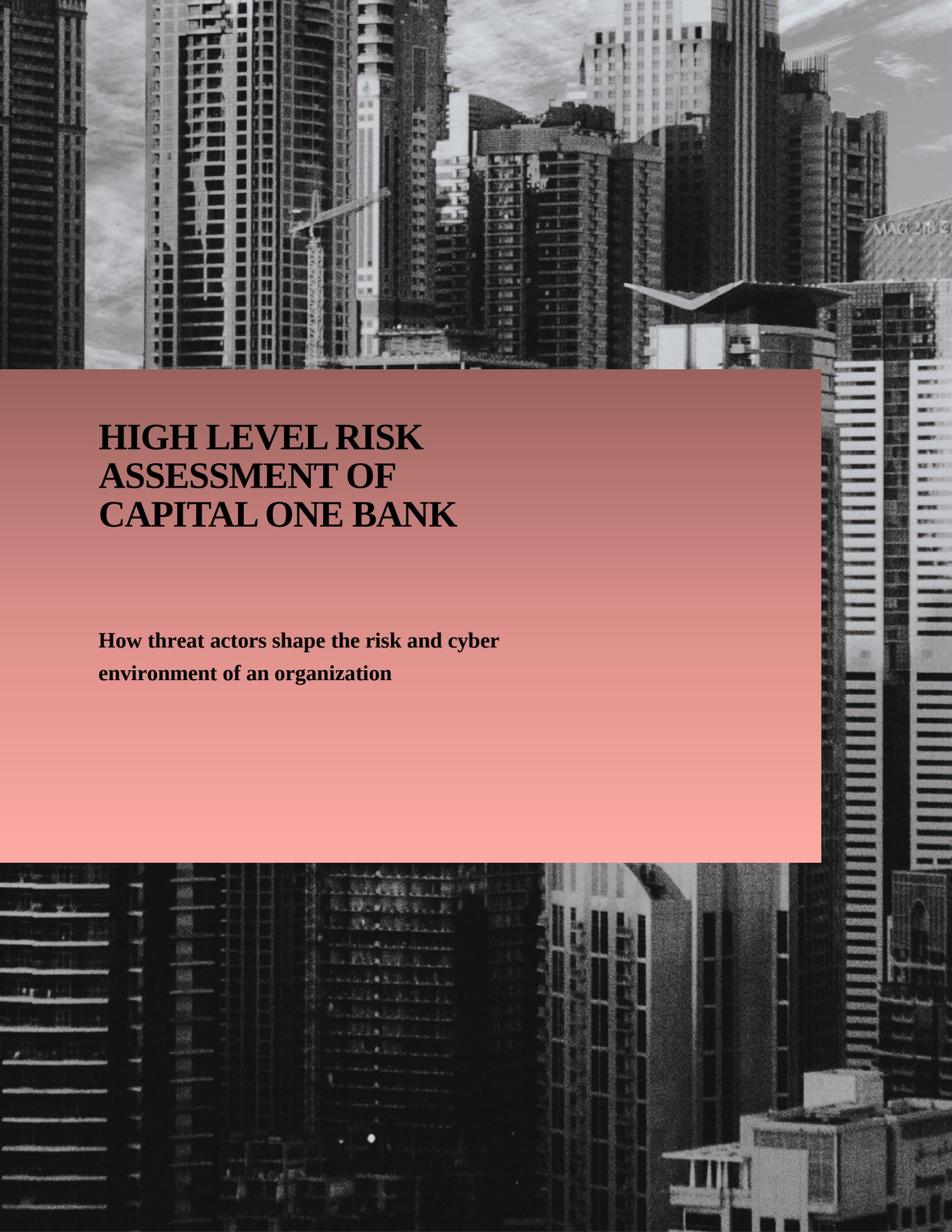

HIGH LEVEL RISK ASSESSMENT OF CAPITAL ONE BANK

How threat actors shape the risk and cyber environment of an organization

Executive Summary

In July 2019, Capital One Bank disclosed to the public that threat actors had gained access to customer data from it's AWS-hosted environment and exfiltrated about 106 million U.S and Canadian consumer PII information such as credit-card data and much more. Investigation and forensic analysis showed an application-layer access-control failure chain where server-side request forgery (SSRF) was exploited in a web component to gain access to an EC2 instance metadata service to obtain credentials for IAM roles that exposed the data of millions of consumers. In terms of risk posture, pre-incident there are confidentiality risks around API/WAF and trust boundaries, identity scoping for workloads, and exfiltration detection is under-mitigated [1], [2]. Our proposed risk assessment discloses these gaps in risk assessment using NIST framework, ISO 31000 and COBIT 2019 [3], [4] to close these vulnerabilities via API hardening, IMDSv2 enforcement, better IAM structure and detection engineering for abnormal access. Residual risks remain around token theft but are managed with phishing resistant MFA, continuous testing program and purple-team cycles.

Introduction

1.1 Purpose

To provide executives and risk committees with a clear, evidence based view of why the 2019 breach was possible and how to prevent such an event in the future. This report translates incident facts into a structured picture and is mapped to NIST CSF 2.0 and COBIT 2019, concluding with prioritized controls, KPIs, owners of risk on an individual level and a rollout plan for risk acceptance and mitigation. It is designed to support decisions on funding, timelines and overall risk posture of the company.

1.2 Scope

In scope: Customer PII hosted in cloud instances and the application stack; identity and access for human and non-human peripherals (IAM roles, tokens) [5]; platform/network boundaries (WAF, IMDS), monitoring and response (SIEMs) and third party API access [6].

Out of scope: Fraud operations and legal strategy and deep forensics beyond publicly available data; legacy platforms and shadow IT present in banking environment across branches [7]; PCI-DSS systems are not considered due to variance and lack of public data.

Timeline and Method: 90 day plan for containment, followed by phase 2 of hardening, and phase 3 of optimization, where a qualitative 5x5 risk matrix heat map and table shows explicit owners and KRIs.

Assumptions: All data is publicly available from the 2019 incident, where certification scope is not assumed to be equaled to full control effectiveness due to lack of implementation of certain steps and procedures.

Organization Background and Environments

2.1 Background

Capital One is a large U.S financial institution that offers retail banking, loans and other services to consumers. It operates under a cloud-centric posture using AWS and is supervised by the OCC and Federal Reserve [1], [2], so it is subject to sectoral and privacy/security obligations like GLBA Safeguards Rule [8] and FFIEC handbooks [9]. This creates strong expectations for risk management, incident response and overall data protection.

2.2 Risk Environment

Risk Drivers:

- High Value PII (SSNs, date of births with names, account numbers)
- Rapid Digital Delivery services (credit card infrastructure); large API footprint; ephemeral cloud credentials
- Complex IAM with human and non-human identities
- Low risk tolerance for PII compromise/regulatory breaches; low tolerance for long unavailability for customer facing services

2.3 Operational Environment

- People: Platform teams, Security engineers, third party vendors, etc.
- Processes: SDLC with CI/CD; risk assessments; incident response
- Technology: API gateways and WAF, EC2 instances, S3 data stores, IAM roles, SIEMs, Key Management Systems

2.4 Cyber Environment

Control Landscape (Pre-incident):

- **Identity and Access:** IAM; MFA for login; PAM for admin flows
- **App Security:** WAF front ends
- **Data Security:** Encryption at rest; data classification; tokenization used in instances; governance in API use

2.5 Regulatory Environment

- **GLBA Safeguards Rule (U.S):** Requires written information for security program, testing, risk assessment, and oversight of service providers [8]
- **Breach and Response Notifications**: multi-agency coordination and customer remediation
- **OCC/FRB supervisory expectations**: governance, issue management and board oversight [10]

Incident Synopsis

Public disclosure was on the 29th of July, with investigation dated March-July.

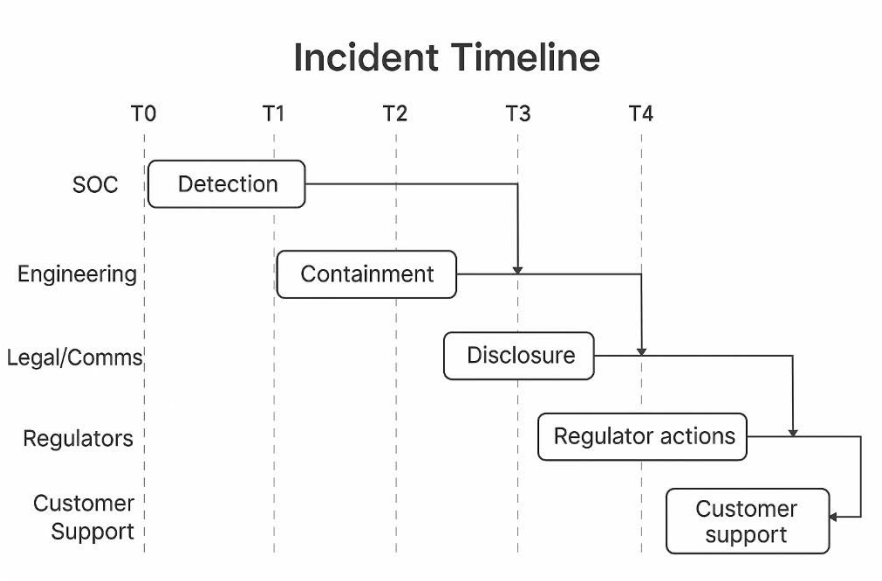

Figure 1: Incident Timeline

FBI arrest followed disclosure to the public where 106 million were affected, as well as 140k SSNs, 80k bank accounts, and more. The timeline is given in figure 1 and shows the steps taken until the public was made aware of the incident. The attack path is detailed in figure 2 and as follows:

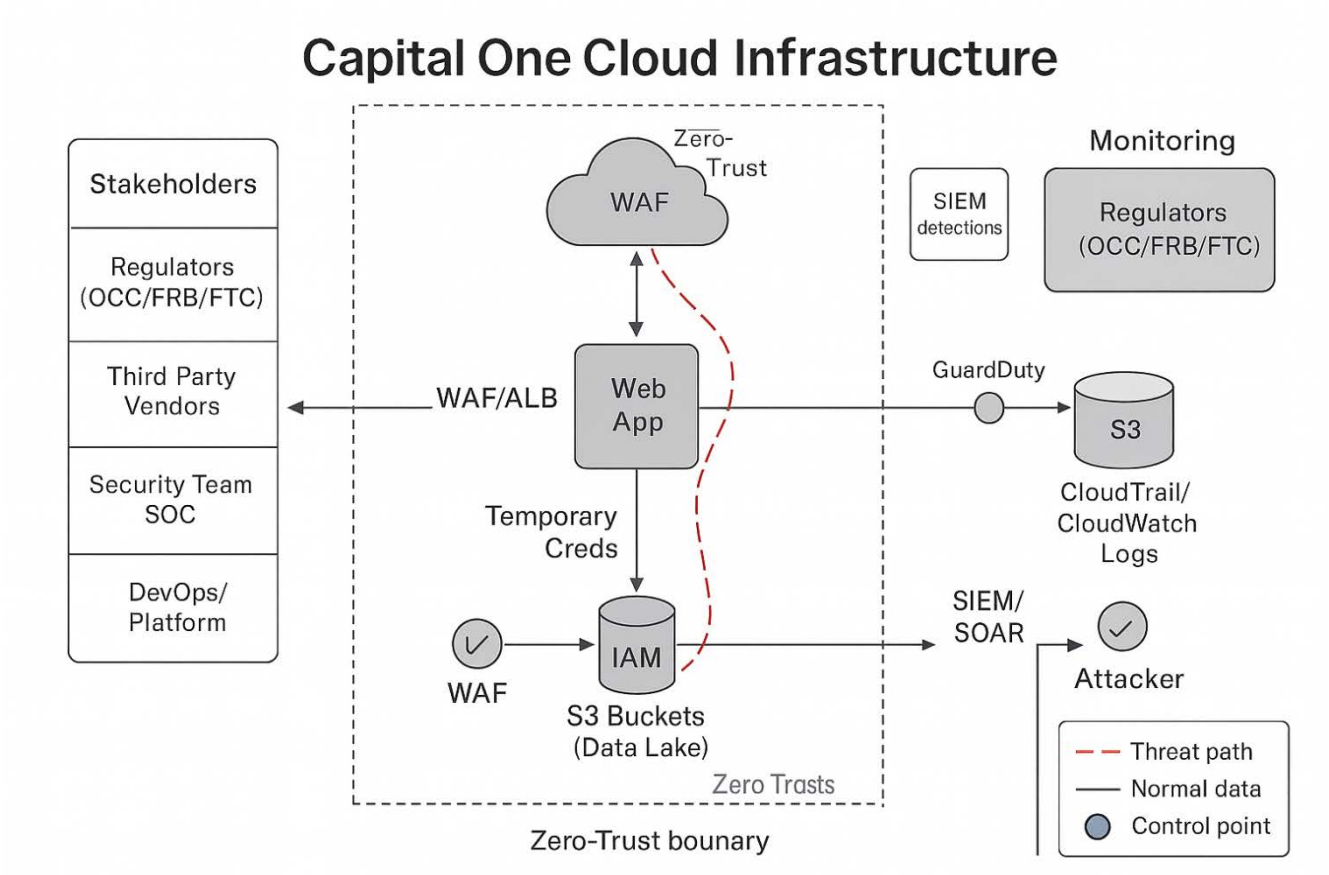

Figure 2: Capital One Cloud Infrastructure During Attack

- SSRF via misconfigured WAF rule allows internal HTTP calls
- Access to IMDSv1 returns role credentials for an EC2 role with S3 permissions
- Using those credentials, threat actors enumerate and read S3 buckets with credit-application data
- Exfiltration: later public tip offs accelerate containment and arrest

This attack worked due to over-permissive IAM on a workload role, insufficient detections for abnormal logins, and trust-boundary assumptions (WAF to IMDS).

Risk Assessment Methodology

4.1 Crown-Jewel Assets

Asset	**Description**	**Security objective (C.I.A triad)**	**Value/impact rationale**
Credit application data	PII/financial attributes; years of records	**C** very high; **I** high	Regulatory exposure, identity theft, reputational harm
Customer systems (CRM/BSS)	Identity and servicing platforms	**I** high; **C** high	Accuracy and trust in customer servicing
S3 data lakes & buckets	Structured/unstructured cloud stores	**C** very high; **A** high	Bulk data exfil potential
Workload identities (IAM roles)	Non-human roles & policies	**I** high	Trust fabric for services and automation
Telemetry (CloudTrail/ALB/WAF logs)	Detection & forensics data	**I** high; **A** high	Timely incident response & evidence chain

Table 1: Capital One Assets with Assessment for Security Posture

From the table 1 we see that Assets like credit card information and S3 data buckets both are extremely Confidential, with Integrity high for PII and Availability high for exfil-able data. Using the CIA triad, we can thus show what assets would be most likely targeted by threat actors. For more info, on CIA triad, refer to figure 3, [11] and [12].

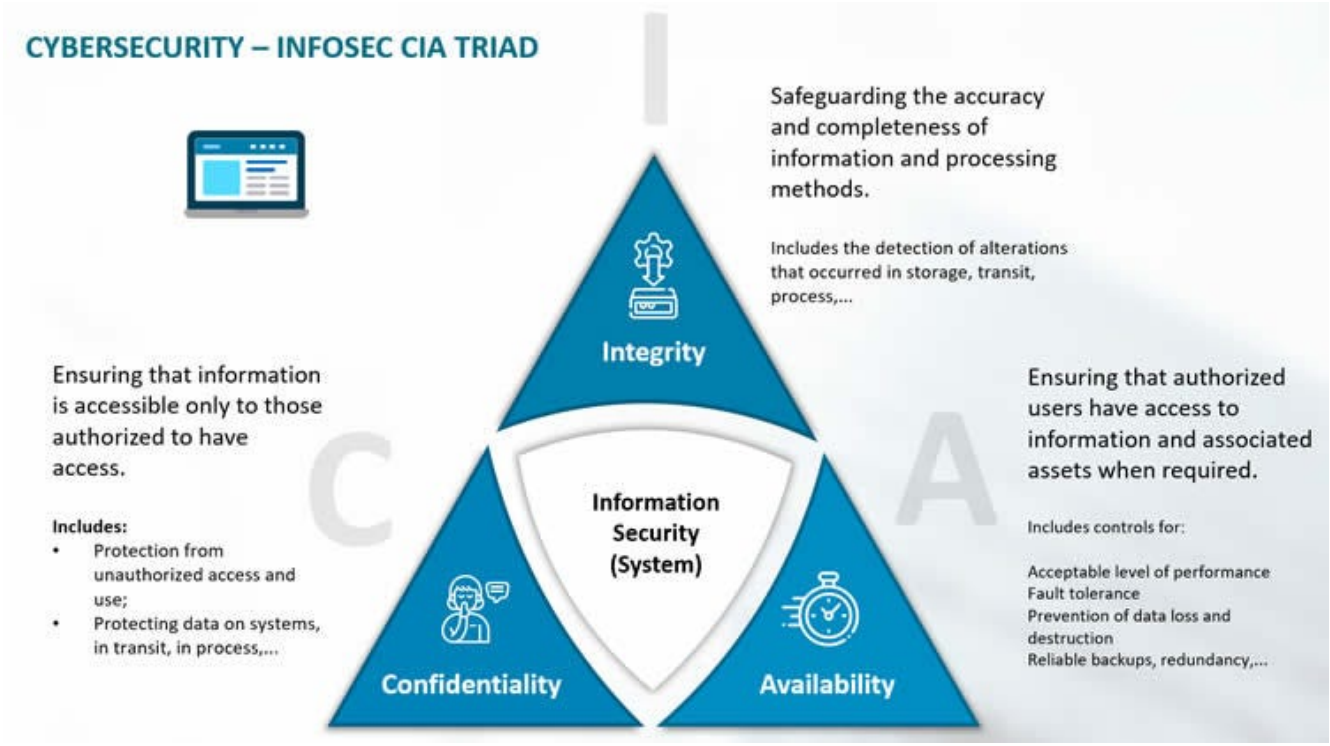

Figure 3: CIA Triad Illustrated

4.2 System Threats

Threat	Vector	Actor	Primary effect
SSRF & broken access control	App-layer forged/internal requests	External opportunistic	Role credential theft → data reads
Credential theft (tokens/keys)	Metadata exposure; leaked keys	External or insider	Privilege misuse
Misconfiguration drift	Rapid delivery; IaC gaps	Internal accident	Latent exposure
Insider misuse	Excess entitlements	Malicious/negligent insider	Unauthorized bulk access
Data exfiltration	Large S3/API responses	External	Confidentiality loss

Table 2: Capital One Threats with Assessment for Security Posture

From table 2 we see that threats determine the vector of approach and have an effect on whether it favors external/internal threat actor to exploit, and also what exploitation can cause for the overall security environment of Capital One.

4.3 System Vulnerabilities (Pre-incident)

Vulnerability	Category	Representative weakness	Likelihood	Impact
IMDSv1 exposure behind WAF	Cloud platform	Metadata reachable via SSRF	Likely	Severe
Over-permissive IAM role	Identity	Wildcard List/Get on S3 paths	Possible	Major
WAF rule misconfiguration	App security	Insufficient input validation	Likely	Major
Detection blind spot	Monitoring	No high-fidelity rules for abnormal S3 listings	Possible	Major
Data egress governance gaps	Data	No caps/redaction/DLP on bulk responses	Possible	Major

Table 3: Capital One Vulnerabilities with Assessment for Security Posture

From table 3 we can calculate Risk=Likelihood x Impact to find Risk of certain vulnerabilities on assets and how threat actors can exploit them [13]. More on this in our heat map and risk matrix in the following sections.

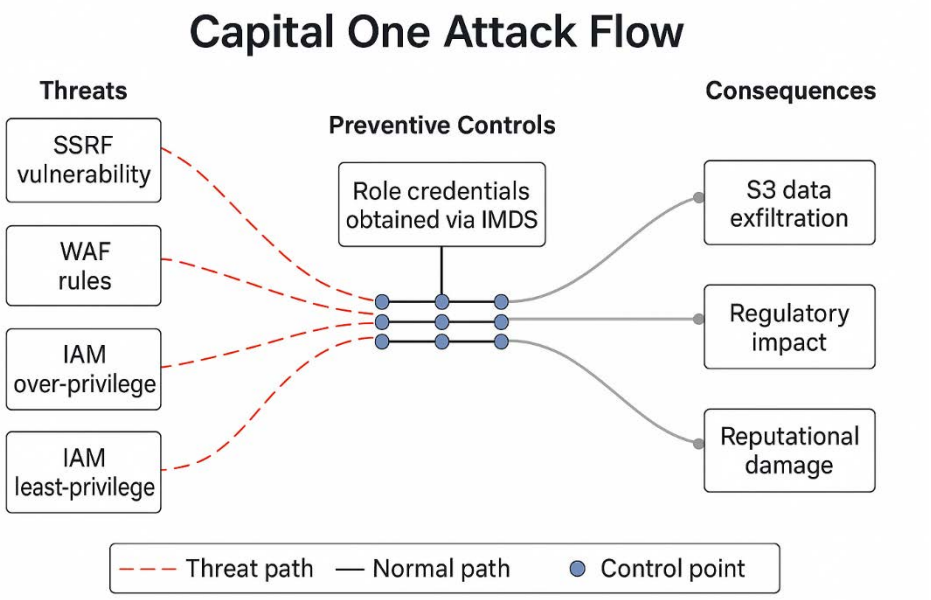

Figure 4: Capital One 2019 Breach Attack Flow

Remediation

5.1 Current Controls (Pre-incident)

Domain	Typical state	Strength	Weakness
Identity & Access	IAM roles for workloads; MFA for humans	Cloud-native identity primitives	Role policies not fully least-privilege; machine identities not in PAM
Perimeter/App Security	WAF fronting web apps	Commodity protection vs OWASP Top 10	SSRF path not blocked; rule misconfiguration possible
Data Security	Encryption at rest/in transit; tokenization used	Baseline cryptography	Tokenization uneven; S3 access patterns not strictly governed
Monitoring	SIEM + cloud logs; EDR/NDR	Telemetry existed	Detections weak for “legit credentials doing odd things”
SDLC	CI/CD pipelines; change management	Speed & automation	Security gates inconsistent across teams/services

Table 4: Capital One Existing Controls Pre-incident

We also note that since Capital One is a U.S entity, it is mainly governed and has obligations to GLBA, OCC supervision, so adherence to certifications such as ISO 31000 may exist but governance/control scope does not mean consumer facing workloads are implemented as such, so we use an evidence based assumption for what is in place in the organization [3], [8].

5.2 Gap analysis & control objectives (NIST CSF 2.0 ↔ COBIT 2019 ↔ CIS v8)

Objective	Standard mapping	Current (2019)	Target	Gap	Priority	Quick wins
Shut SSRF paths to IMDS	**CSF PR.PS; CIS 12**	IMDSv1 accessible if SSRF	IMDSv2; hop-limit; WAF/ALB SSRF rules	High	**P1**	Block 169.254.169.254; SSRF signatures
Tighten IAM for workloads	**CSF PR.AA; CIS 6**	Broad S3 rights on role	Least privilege; resource-level policies; SCP guardrails	High	**P1**	Remove *:*; scope paths; deny exfil APIs
Detect abnormal S3 use	**CSF DE.CM/DE.AE; CIS 8**	Blind to legit-looking abuse	UEBA: list-then-get patterns; byte thresholds; odd geos	High	**P1**	GuardDuty/SIEM rules; auto-quarantine role
Govern API/WAF configs	**COBIT BAI03/06; CSF PR.PS**	Inconsistent across services	Central rule library; IaC policy-as-code gates	Medium	**P2**	OPA/Conftest in CI; approval gates
Egress/DLP on data APIs	**CSF PR.DS; CIS 13**	Large responses possible	Caps/redaction/tokenization; allow-lists	Medium	**P2**	Gateway plugin; response size/row limits
Assurance metrics & KRIs	**CSF GV.RR; COBIT MEA01**	Reactive metrics	Board KRIs; control attestation cadence	Medium	**P3**	% roles w/ IMDSv2; S3 policy drift; MTTD/MTTR

Table 5: Capital One Gap Analysis [3], [4], [14]

The GAP table ties each vulnerability from the incident to a specific NIST CSF category, COBIT objective, and CIS v8 control, then ranks what to fix. The P1 priorities are to lock down API access and build a single API registry so shadow endpoints do not work, enforce SDLC security gates that block

bad WAF/IEM patterns, and add detection engineering to S3 buckets. P2 strengthens data-egress and P3 adds governance and KRIs for program capability attestation.

5.3 Control Analysis for Different Frameworks

NIST CSF 2.0	COBIT 2019	CIS v8	Practical measure
GV.RR Risk governance	EDM03, APO12	17 (IR)	Risk appetite for data exfil; KRI pack
ID.AM Asset management	APO03, BAI09	1 (Asset inventory)	Cloud asset/role inventory; API registry
PR.AA Identity & access	DSS05	5/6 (Acct & Access Management)	Least privilege IAM; short-lived creds
PR.PS Platform security	BAI03/06	12 (Network)	IMDS hardening; SSRF controls; micro-seg
PR.DS Data security	DSS06, BAI10	3 (Data protection), 13 (DLP)	Egress caps & tokenization
DE.CM/DE.AE Monitoring	MEA01, DSS05	8 (Audit logs), 7 (CEM)	UEBA for S3/API patterns
RS.MI/RS.CO Response	DSS02	17 (IR)	SOAR playbooks; customer comms
RC.RP/RC.IM Recovery	DSS04	11 (Recovery)	Restore drills; lessons learned

Table 6: Capital One Control Implementation Analysis [3], [4], [14]

In table 6 we see how each NIST CSF 2.0 capability lines up with the closest COBIT 2019 process and practical CIS v8 controls, so we can know which department owns it and is responsible. This is ‘map’ that turns framework language into concrete controls that will be used as audit-ready evidence. Implementation of organizational, people, physical and technological controls require cross -framework investigation so that control implementation adheres to regulatory requirements and compliance requirements for the country as well as alignment with company policies for cyber defense in depth.

5.4 Control Objectives – Justification, Design and Evidence

Control objective	Why now (risk)	Standards	Effect on risk	Proof (tests/metrics)
API authN/Z + mTLS + rate limits	Blocks bulk reads on public/partner APIs (R1,R2)	CSF PR.AA/PR.PS; COBIT DSS05/BAI03; CIS 6/12	L ↓ Likely→Unlikely; I capped	100% OAuth2+mTLS; rate-limit trends; gateway config & pen-test
IMDS hardening + SSRF rules	Breaks SSRF→IMDS path (R1)	CSF PR.PS; COBIT BAI03; CIS 12	L ↓ Likely→Unlikely	100% IMDSv2; WAF blocks 169.254.*; red-team blocked
Least-privilege IAM + SCPs	Removes over-broad S3 access (R2)	CSF PR.AA; COBIT DSS05; CIS 5/6	L ↓ Possible→Rare; I ↓ Severe→Major	0 wildcards; scoped policies; drift report
Detection engineering + SOAR	Finds “legit creds, odd behavior” (R3)	CSF DE.CM/DE.AE; COBIT MEA01; CIS 7/8	Dwell time ↓; Residual manageable	MTTD≤10m, MTTR≤60m; purple-team catch-rate
Egress caps/redaction/DLP	Limits payload volume/sensitivity (R4)	CSF PR.DS; COBIT DSS06/BAI10; CIS 3/13	I ↓ Severe→Major	% endpoints with caps/redaction=100 %; DLP stats
API registry + policy-as-code	Prevents shadow APIs & bad configs (R2,R3)	CSF ID.AM/PR.PS; COBIT BAI06; CIS 16	L ↓ across multiple risks	100% builds pass; 0 unregistered APIs

Table 7: Capital One Control Implementation Analysis on Risk [3], [4], [14]

The gap table 7 links major risk to a specific control objective (P1, P2, P3) and its best practice control anchors where we show how Likelihood & Impact decreases upon implementation of certain controls and quick wins that result from them. This is so to show how our analysis is systematic, justified and auditable against recognized standards.

5.5 Remediation Plan Rollout

P1 (0-90 days): Close the Breach

- IMDSv2 everywhere, set metadata response limit [16]
- IAM least privilege sprint for all workloads that works with PII, deny data-exfil APIs, add service control policies (SCPs)
- SSRF protections with WAF rules for SSRF signatures, block HTTP ranges and data egress policies
- Detection Engineering Implementation with high fidelity SIEM rules for S3 buckets, auto revoke role sessions with SOAR [6], [17]
- Crisis comms aligned to regulators with credit and identity protection

P2 (90-180 days): Build Guardrails

- Policy-as-code in CI/CD and deploy block on IAM anti-patterns
- Implement API gateway plugins for response size caps for high risk identifiers and data egress governance
- PAM for non-human entities with short-lived credentials for CI/CD services
- Zero-trust segmentation for endpoint protection
- Quarterly control attestation with KRI metric dashboard and internal audit against COBIT objectives

P3 (180-360 days): Optimize and Evidence

- Purple-team API exfil for adversary simulations to check if control implementation works
- Contractual cyber clauses to renew vendors to add adjustments to cyber and risk environment as needed
- Publish control coverage metrics and external ISO 31000 certification adherence to demonstrate governance maturity

Risk Assessment – before vs after

6.1 Top Risks

ID	Risk statement	Inherent L	Inherent I	Inherent level
R1	SSRF→IMDS yields role creds, enabling bulk S3 reads	Likely	Severe	Extreme
R2	Over-permissive IAM role enables broad data access	Possible	Major	High
R3	Abnormal S3/API reads evade detection & triage	Possible	Major	High
R4	Uncontrolled egress returns large sensitive payloads	Possible	Severe	Extreme
R5	Insider misuse of service creds	Possible	Major	High

Table 8: Capital One Risks Before Incident

Proposed controls	Residual L	Residual I	Residual level	Owner
IMDS hardening; SSRF rules; least privilege; detections	Unlikely	Major	Moderate	CISO
Resource-scoped policies; SCPs; CI gates	Rare	Major	Low	Identity Lead
UEBA rules; SOAR auto-contain	Unlikely	Major	Moderate	SecOps Manager
Egress caps; redaction; tokenization	Unlikely	Major	Moderate	Data Sec Lead
Brokered short-lived creds; PAM;	Unlikely	Major	Moderate	TPRM Lead

Table 9: Capital One Risks After Control Implementation

Table 8 and 9 above shows the five board-level risks with owners before/after ratings so we can see the impact our controls have on risk, likelihood and impact. R1 is the driver, where risk drops from extreme to moderate with IMDS hardening and other control implementations. R2 falls to low with least-privilege policies, with R3-R5 each moving from high/extreme to moderate after P1-P2 remediation plan rollout. The table also assigns the owners accountable for each risk such as CISO for R1, TPRM lead for R5 and so on, which makes remediation auditable, and time bound.

6.2 Heat Map (Qualitative)

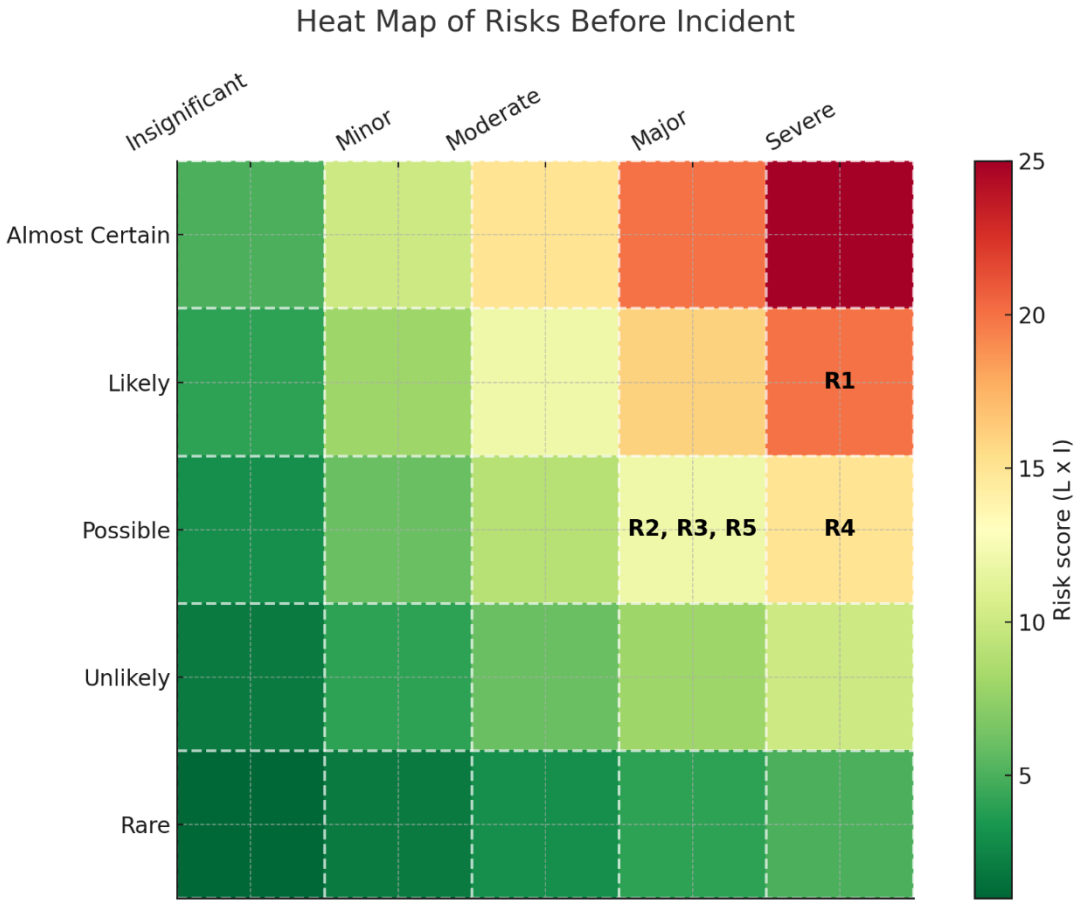

Figure 5: Heat Map of Risk Before Incident (L x I)

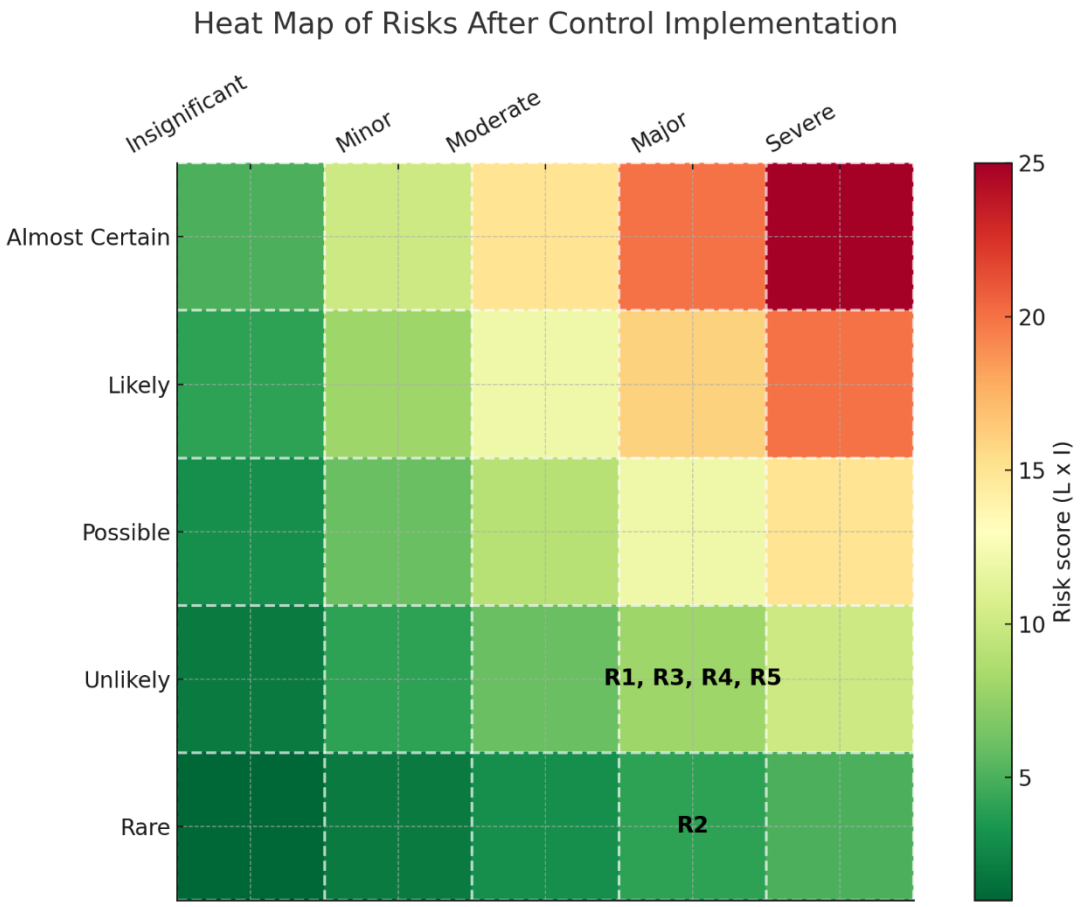

Figure 6: Heat Map of Risk After Control Implementation (L x I)

6.3 Risk Assessment of Results and Residual Risk Analysis

From the Heat Maps in figures 5 and 6 and table 8 we see that before Risk was very high for each vulnerability where Inherent Likelihood of exploitation was either likely or possible with impact being major or severe for the organization, so Risk = L x I which gave inherent risk as Extreme or High depending on R1-R5 risks [13], [15], [20]. After implementation of P1 and P2 controls we see that the cluster for R1-R5 moves to the bottom of the heat map showing dramatic decrease in likelihood of unwanted incident occurring, with the biggest movement comes from hardening the credential-theft path with IMDSv2 + SSRF controls. This hasn't decreased the impact of such an event much, only 1 or 2 stages from possible to unlikely or rare due to the residual impact such an event can cause for the organization as PII information is a very sensitive asset. But we see that overall Residual risk is greatly diminished to Moderate or low for R1-R5. This is because:

- R1 – Drivers were IMDSv2 enforcement and WAF SSRF signatures that block metadata hop and least-privilege IAM prevents broad listings, which reduced residual risk to moderate from an inherent risk of extreme
- R2 – Drivers were resource-level S3 policies, SCP guardrails, CI policy-as-code blocks risky changes which changes residual risk to low from an inherent risk of high
- R3 – Drivers were SOAR auto-contains anomalous data egress to detect data exfils, which reduces residual risk to moderate from an inherent risk of high
- R4 – Drivers were tokenization for high risk data identifiers which also helped uncontrolled S3 bucket data egress and detection blind spots which reduces residual risk to moderate from an inherent risk of extreme
- R5 – Drivers were short-lived credentials and per-vendor policy scopes to reduce insider misuse which decreases residual risk to moderate from an inherent risk of high

Residual risk exposure we must still manage include:

- Session hijacks via advanced techniques – mitigate this risk by continuous tokenization of high risk assets and CI hardening [18]
- Novel API flaws – mitigate this risk by employing a dedicated purple team, bug bounty programs and more
- Covert exfil – mitigate this risk with honey pots in system, high-order analytics and periodic scenario tests

We also have metrics for guardrails for risk acceptance (KRIs):

- IMDSv2 coverage is 100% with IAM roles with resource policies, OAuth/WAF policy-as-code implementation being complete across all data servers
- MTTD for abnormal S3 patterns < 10 minutes with containment scenario being done under 60 minutes [19]
- DLP/egress cap blocks trends downward during periodic scenario risk assessment

With all these conditions monitored, residual risk is within appetite and breaches of any KRI threshold that we detailed require immediate escalation to the board risk committee and their respective risk owners. And since risk is within moderate range, residual risk is accepted with monitoring only needed with adherence to management of periodic quarterly purple team tests on KRI thresholds.

6.4 Why the proposed program would have likely avoided the breach

As detailed by our control methods, we can say that the incident would not have taken place as:

- IMDSv2 + SSRF controls would have blocked or frustrated the credential-theft path as referred to in previous tables with additional hurdles like identity and metadata hoping would also make the threat actor and attack path nullified
- Least-privilege IAM + SCPs would have reduced the continuous privilege escalation that occurred once one account was compromised so would cancel out lateral movement paths
- Detection engineering would have flagged abnormal S3 access patterns swiftly which would cut off access automatically and reduced time threat actors are in the system (if any are in system that is)
- Data egress caps and tokenization would have limited volume of data exfiltration in the event an authorization bypass occurs so a system compromise would not make asset compromised
- Policy-as-code gates would have stopped misconfigured WAF/IAM patterns from deploying to production phase in the first place

We also conclude that these measures taken directly to target the vulnerabilities and defense failures align with regulatory expectations and laws that are safeguarded under GLBA and supervisory guidance (more on GLBA in the figure 7 below and [8]).

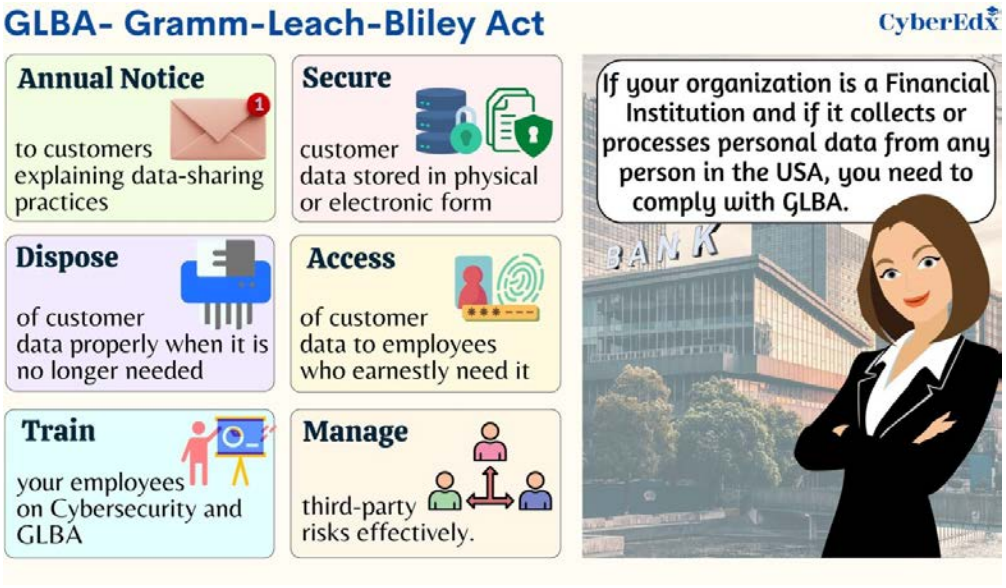

Figure 7: Graham-Leach-Bliley Act that Capital One is compliant to

6.5 Implementation Roadmap and RACI

Workstream	R	A	C	I
IMDS hardening + SSRF controls	Platform Engineer	CISO	App Owners	Compliance
IAM least-privilege & SCPs	Identity Engineer	CTO	Security Architect	Internal Audit
Detection engineering & SOAR	SecOps	CISO	Data Security	MDR/Vendors
Egress caps & tokenization	Data Security	CISO	Network	Legal/Privacy
Policy-as-code in CI	Developers/Platform	CTO	Dev Leads, Security Architect	PMO
Supplier access reforms	Vendor Manager	CFO	Legal, Security	Suppliers

Table 8: Capital One Control RACI Table

Finally, our report would like to illustrate specific owners of control implementations whether it is organizational, people, technological or more. RACI is Responsible Accountable Consulted and Informed [20], and in table 8 we detailed which owners are a part of each category for each control workstream that must be implemented to manage risk. This matrix ties each control objective to a named owner and escalation path which streamlines decision making and adherence to compliance which gives auditors evidence of governance discipline as detailed in NIST CSF 2.0 and COBIT 2019 framework.

Conclusion

In summary, this report goes through public sources about the 2019 cloud breach incident of Capital One bank and provides a clear risk picture across business, operational, cyber and regulatory environments, then identifies top drivers of risk, maps them to specific aligned control objectives that are technological, organizational, people and more and forms a remediation plan (P1, P2, P3) that targets the exact failure modes. The plan includes deployment of solutions such as API hardening, IMDSv2/SSRF deployment, least-privilege IAM guardrails, detection engineering with SOAR and data-egress controls; all of which

are explicitly linked to NIST CSF 2.0, COBIT 2019 and CIS v8 with a RACI table assigning accountable owners for all risks and control implementations.

Implementing these controls moves risk posture from inherent extreme/high to residual moderate/low risks with session hijacking, novel API logic flaws and covert data exfiltration being residual risks that have to be actively monitored and governed by KRIs, purple-team tests and policy-as-code gates. This systematic analysis is built on an evidence-based structure with coverage metrics, MTTD/MTTR targets with clear justification and alignment to best practices, all while adhering to regulatory and compliance requirements. The detailed controls would have prevented the breach and contained any lateral spread and would have provided a defense that on paper has created a defensible basis for risk acceptance with defined thresholds.

References

1. Novaes Neto, N., Madnick, S., Moraes G de Paula, A., & Malara Borges, N. (2020). A case study of the capital one data breach. *Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha, A Case Study of the Capital One Data Breach (January 1, 2020)*.
2. Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the capital one data breach: Critical lessons learned. *ACM Transactions on Privacy and Security*, *26*(1), 1-29.
3. Efe, A. (2023). A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. *Denetim ve Güvence Hizmetleri Dergisi*, *3*(2), 185-205.
4. Fadya, M., & Utama, D. N. (2025). Towards Secure Information Systems: Developing and Implementing an Information Security Evaluation Model Using NIST CSF and COBIT 2019. *TEM Journal*, *14*(1), 182.
5. Desai, P., & Hamid, T. (2021). Best Practices for Securing Financial Data and PII in Public Cloud. *International Journal of Computer Applications*, *975*, 8887.
6. Rahmawati, T., Shiddiq, R. W., Sumpena, M. R., Setiawan, S., Karna, N., & Hertiana, S. N. (2023, November). Web Application Firewall Using Proxy and Security Information and Event Management (SIEM) for OWASP Cyber Attack Detection. In *2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)* (pp. 280-285). IEEE.
7. Silic, M., & Back, A. (2014). Shadow IT–A view from behind the curtain. *Computers & Security*, *45*, 274-283.
8. Pepper, D., Ross, S. L., Diamond, E., & US, N. R. F. (2024). Gramm-Leach-Bliley Act (GLBA) Privacy & Data Security.
9. Pinckard, J. L., Rattigan, M., & Vrtis, R. A. (2016). *A Mapping of the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) to the Cyber Resilience Review (CRR)* (No. CMUSEI2016TN008).

10. Griffin, N. (2023). Federal Reserve And OCC Release 2023 Bank Stress Test Scenarios. *Mondaq Business Briefing*, NA-NA.
11. Mohanty, S., Ganguly, M., & Pattnaik, P. K. (2018). CIA triad for achieving accountability in cloud computing environment. *International Journal of Computer Science and Mobile Applications*, *6*(3), 38-43.
12. Yee, C. K., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, *8*(2), 34-42.
13. Enyoghasi, C., & Badurdeen, F. (2022). Evaluating Performance of a Product Design: Risk Identification for Likelihood and Impact Analyses. In *IISE Annual Conference. Proceedings* (pp. 1-6). Institute of Industrial and Systems Engineers (IISE).
14. Bashofi, I., & Salman, M. (2022, June). Cybersecurity maturity assessment design using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. In *2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)* (pp. 58-62). IEEE.
15. Goodman, C. (2019, November 27). Risk Heat Map – A Powerful Visualization Tool. Balbix. https://www.balbix.com/insights/cyber-risk-heat-map/
16. BALAKRISHNA, B. (2023). SECURING AWS EC2: STREAMLINING IMDS TRANSITION FROM THIRD-PARTY IMDSV1 CALLS TO IMDSV2 WITH PROXY SERVER INTEGRATION. *INTERNATIONAL JOURNAL*, *12*(11), 2158-2163.
17. Yeboah, F. A. (2024). *Detecting and Safeguarding Against Cybersecurity Attacks Targeting Wireless Networks: A Comprehensive Approach to Integrate IDS/IPS, SIEM and SOAR* (Master's thesis, University of Cincinnati).
18. Jain, V., Sahu, D. R., & Tomar, D. S. (2015, February). Session hijacking: threat analysis and countermeasures. In *Int. Conf. on Futuristic Trends in Computational Analysis and Knowledge Management*.
19. Dahlberg, G. (2025). Exploring Incident Management: A Comparative Study of Splunk Enterprise, Graylog Open and Syslog-ng and their Impact on Mean Time to Resolution (MTTR).
20. Hartono, Y., Cahyo, W. N., & Immawan, T. (2024). The Assignment of Risk Mitigation Tasks Based on The RACI Matrix and Key Risk Indicator. *Jurnal Ilmiah Teknik Industri*, 235-244.