not held onto data that was serving no real purpose. Combine this with failure to properly encrypt the data and control access to it resulted in the breach being as widescale as it was.

**Best Approaches**:

There are several improvements that can be made to information assurance policy to help reduce the risk the company carries in hosting the large amounts of sensitive data associated with a financial institution. Firstly, the company needs to institute monitoring protocols and practices to track who is accessing data, when they are doing and what they are doing with the data being accessed. This can be done with networking monitoring tools and API developed to track roles assigned to specific users on the system. By doing this, it will aid in the discovery and traceability of data access. These kinds of monitoring tags can be flagged and reviewed when access is granted, and suspicious activities are performed.

A second improvement is to update the information and data retention policy to look at it from a risk perspective as opposed to an asset-based perspective. This is something that needs to be changed industry wide. While data can be an asset to hold and can provide customer metric data from business projections, holding sensitive data increases the risk the company faces as a target of attack for access to this information. By implementing a data retention policy that dictates a length of time that this data is kept, the company reduces the potential risk and impact associated with this data while still maintain the positive side to storing the data as an asset.

Lastly, implementation of multi factor authentication on the system aids in protecting all areas of the system. Logging in, accessing information, modifying, viewing, or extracting sensitive information would all benefit from the addition of multifactor authentication. “Temporary credentials could require a second factor of authentication. It might seem like this defeats the purpose of being able to pull credentials out of thin air, but if IAM Roles required a second cryptographically difficult to guess string then it allows for two things: First, attackers who can access the metadata service but can't read the second factor from disk or source code are not able to use the credentials they retrieve from a successful SSRF attack. Second, employees who are handling this second factor string do not need to take too many precautions to protect it. They can treat it like a secret, but by itself it is not sensitive so fewer precautions would need to be taken when handling the second factor” (Evan, n.d.).

**Risk Matrix**:

Chart, treemap chart

Description automatically generated

Figure 2 - Risk Matrix (Boogaard, 2022)

To address the possible risks of Capital One’s system, a risk matrix is used to compare the likelihood of a risk occurring to the impact that risk will have on the system and the company in the event of its’ occurrence. The above risk matrix categorizes events from very likely to very unlikely with impacts ranging from insignificant to catastrophic. In the case of the data breach, the firewall breach would be ranked in the medium range. It had a possible attack vector that the attacker took advantage of. The impact of the breach was moderate, while it was a massive breach of customer data, it did not affect the day-to-day operations of the company. It still required the attention of the company and necessitated revision of the current system configuration. The risk that retaining old data carries is one that is relatively low in possibility but is not unlikely to have an impact. The risk the company takes by retaining this data is one that increases with time as the size of the data store is increased. This risk increases in severity with time. While it remains possible, the longer they decide to retain data, the higher the impact it will have if the time comes again that it is accessed and/or stolen.

These risks can be managed with revision of the current policies as addressed in earlier sections. No solution exists that eliminates all the risk associated within a system but minimizing errors and approaching topics from a risk perspective aid to minimize risks associated with each category.

**Incident Response Protocols**:

There are six steps to an incident response plan that are necessary to set protocols in place to handle any incident that occurs for an organization. Preparation, Detection & Identification, Containment, Remediation, Recovery and Post-incident Activities. Capital One’s response to the 2019 incident gives insight into what the company currently has in place for Incident Response Protocols. “From Capital One’s announcement, we can determine they took the following steps to validate and mitigate the reported findings:

* Immediately fixing the configuration vulnerability
* Working with the FBI to arrest the person responsible
* Determining exactly what type of information was compromised and how many individuals in the US and Canada were impacted
* Performing an analysis to determine if the information was shared or used for fraud
* Notifying customers
* [Answering FAQs](https://www.capitalone.com/facts2019/) like: What was the vulnerability that led to this incident? When did this occur? Was the data encrypted and/or tokenized? Did this vulnerability arise because you operate on the cloud?
* Making information about the incident available on their online and easily accessible.” (Harvey, 2019)

Along these lines we can establish new protocols for the company to follow in the event of future incidents and better prepare for such incidents. As part of the preparation phase, it is important for the company to establish an Incident Response Team (IRT) to be activated upon detection of an event. Appropriate lines of communication should be pre-defined to follow when the incident response is activated and have all the necessary tools available for use at the time of an incident. Any support services that will be necessary should also be identified and defined such as law enforcement, or cyber security research and advisors.

Identification and notification of an incident can occur from within the company or outside the company. The company will have in place and maintain a responsible disclosure form on the company website for external individuals to report any information of a security breach or failure in the company’s system. Identifying an event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence will be preserved, and forensic analysis may be conducted consistent with legal requirements.

Following proper identification of an event, the incident needs to be contained as fast as possible to minimize damage caused by the incident. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties.

Once the incident is contained, the situation needs to be remediated by addressing all the components and symptoms of the incident. This includes proper testing after the remediation to ensure the incident does not happen again.

The recovery step is to recover and restore all data and systems to a working state to allow business to continue to operate as normal. Prior to restoring systems to normal operation, it is critical that the IRT validate the system to determine that eradication was successful, and the network is secure. If feasible, the system should be installed in a test environment to determine functionality prior to re-introduction into a production environment. Furthermore, network monitoring should be implemented for as long as necessary to detect any unauthorized access attempts.

Lastly, Post Incident Activities are performed to learn from the incident and recommend any further actions necessary to improve the system to prevent further incidents. Reporting and post-incident analysis on the system that were the target of the incident and other potentially vulnerable systems. The objective of this phase is continued improvement to applicable security operations, response capabilities, and procedures.

**Justification of IRP**:

The goal of an Incident Response Plan to prepare for an incident occurring that involves a breach of system security. The plan is put in place to set necessary procedure on how to respond to an incident to minimize its impact and damage and well as resolve the issues caused by the incident to keep the system running to prevent a disturbance in normal business operations. Identification “involves detecting deviations from normal operations in the organization, understanding if a deviation represents a security incident, and determining how important the incident is” (Cynet, 2022). By analyzing events, correlating data from multiple sources and documenting everything incident responders are doing, all questions can be answered in the standard who, what, when, where, why, and how question format about the incident.

“The goal of containment is to limit damage from the current security incident and prevent any further damage. Several steps are necessary to completely mitigate the incident, while also preventing destruction of evidence that may be needed for prosecution” (Cynet, 2022). This is the biggest step in mitigating threats. While preparation will set up the company to best handle any incident that occurs, it is not feasible to think the company is 100% safe from an incident, regardless of how much planning they try to do. Because of this, the company’s incident response team and their ability to contain the damage caused by an incident is the biggest chance the company has at mitigating damage and loss. Remediation and recovery of an incident follow closely with containment. “NIST believes that containment, eradication, and recovery are all overlapping phases. For example, as you contain threats within your systems, you should not wait to eradicate issues until all threats are found. Rather, you should contain and eliminate threats as soon as possible, even if other threats remain” (Cynet, 2022). Whether these three steps are viewed as one or three separate phases, they all serve the same end goal and must be handled swiftly and decisively.

Finally, there are always lessons to be learned. Every company is vulnerable to an incident occurring regardless of what they do to prevent them. When an incident does occur, it is vital that lessons are learned from the incident and implemented into the company policy to prevent similar incidents.

**Disaster Response Protocols**:

Disaster response protocols are used to respond to unforeseen natural or human caused disasters such as equipment failure due to power outage or a ransomware attack. The first step in a disaster response plan is preparation, like the incident response plan. The goal of preparing for a disaster is to take inventory of all hardware, software, and data the company has. As part of the preparation, the company must ensure all critical information is backed up. This is designed to guide recovery of critical processes and data in the event of a disaster. To ensure data is protected, the backups taken of the system should encompass a full-scale mirror of the system to restore the system to full working order. Once a disaster has occurred, a similar plan to the Incident Response plan is utilized to get the company back to normal operations. A disaster response team will be used to facilitate the speedy recovery of the system and do so in an organized fashion. Each type of disaster should have a more specific step by step guide, such as fire, flood, electrical outage, or ransomware. This is to dictate specific guidelines for each type of disaster. Once the initial dangers of a natural disaster are handled, the goal becomes restoring the system entirely. This is done by utilizing the backups created of the system. Once this is done, normal operations can commence to allow business to continue. The last part of the disaster plan includes maintaining and updating the disaster response plan with any changes made to the system as they are made to ensure the plan is kept up to date for the most recent version of the company system.

**Justification of DRP**:

The goals of a disaster response plan are to limit the impact a disaster has on the company and its operations. “’Key reasons why a business would want a detailed and tested DRP include:

* To minimize interruptions to normal operations
* To limit the extent of disruption and damage
* To minimize the economic impact of the interruption
* To establish alternative means of operation in advance
* To train personnel with emergency procedures
* To provide for smooth and rapid restoration of service” (Kyndryl, 2022)

By utilizing a mirror back up of the system, the system can be put back online in a fast manner that keeps it fully functional and working order. “A mirror backup will create one compressed file that’s used to recover data after a disaster. You’ll be able to restore your computer just as you had it (settings and all). In a lot of ways, a mirror backup is essentially the same thing as disk cloning (both copy everything from the computer). Disk cloning allows you to transfer data from one hard drive to another, while mirror backups store your data and compress it to just a few small files for when you’re ready to access it again” (Drake, 2020).

**Access Control Protocols**:

The access control protocol to be adopted by Capital One should be the Open Supervised Device Protocol with TLS 1.2 developed by the Security Industry Association (SIA). “SIA encourages broad adoption of this standard –which is already in wide use by many leading manufacturers like Cypress, HID Global and Mercury – and recommends specifying OSDP for any access control installations that require real security and/or will be used in government and other higher-security settings. SIA OSDP is particularly valuable for government applications because it meets federal access control requirements like PKI for FICAM” (SIA, 2022).

**Justification of ACP**:

The benefits of OSDP are listed by the SIA as:

**“Higher Security**

* OSDP is more secure than the most common access control communications protocol.
* OSDP Secure Channel supports high-end AES-128 encryption (required in federal government applications).
* OSDP constantly monitors wiring to protect against attack threats.

**Advanced Functionality**

* OSDP supports advanced smartcard technology applications, including PKI/FICAM and biometrics.
* OSDP supports bi-directional communications among devices.
* OSDP supports advanced user interface, including welcome messages and text prompts.
* OSDP’s use of 2 wires instead of 12+ allows for multi-drop installation, supervised connections to indicate reader malfunctions, and scalability to connect more field devices.

**Ease of Use**

* Audio-visual user feedback mechanisms provide a rich, user-centric access control environment.
* Guesswork is eliminated since encryption and authentication are predefined.
* Low cost of implementation on an embedded device.” (SIA, 2022)

TLS 1.2 “relies on a combination of symmetric and asymmetric cryptography. More specifically, TLS 1.2 replaces the MD5/SHA-1 combination in the digitally signed element with a single hash, ensuring increased security in negotiation during the handshake. At the same time, TLS 1.2 provides improvements to both the client’s and the server’s ability to designate algorithms for the hash and the signature. TLS 1.2 also supports increased authentication encryption and adds TLS extensions and AES cipher suites” (Daniels, 2022).

**Method for Maintaining the Information Assurance Plan**:

There are two big factors in maintaining an information assurance plan. Testing and training. Security awareness training should be implemented to teach all employees the details of the company information assurance plan and the role they play within it. It is vital that employees are trained and kept up to date with the best practices to minimize risk and protect the company information. The second step for maintaining the plan is through audits. This can be done by the information security department or through a third party to assess any security gaps that remain. Constant testing of the information assurance plan ensures that it is kept up to date and set up to be the most effective that it can be.

When choosing implement access control methods, there are three types. Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-based Access Control (RBAC). Each of these has their own advantages and disadvantages based on their use and can be implemented to provide access control protocols to a system.

“Mandatory access control (MAC) is a network-based access control where settings, policy and passwords are established and stored in one secure network and limited to system administrators. This access control is managed from a central computer where an administrator can grant or revoke access from any individual at any time and location. It should be noted that access control technologies are shying away from network-based systems due to limited flexibility. Mandatory access has a set of security policies constrained to system classification, configuration, and authentication. It defines and ensures centralized enforcement of confidential security policy parameters.

Discretionary Access Control is a type of access control system where an IT administrator or business owner decides on the access rights for a person for certain locations physically or digitally. DAC is less secure compared to other systems, as it gives complete control to the end-user over any object they own, and programs associated with it.

As the name suggests, a role-based access control system is when an administrator doesn’t have to allocate rights to an individual but gets auto-assigned based on the job role of that individual in the organization. So, it’s clear. The administrator has less to do with policy making” (Dhote, 2020).

**Justification of Maintenance Plan**:

“New security measures and policies do nothing if employees working with the data are not educated on how to minimize risk. Any time an element of your security program changes, your employees need to be aware. And be sure to document and retain evidence of trainings for future auditing purposes” (Barr Advisory, 2022). Without training employees on the company’s information assurance plan, it is effectively neutralized. Employees from the top level of management to the bottom level employees all need to know their role in establishing and maintaining information assurance. By doing this, the plan is kept as effective as possible by ensuring everyone in the company is playing their part.

“The best way to determine the effectiveness of your information security program is to hire a third-party auditor to offer an unbiased assessment on security gaps. In some cases, this is mandatory to confirm compliance. Third-party assessors can also perform vulnerability assessments, which include penetration tests to identify weaknesses in your organization’s networks, systems, and applications, along with audits against criteria such as ISO 27001, PCI DSS, FedRAMP, and HITRUST; as well as SOC 2® reports using the AICPA Trust Service Principles. Your company can also conduct internal audits to assess controls, policies, procedures, risk management, and more” (Barr Advisory, 2022).

# References

*Data security: barriers to success*. (2017, April 6). Retrieved from Grant Thorton: https://www.grantthornton.global/en/insights/cybersecurity/value-of-data-hub/data-security-barriers-to-success/

AWS. (2022). *Shared Responsibility Model*. Retrieved from Amazon Web Services: https://aws.amazon.com/compliance/shared-responsibility-model/

Barr Advisory. (2022). *How to Implement an Information Security Program in 9 Steps*. Retrieved from Barr Advisory: https://www.barradvisory.com/roadmap-to-implementing-a-successful-information-security-program/

Blanco, J. M. (2020, December 28). *Analysis of a Cyber Attack: Capital One*. Retrieved from Cipher: https://cipher.com/blog/analysis-cyber-attack-capital-one/

Boogaard, K. (2022, May 13). *What Is a Risk Matrix?* Retrieved from Wrike: https://www.wrike.com/blog/what-is-risk-matrix/#What-is-a-risk-assessment-matrix-in-project-management

Cooper, R. (2019, August 16). *Before Capital One breach, internal staff raised red flags* . Retrieved from Washington Business Journal: https://www.bizjournals.com/washington/news/2019/08/16/capital-one-staff-raised-red-flags-before-brea.html

Covert, E. (2021, August 28). *Case Study: AWS and Capital One*. Retrieved from System Weakness: https://systemweakness.com/case-study-aws-and-capital-one-c4ad6cb71c79

Cynet. (2022). *Incident Response*. Retrieved from Cynet: https://www.cynet.com/incident-response/#:~:text=The%20goal%20of%20incident%20response,attacks%20of%20the%20same%20type.

Cynet. (2022). *Incident Response SANS: The 6 Steps in Depth*. Retrieved from Cynet: https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/

Daniels, D. (2022, February 28). *What Is TLS 1.2, and Why Should You (Still) Care?* Retrieved from Gigamon: https://blog.gigamon.com/2021/07/14/what-is-tls-1-2-and-why-should-you-still-care/

Dhote, S. (2020, November 21). *3 Types of Access Control – Pros & Cons*. Retrieved from The Proche: https://www.theproche.com/2020/11/21/3-types-of-access-control-pros-cons/

Drake, A. (2020, February 3). *The 7-Minute Guide to Mirror Backup: What You Need to Know*. Retrieved from G2: https://www.g2.com/articles/mirror-backup#:~:text=Pros%20of%20mirror%20backup&text=Additionally%2C%20this%20backup%20method%20takes,to%20load%20the%20entire%20backup.

Ennis, D. (2020, May 4). *Capital One hires away Goldman’s CISO to help with breach response*. Retrieved from Banking Dive: https://www.bankingdive.com/news/capital-one-goldman-sachs-ciso-breach-Andy-Ozment/577286/

Evan, J. (n.d.). *Preventing The Capital One Breach*. Retrieved from EJJ: https://ejj.io/blog/capital-one

Harvey, S. (2019, November 8). *Lessons Learned from Capital One’s Incident Response Plan*. Retrieved from Kirkpatrick Price: https://kirkpatrickprice.com/blog/lessons-learned-from-capital-ones-incident-response/

*Information on the Capital One Cyber Incident*. (2022, April 22). Retrieved from Capital One: https://www.capitalone.com/digital/facts2019/

Kirk, J. (2019, July 31). *Capital One: Where Did the Bank Fail on Defense?* Retrieved from Data Breach Today: https://www.databreachtoday.com/capital-one-where-did-bank-fail-on-defense-a-12858

Kost, E. (2022, May 12). *Top 12 Cybersecurity Regulations for Financial Services*. Retrieved from UpGuard: https://www.upguard.com/blog/cybersecurity-regulations-financial-industry

Kyndryl. (2022). *What Is a Disaster Recovery (DR) Plan?* Retrieved from Kyndryl: https://www.kyndryl.com/us/en/learn/disaster-recovery-plan

Lalloobhai, M. (2020, September 9). *The OCC Fines Capital One Bank for 2019 Cybersecurity Breach*. Retrieved from Weaver: https://weaver.com/blog/occ-fines-capital-one-bank-2019-cybersecurity-breach

Neto, N. N., Madnick, S., Paula, A. M., & Borges, N. M. (2020, March). *A Case Study of the Capital One Data Breach.* Retrieved from MIT Sloan: https://web.mit.edu/smadnick/www/wp/2020-16.pdf

Norwich University Online. (2018, July 2). *The 5 Pillars of Information Assurance*. Retrieved from Norwich University: https://online.norwich.edu/academic-programs/resources/the-5-pillars-of-information-assurance

Schinder, D. (2005, August 2). *Ethical issues for IT security professionals*. Retrieved from Computer World: https://www.computerworld.com/article/2557944/ethical-issues-for-it-security-professionals.html

SIA. (2022). *Open Supervised Device Protocol (OSDP)*. Retrieved from Security Industry Association: https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/

Yakencheck, J. (2019, August 19). *Lessons of the Capital One Data Breach*. Retrieved from Infosecurity Magazine: https://www.infosecurity-magazine.com/infosec/lessons-from-the-capital-one-data/