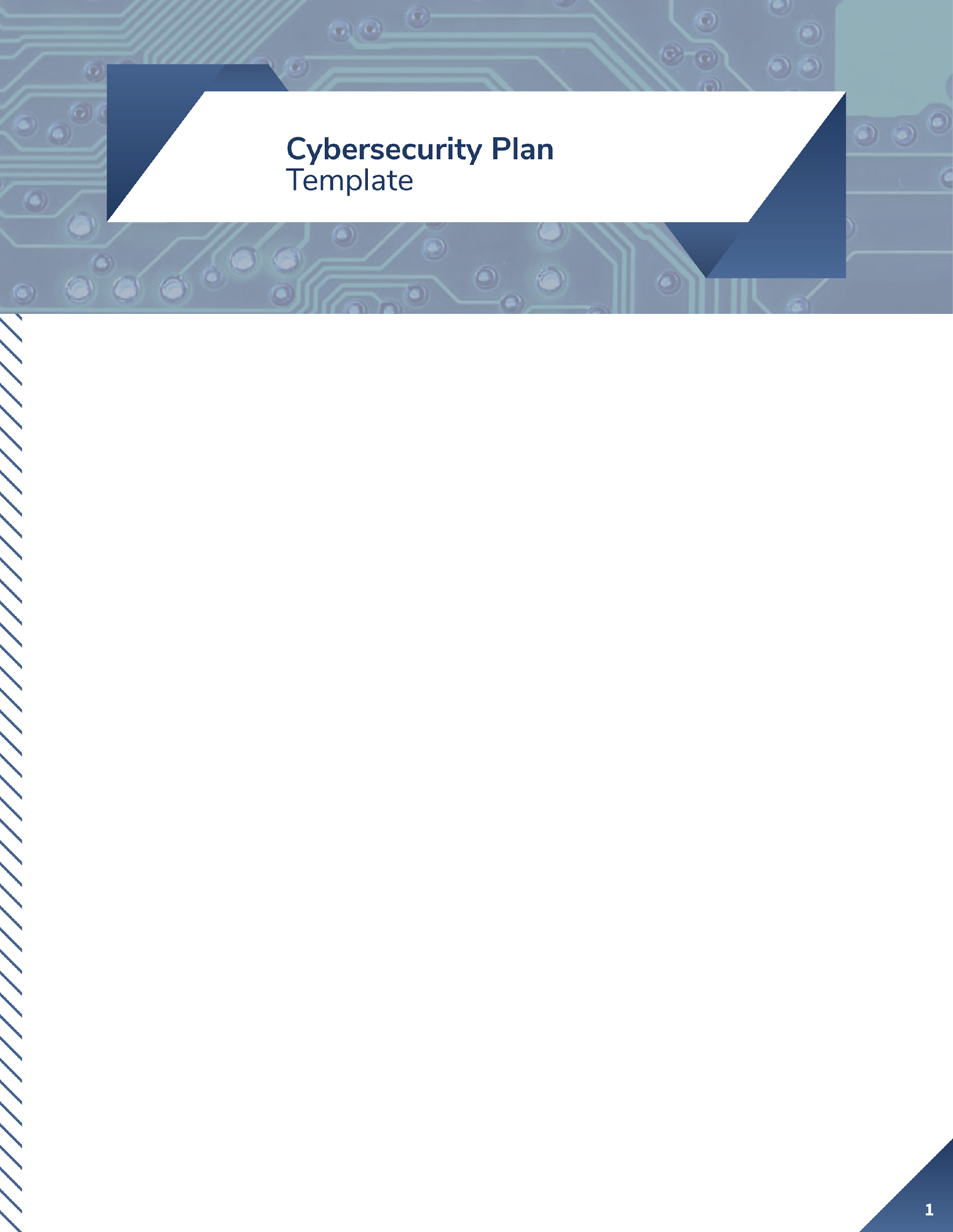
**Purpose**

The primary purpose of this cybersecurity plan is to safeguard Target’s customers, partners, and operational data by ensuring the protection and integrity of all information and systems. After the 2013 data breach that compromised 98 million customers' data, Target recognizes the critical importance of cybersecurity in protecting sensitive data and maintaining trust with its stakeholders. This plan will serve as a comprehensive approach to managing cybersecurity risks, outlining roles, policies, and procedures to proactively protect Target's systems, data, and network from threats while responding effectively to potential cybersecurity incidents.

By establishing this cybersecurity plan, Target affirms its commitment to fortifying its security posture and ensuring compliance with industry standards, such as the Payment Card Industry Data Security Standard (PCI-DSS) and other relevant regulations. The plan’s execution will be an essential part of Target’s efforts to demonstrate to customers, shareholders, and regulators that their data is handled with the utmost security.

**Scope**

This cybersecurity policy applies to all employees, contractors, and third-party vendors who access Target’s systems, networks, and data. The scope of this policy covers the following:

**Who**: All personnel with access to Target's systems, including employees, contractors, and vendors.

**What**: The policy applies to all information systems, including point-of-sale (POS) systems, customer databases, e-commerce platforms, and internal corporate networks.

**When**: This policy is in effect at all times, regardless of the employee’s location, whether they are accessing systems remotely or on-site.

**Where**: It applies to all of Target’s locations, whether physical stores or corporate offices, and to employees accessing data and systems from remote locations.

**Exceptions**: Any exceptions to this policy must be approved by the Chief Information Security Officer (CISO). This includes emergency situations where policy deviations may be necessary to address critical business operations or emerging threats.

**Plan Framework**

Target Corporation will adopt the NIST Cybersecurity Framework (CSF) as the foundation of this cybersecurity plan. The NIST CSF is widely recognized for its comprehensive structure, offering a solid foundation to improve security practices and manage cybersecurity risks effectively. By leveraging this framework, Target can ensure that its cybersecurity policies are aligned with best practices in risk management and resilience-building.

Target will focus on the five Core Functions of the NIST CSF, selecting subcategories most relevant to addressing vulnerabilities revealed by the 2013 data breach.

**Core Functions and Subcategories**

# 1. Identify

The identification function is important for understanding the context and risks within the organization, including the organization's assets, business environment, and risk management strategy. In the case of the 2013 target breach, multiple identification builds may have helped prevent or mitigate the attack.

Asset Management: target failed to properly manage access to third-party vendors, and HVAC vendors had access to some of target's network resources, but security controls were inadequate.

Lesson: It is critical to manage assets comprehensively and monitor all devices that interact with your company's network.

Best practice: Do a thorough inventory of all network fields and users to determine who has access to their systems.

Risk management: Inadequate risk assessment of third-party access. An attacker could use a vendor's leaked commentary to attack target's network.

The lesson: Risk assessments and security testing of supplier systems should be conducted regularly, and more stringent security requirements should be imposed on external partners.

Best practice: Conduct an ongoing risk assessment of third-party partners for vulnerabilities in systems you screen connected to internal networks.

Governance: Lack of oversight and clear cybersecurity governance is evident in target's failure to implement proper network segmentation and internal security controls to quickly detect and respond to attacks.

The lesson: It is critical to put cybersecurity governance in line with optimal timing and to include strict network traffic and city-wide monitoring policies.

Best practices: Establish a cybersecurity governance framework with clear roles and responsibilities, and ensure senior management is held accountable for security policy.

Target did not effectively manage the access rights of third-party suppliers, especially the HVAC supplier, which had the right to access some network resources. Due to inadequate security measures, attackers could gain access to the company's network through these channels. The supplier should keep a record of all devices and a list of users and systems, and clarify the purpose and access rights of each system. Used to protect user data and network security. At the same time, it is necessary to regularly check and update the access rights of third parties to ensure that only the required resources can be accessed, so as to improve user data security.

**Reference:**

National Institute of Standards and Technology (NIST). (2018). **Framework for Improving Critical Infrastructure Cybersecurity** (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Ponemon Institute. (2014). **2014 Cost of Data Breach Study: Global Analysis**. IBM Security. https://www.ibm.com/security/data-breach

National Institute of Standards and Technology (NIST). (2016). **NIST Special Publication 800-171 Rev. 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**. https://doi.org/10.6028/NIST.SP.800-171r1

# 2. Protect

Protection features take measures to protect critical systems, detect instrument activity and reduce the impact of potential security incidents. Access control: The target breach occurred with varying access controls, especially by revealing the credentials of third-party vendors, allowing attackers to easily access payment systems within the network.

Lesson: Implementing stronger access controls and minimum integrity principles can effectively prevent data breaches

Best practice: Require multi-factor authentication for all internal and third party access to relational systems, and are network segmentation, ensuring that third party access is limited to necessary system functionality

As a result of malware installed on the POS terminal, the credit card clerk was intercepted and the malware was not adequately encrypted or protected. Lesson: The fact that encrypting data and ensuring that the vault is managed securely can mitigate the impact of data theft. Best practice: Encrypt sensitive data at rest and in transit, including on POS systems, while regularly reviewing and updating encryption methods

Target's access control mechanism has vulnerabilities that allow attackers to easily gain access to the payment system, requiring multi-factor authentication for internal and third-party access, especially when it comes to critical systems, and dividing the network into multiple isolated areas to ensure that third-party access is limited to essential system functions.

**Reference:**

Center for Internet Security (CIS). (2020). **CIS Controls v7.1: Critical Security Controls for Effective Cyber Defense**. https://www.cisecurity.org/controls/cis-controls-list/

National Institute of Standards and Technology (NIST). (2020). **NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations**. https://doi.org/10.6028/NIST.SP.800-53r5

U.S. Federal Trade Commission (FTC). (2016). **Start with Security: A Guide for Business**. https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

# 3. Detect

## ***Execution of the Vulnerability Management Plan***

### **1.Regular Auditing of the Vulnerability Management Plan**

Target will conduct regular monthly audits of its vulnerability management plan to ensure it is continuously effective. These audits will involve reviewing system logs, vulnerability scans, and detecting any anomalies in network activity. By systematically checking the systems, Target can identify any weaknesses early, allowing them to patch vulnerabilities before they can be exploited.

The importance of these audits stems from the 2013 breach, where undetected vulnerabilities allowed malware to go unnoticed for weeks. Regular audits would prevent this by ensuring that detection systems are functioning properly, that alerts are acted upon, and that no vulnerabilities, such as those from third-party vendors, are overlooked. This process ensures continuous monitoring and a proactive security posture.

### **2. Tabletop Exercises for Inactive Portions**

Portions of the vulnerability management plan that haven’t been actively used will be tested via tabletop exercises. These exercises simulate theoretical scenarios and walk the response team through how they would manage a potential security incident. This ensures that all personnel are aware of their roles and responsibilities even if they haven’t had to execute these procedures in real-world events recently.

Tabletop exercises are critical because they provide opportunities to rehearse handling potential incidents without the pressure of an active breach. By regularly practicing, Target can ensure that its cybersecurity team is ready for any eventuality, including handling complex vulnerabilities like those that went undetected in 2013. This helps identify procedural gaps and areas for improvement before a real incident occurs.

### **3. Functional Exercises Every Six Months**

Every six months, Target will conduct live **functional exercises** that simulate real-world cyberattacks. Unlike tabletop exercises, these tests use actual systems and involve both personnel and detection tools to simulate a breach and response. The goal is to see how well the detection tools and the incident response team perform under the stress of a live threat.

Functional exercises are crucial for evaluating the effectiveness of malware detection systems and ensuring that personnel can respond swiftly and effectively. For instance, if the functional exercises had been in place in 2013, the response team would have had practice identifying and mitigating a breach like the one involving the BlackPOS malware. These exercises provide valuable insights into how well Target's security systems can detect and respond to intrusions, making the organization more resilient to future cyber threats.

References:

* The NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, provides more information on conducting incident exercises.
  + <https://www.nist.gov/privacy-framework/nist-sp-800-84>

# 4. Respond

## ***Execution of the Incident Response Plan***

Incident Response Auditing

Monthly Audits: The incident response plan will undergo regular audits at least once a month to ensure its components are still relevant, up-to-date, and effective. These audits will review response readiness, including incident tracking, role assignments, communication protocols, and compliance with industry standards like PCI-DSS.

Tabletop Exercises for Unused Portions: Parts of the incident response plan that have not been used recently will be tested through tabletop exercises. These are simulation-based exercises where team members walk through the steps of responding to a hypothetical incident without executing live operations.

Functional Exercises Every Six Months: Every component of the incident response plan will be tested in a live functional exercise at least every six months. These exercises simulate real-world conditions, requiring teams to handle a simulated breach or cyberattack as if it were happening in real time.

Immediate Isolation of Affected Systems: If a breach is detected, the affected systems, such as the POS network, will be immediately isolated from the rest of the business network to prevent the attack from spreading. This can involve disconnecting compromised servers, blocking network traffic, or disabling certain user accounts.

Incident Containment Procedures: Specific steps will be defined for isolating systems and securing compromised areas, which may include shutting down infected systems, resetting credentials, and working with vendors or third-party service providers to limit damage.

Forensic Analysis and Incident Investigation

Forensic Investigation: Following containment, a forensic analysis will be performed to understand how the breach occurred. This will include examining logs, reviewing malware samples (such as BlackPOS malware), and analyzing the network for potential vulnerabilities exploited by the attackers.

Involvement of Cybersecurity Experts: Forensic analysis will be conducted by cybersecurity experts who can assess the full impact of the breach, including data that was compromised and the systems affected. They will also recommend further remediation actions.

Communication Protocols

Customer and Stakeholder Notification: Within 72 hours of detecting the breach, Target will notify affected customers, stakeholders, and regulatory bodies. The notification will include details on what data was compromised, what actions Target is taking to address the breach, and what steps affected parties should take to protect themselves.

Internal Escalation Procedures: Once an incident is detected, it will be escalated internally to the appropriate teams, including legal, PR, IT security, and executive management. This ensures all departments are aligned and able to coordinate a swift, effective response.

References:

* NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, provides more information on conducting incident exercises.
  + <https://www.nist.gov/privacy-framework/nist-sp-800-84>
* NIST SP 800-161, Revision 2, *Computer Security Incident Handling Guide*, provides more information on executing an Incident Response Plan.
  + <https://www.nist.gov/publications/computer-security-incident-handling-guide>

# Recover

#### **Execution of the Incident Recovery Plan**

After a cybersecurity incident, the recovery phase is critical to ensuring that Target’s operations return to normal with minimal disruption and future vulnerabilities are addressed. The incident recovery plan will focus on restoring systems and data to their pre-incident state, improving security postures, and communicating with all stakeholders.

**Recovery Plan Auditing:**

**-Monthly Audits:** The incident recovery plan will undergo regular monthly audits to ensure that it remains updated and relevant. These audits will involve testing backup systems, verifying data restoration processes, and ensuring the availability of all critical systems after a breach.

**-Lesson from 2013 Breach:** Following the 2013 data breach, it became clear that organizations need a well-documented and regularly tested recovery process. Target’s systems were down for an extended period, resulting in customer dissatisfaction and reputational damage. Had a recovery plan audit been in place, the response could have been faster.

**-Best Practice:** Conduct monthly recovery plan audits to ensure business continuity measures are prepared and effective for responding to various types of cyber incidents.

**Tabletop Exercises:**

- **Testing of Unused Portions:** Any sections of the recovery plan that have not been used recently will be tested through tabletop exercises. These exercises simulate potential recovery scenarios without disrupting live systems and ensure that personnel understand the recovery process.

- **Lesson from 2013 Breach:** A clear, practiced recovery procedure could have helped Target mitigate damage and rebuild trust more quickly after the breach.

- **Best Practice:** Use regular tabletop exercises to walk through recovery scenarios, ensuring readiness and pinpointing weaknesses in the plan.

**Functional Exercises:**

- **Live Recovery Testing Every Six Months:** Every component of the recovery plan will be tested in a functional exercise at least every six months. This will involve simulating a real-world breach and executing the recovery plan on live systems to assess response effectiveness.

- **Lesson from 2013 Breach:** Without live functional exercises, it’s difficult to know how well systems and personnel will handle an actual recovery. The delay in Target's response highlights the importance of thorough functional testing. -

**Best Practice:** Conduct biannual live recovery drills to test the ability to restore systems, particularly after critical incidents like malware attacks or data theft.

**Restoration of Systems and Data:**

-**System Restoration Procedures:** During a recovery phase, Target will ensure that affected systems are securely restored and hardened to prevent future exploitation of the same vulnerabilities.

- **Lesson from 2013 Breach:** The malware used in Target’s breach exploited a weakness in the POS system. The restoration process should include patching these vulnerabilities to prevent repeat attacks.

- **Best Practice:** Ensure systems are restored with security improvements in place. Systems must be revalidated before returning to full operational status.

**Backup Verification and Integrity Testing:**

-**Data Backup Verification:** Part of the recovery process will involve verifying that backups are intact and have not been compromised. Target will ensure that data can be restored from these backups without corruption.

- **Best Practice:** Regularly test backup integrity and ensure that data restoration processes are effective.

- **Example:** The impact of the 2013 breach could have been mitigated had Target efficiently restored systems using uncompromised backups.

**Communication During Recovery:**

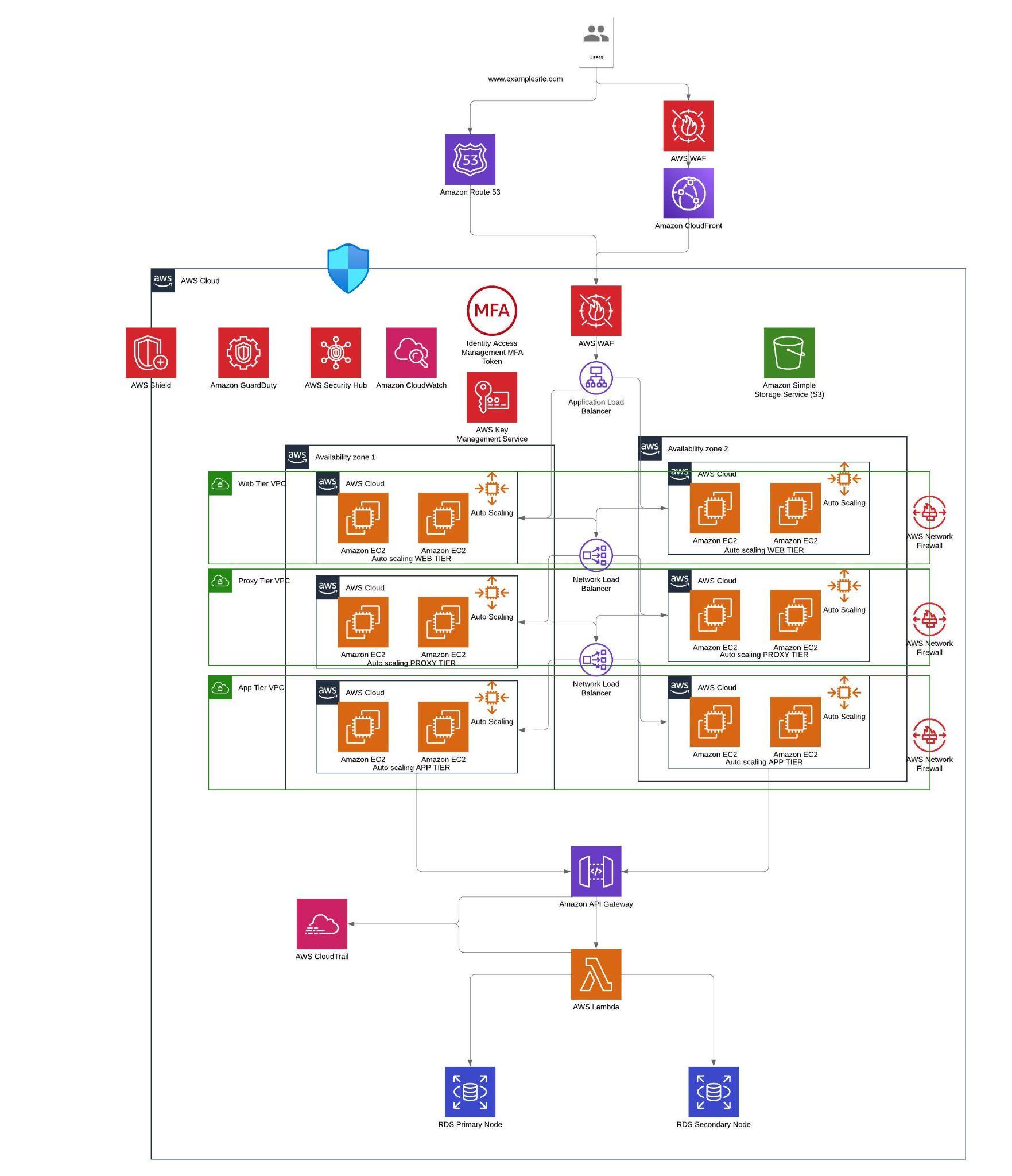
-**Stakeholder Communication:** Communication with stakeholders during the recovery process is critical. Target will notify customers, regulatory agencies, and shareholders of its recovery efforts, focusing on transparency and rebuilding trust.

- **Lesson from 2013 Breach:** Poor communication exacerbated Target’s reputational damage. A clear, effective communication strategy is crucial.

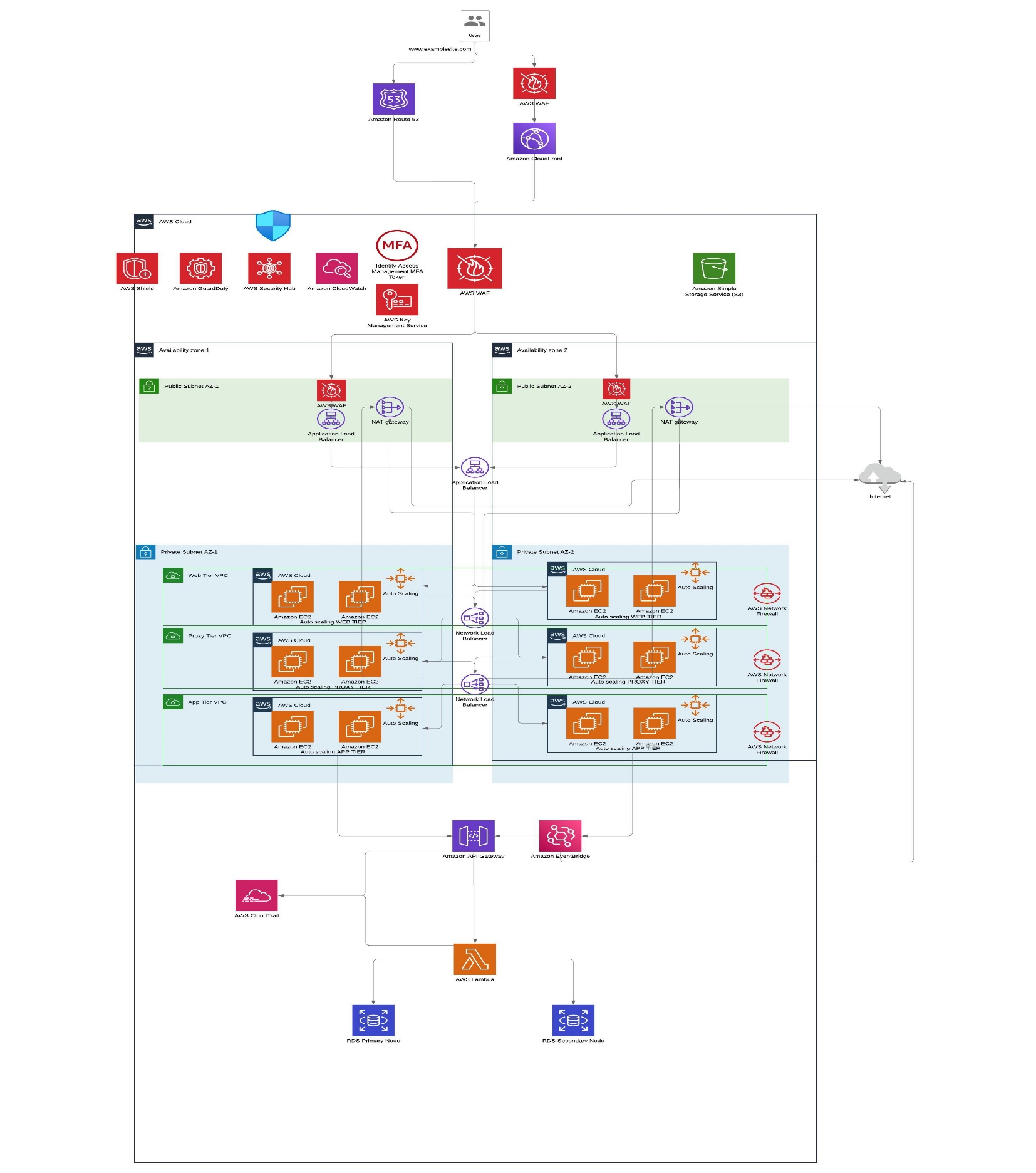
- **Best Practice:** Establish a clear, documented process for communicating recovery progress to all stakeholders.

**ARCHITECTURE DIAGRAM**

**INITIAL DIAGRAM BASED ON FRAMEWORK FOR ZERO TRUST MODEL**



FINAL ARCHITECTURE DIAGRAM BASED ON CYBERSECURITY PLAN TO PREVENT A DATA BREACH LIKE TARGET (2013)



KEY CONCEPTS OF ARCHITECTURE

**Network Segmentation:**

* The architecture uses a multi-VPC design with two primary zones: "Private Subnet AZ-1" and "Private Subnet AZ-2"
* Each subnet is positioned in different Availability Zones (AZs) for high availability
* The design implements proper network isolation with clear boundaries between public and private resources

**Availability Zone Strategy:**

* Resources are distributed across two AZs for redundancy
* Each AZ contains identical infrastructure components demonstrating a proper high-availability design
* Load balancers are positioned to distribute traffic across these AZs

**Integration Pattern:**

* Amazon EventBridge serves as the central event bus/integration layer
* It acts as a serverless event router between different components of the architecture
* The pattern shows decoupled communication between services

**Security Architecture:**

* MFA (Multi-Factor Authentication) is implemented at the top level
* Clear separation between public-facing and internal resources
* Security groups and network ACLs are implied in the VPC design

**Scalability Design:**

* Auto Scaling is implemented across both AZs
* The architecture shows horizontally scalable EC2 instances
* Load balancers are positioned to distribute traffic effectively

**Service Integration:**

* AWS Lambda is used for serverless compute
* Integration with monitoring and logging services
* S3 for storage integrated into the broader architecture

The architecture follows AWS best practices for enterprise-scale applications with proper attention to security, high availability, and scalability while maintaining clear service boundaries and communication paths.

**Services Used in the Architecture:**

1. **Amazon Route 53** – For DNS and domain management.
2. **Amazon CloudFront** – For content delivery network (CDN) to deliver web content globally.
3. **AWS WAF (Web Application Firewall)** – For protecting web applications from common threats like SQL injection and cross-site scripting (XSS).
4. **Amazon S3** – For static content storage, like website files.
5. **Amazon EC2** – For scalable compute instances, across web, app, and proxy tiers.
6. **Amazon RDS (Relational Database Service)** – For managing relational databases (e.g., MySQL, PostgreSQL).
7. **Amazon API Gateway** – For creating, publishing, maintaining, monitoring, and securing APIs.
8. **AWS Lambda** – For running backend functions and microservices without provisioning servers.
9. **Amazon GuardDuty** – For threat detection using machine learning and anomaly detection.
10. **AWS Security Hub** – For unified security checks and insights.
11. **Amazon CloudWatch** – For monitoring and observability of cloud resources and applications.
12. **AWS Key Management Service (KMS)** – For encryption key management.
13. **Auto Scaling** – For automatically scaling EC2 instances in response to load.
14. **Application Load Balancer** – For distributing incoming traffic across EC2 instances.
15. **Network Load Balancer** – For handling high throughput and connection-based traffic.
16. **VPC (Virtual Private Cloud)** – For network segmentation into web, app, and database tiers.
17. **AWS Network Firewall** – For filtering traffic between VPCs and controlling ingress/egress traffic.
18. **AWS CloudTrail** – For logging all API calls and actions across AWS services.
19. **IAM (Identity and Access Management) with MFA** – For user authentication and enforcing Multi-Factor Authentication for privileged access.
20. **VPC Flow Logs** – For capturing IP traffic going in and out of the VPCs.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **AWS Service** | **AWS Service Description** | **NIST Category** | **NIST Subcategory** | **Why did you include the service? What purpose does it serve?** |
| Amazon VPC | Amazon VPC allows you to provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define. | Protect (PR) | PR.AC-5 (Network Segmentation) | Included for network segmentation to isolate web, application, and database tiers, preventing unauthorized traffic flow between them. VPC ensures isolation of resources and limits exposure to external threats. |
| AWS IAM (with MFA) | AWS IAM manages access to AWS resources securely with granular permissions. Multi-Factor Authentication (MFA) adds an extra layer of security for critical system access. | Identify (ID) | ID.AM-2 (Authorization) | IAM is used to control access, ensuring that only authorized users and services can interact with critical AWS resources. MFA is added for securing administrative accounts. |
| Amazon CloudTrail | Amazon CloudTrail enables governance, compliance, and operational and risk auditing by logging all actions taken in AWS services. | Detect (DE) | DE.AE-1 (Audit Logging) | CloudTrail provides detailed logs of API activity, which is crucial for auditing and investigating security events, ensuring traceability in case of breaches or misuse. |
| AWS GuardDuty | A threat detection service that continuously monitors for malicious activity and unauthorized behavior. | Detect (DE) | DE.CM-6 (Monitoring for Threats) | Included to automatically detect and alert for suspicious activity or potential threats in the AWS environment, enabling real-time threat detection. |
| AWS WAF | AWS Web Application Firewall (WAF) protects web applications from common web exploits like SQL injection and cross-site scripting (XSS). | Protect (PR) | PR.PT-3 (Access Control for Web Services) | Included to prevent known attack vectors that can be used to breach web applications, ensuring the security of the front-end tier. |
| Amazon S3 | Amazon Simple Storage Service (S3) offers scalable storage for data, including logs and backups. | Protect (PR) | PR.DS-1 (Data-at-Rest Encryption) | Used to securely store data with encryption to protect sensitive logs and data backups in a scalable manner. S3 provides integrity and availability for stored data. |
| AWS Security Hub | A unified security service that aggregates findings from multiple AWS services (GuardDuty, CloudTrail, etc.) to provide a comprehensive security view. | Identify (ID) | ID.GV-1 (Governance and Risk Management) | Provides a consolidated view of security posture across the environment, helping in risk assessment and mitigation. |
| Amazon RDS | Amazon Relational Database Service (RDS) provides scalable and secure database management with encryption at rest and in transit. | Protect (PR) | PR.DS-1 (Data-at-Rest Encryption) | Used for managing and securing customer data, ensuring encryption at rest and in transit to protect sensitive data stored in the database. |
| AWS CloudWatch | Amazon CloudWatch provides real-time monitoring and observability for AWS resources. | Detect (DE) | DE.CM-7 (Continuous Monitoring) | Included to monitor system performance, resource usage, and to detect any anomalies in behavior, helping in quick identification of performance or security issues. |

#### **Plan Summary:**

This cybersecurity plan addresses the security needs for protecting an organization's cloud infrastructure, with a particular focus on preventing incidents like the 2013 Target data breach. The plan includes a detailed architecture incorporating AWS services such as Amazon VPC, IAM with MFA, CloudTrail, and AWS WAF to provide network segmentation, secure access controls, auditing, and application protection.

#### **Strategy for Implementing the Plan:**

The strategy revolves around segmenting the architecture into isolated VPCs for different application layers, enforcing strict IAM policies with MFA, and utilizing real-time monitoring and logging through CloudWatch and CloudTrail. AWS GuardDuty and WAF provide continuous threat detection and prevention, ensuring the environment is secured from external and internal threats.

#### **Evolution of the Plan with the Business:**

As the business scales or changes, this plan will evolve by adding more resources or adjusting configurations within AWS services like Auto Scaling and S3 to match traffic loads and data storage needs. Security Hub and GuardDuty will continually adapt as they automatically detect new threats and vulnerabilities in real-time, ensuring the environment remains secure.

#### **Next Steps:**

The next steps include finalizing the configuration of all AWS services, ensuring proper IAM roles and permissions are in place, setting up CloudTrail logs, and testing security mechanisms like WAF and GuardDuty. Regular reviews of logs and continuous monitoring will ensure the plan remains effective and up to date with emerging threats.

**Summary：**

This cybersecurity plan establishes a comprehensive approach to safeguarding sensitive data within Target’s cloud infrastructure, emphasizing measures to prevent incidents like the 2013 data breach. Key components include a structured architecture utilizing AWS services such as Amazon VPC for network segmentation, IAM with MFA for secure access control, CloudTrail for audit logging, and AWS WAF for application protection. These services collectively provide robust protection across the NIST Cybersecurity Framework’s core functions: Identify, Protect, Detect, Respond, and Recover.

Implementing this plan involves a strategic focus on network isolation, strict access policies, and continuous monitoring. As the organization evolves, the plan will adapt by scaling resources, enhancing configurations, and integrating advanced threat detection through tools like AWS Security Hub and GuardDuty.

The next steps prioritize securing IAM roles, configuring AWS services, and testing detection and prevention tools to ensure readiness against potential threats. This continuous review and adaptation will help maintain a strong security posture, building trust with customers and compliance with industry standards.