Project 2: Verizon Wireless Risk Management Q2 2025

Marley Willyoung, ***Student Member, IEEE***,

CSEN250
School of Engineering, Santa Clara University
Santa Clara, United States

This report is a continuation of Project 1, in which we identified eight critical threats to Verizon's wireless infrastructure spanning social engineering vulnerabilities, SIM swapping attacks, supply chain risks, and more. Building on those findings, we now employ a structured risk assessment methodology, guided in part by the NIST SP800-53 control framework [1]. Our analysis draws on internal Verizon materials *Data Breach Investigations Report* [2]), and practical insights from our previous analysis.

Abstract: This report presents a formal risk assessment of Verizon's wireless infrastructure by leveraging data from the 2024 *Data Breach Investigations Report (DBIR)* [2] and expanding upon the eight key vulnerabilities highlighted in Project 1. We classify Verizon's critical information assets, apply a threat severity analysis, and map vulnerabilities to relevant controls guided by NIST SP800-53. The resulting five deliverables—an asset classification worksheet, asset value weighting analysis, threat severity table, TVA controls worksheet, and risk ranking matrix—enable Verizon to evaluate its exposure, prioritize remediations, and align cybersecurity strategy with recognized industry standards.

Index Terms: Risk Assessment, Verizon, Telecommunications Security, NIST SP800-53, DBIR, Wireless Infrastructure

Executive Summary

Overview

Verizon's role as a major telecommunications and internet services provider makes it a high-value target for adversaries seeking to compromise wireless data and infrastructure. In our previous analysis, we identified eight prominent threats ranging from social engineering and insider misuse to advanced persistent threats (APTs), each capable of disrupting Verizon's operations or compromising sensitive customer data [3]. Recent incidents in the telecom sector such as T-Mobile's 2022 data breach [4] further show how these large providers remain top targets for financially motivated and state-sponsored attackers alike.

As shown in Figures 1 and 2, Verizon's own *2024 Data Breach Investigations Report (DBIR)* [2] continues to highlight the rise of privilege misuse, social engineering, and denial-of-service (DoS) events. Notably, social engineering and system intrusions fluctuate over time but remain consistently high, reflecting attackers' ongoing focus on human vulnerabilities and sophisticated entry methods. Likewise, "basic web application attacks" and increasingly complex supply chain intrusions underline how evolving technology demands an equally adaptable security strategy [5], [6].

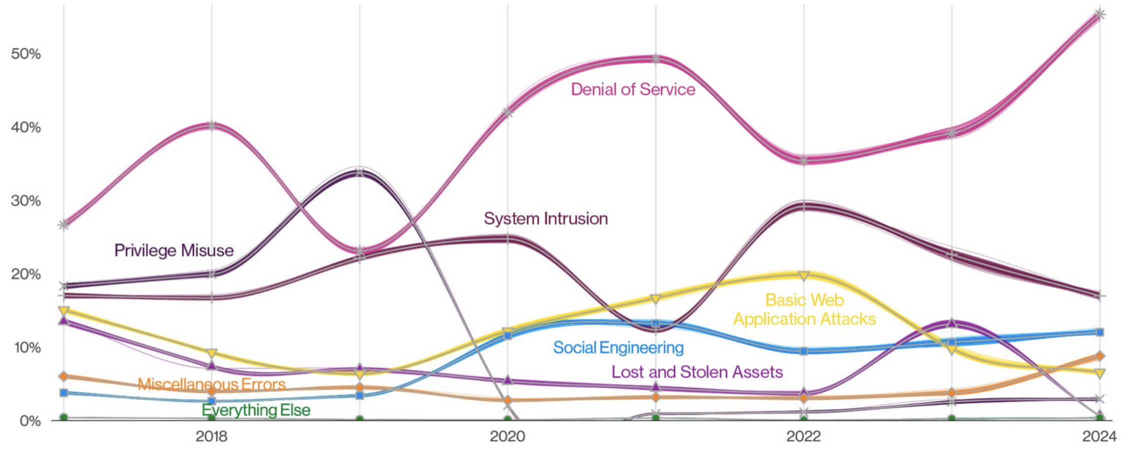

Figure 26. Patterns over time in incidents

Fig. 1. [2].

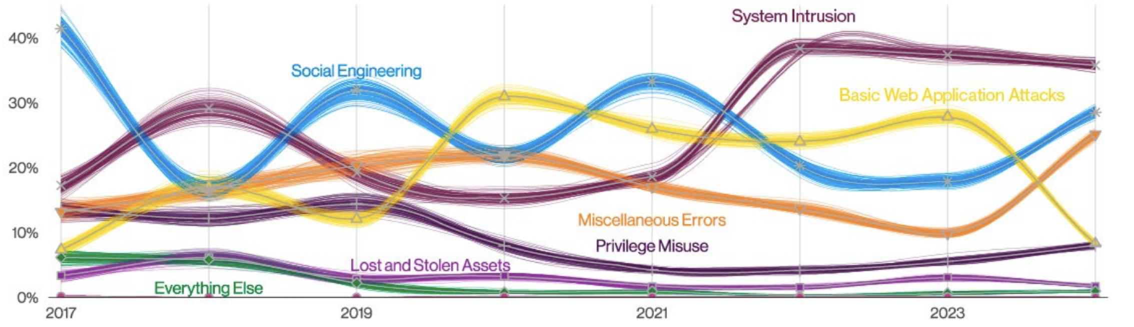

Figure 27. Patterns over time in breaches

Fig. 2. [2].

Building on these findings, this report takes a formal risk assessment approach. We classify Verizon's critical assets, estimate the likelihood and impact of key threat scenarios, and measure residual risk against the organization's strategic tolerance. By referencing both the high-level vulnerabilities from Project 1 and the latest DBIR data, we map technical exposures (e.g., unpatched gateway firmware, insider access to billing platforms) to standardized risk categories. Through this structured process, we aim to develop clear response strategies and mitigation plans based on the NIST SP800-53 framework. Such practices align with broader incident response best practices recommended by NIST [7] and are increasingly vital when, as the *IBM Cost of a Data Breach Report* indicates, the financial impact of a breach continues to climb [8].

Critically, the rise in ransomware and extortion is evident in the DBIR, with attackers leveraging zero-day exploits in telecom ecosystems. Social engineering and privilege misuse remain among the most prominent threats over the past several years, as fraudsters continually refine methods to exploit human weaknesses. Such urgency necessitates a thorough assessment of Verizon's wireless systems, covering not only technical aspects (SS7/Diameter signaling, home gateway hardware) but also employee training and partner processes. This risk profile becomes the foundation for prioritizing security controls, aligning Verizon's defense measures with industry best practices and creating both operational continuity and data confidentiality in an ever-evolving threat landscape.

Table of Abbreviations

Abbreviation	Description
IRP	Incident Response Plan
NIST	National Institute of Standards and Technology
APT	Advanced Persistent Threat
SS7	Signaling System No. 7
DBIR	Data Breach Investigations Report
PCI DSS	Payment Card Industry Data Security Standard
IAM	Identity and Access Management
CPE	Customer Premises Equipment

TABLE I
COMMON ABBREVIATIONS

Review of Identified Threats

Verizon's wireless infrastructure faces an evolving range of cyber threats, driven by advancements in attack methodologies and the increasing reliance on digital services. Our analysis, based on findings from Project 1 and the 2024 *Data Breach Investigations Report (DBIR)* [2], identifies eight primary threats that pose significant risks to Verizon's security posture.

1) **SIM Swapping and Account Takeovers:** Attackers exploit weak identity verification processes and social engineering tactics to fraudulently transfer subscriber phone numbers to new SIM cards, bypassing SMS-based authentication and gaining unauthorized access to financial accounts and personal data.
2) **Insider Threats and Social Engineering:** Employees and third-party vendors with privileged access may be coerced, bribed, or manipulated into granting unauthorized access to sensitive systems. Business email compromise (BEC), phishing, and pretexting account for a significant portion of these attacks.
3) **SS7 and Diameter Protocol Exploits:** Vulnerabilities in telecommunications signaling protocols allow attackers to intercept calls, track subscriber locations, and manipulate authentication messages exchanged between carriers.
4) **Home Wi-Fi Gateway Exploits:** Verizon-issued routers and IoT devices are susceptible to

remote attacks due to outdated firmware, default configurations, and unpatched vulnerabilities, enabling network intrusion, data interception, and botnet integration.

5) **Advanced Persistent Threats (APTs) and Zero-Day Exploits:** Nation-state actors and cybercriminal groups exploit previously undisclosed vulnerabilities to establish persistent footholds within Verizon's infrastructure, often leading to data exfiltration, service disruption, or long-term espionage.
6) **Supply Chain Compromises:** Malicious actors exploit third-party vendors by injecting backdoors into firmware updates, software dependencies, or networking hardware before deployment, gaining access through trusted supply chain relationships.
7) **Ransomware and Extortion Attacks:** Cybercriminals deploy ransomware to encrypt critical systems, exfiltrate sensitive data, and demand ransom payments, often threatening to leak customer or corporate records if demands are not met.
8) **Distributed Denial-of-Service (DDoS) Attacks:** Large-scale botnets and automated attack frameworks are leveraged to disrupt Verizon's network services, degrading availability for customers and critical infrastructure by overwhelming core components with malicious traffic.

Risk Management Methodology

Risk Management Planning Team (RMPT)

Verizon's security policies and industry best practices involve assigning a Risk Management Planning Team (RMPT) assigned personnel responsible for overseeing the risk assessment process, listed in Table II below.

	Role	**Assigned Member**
1	Team Leader (InfoSec Department)	Marley Willyoung
2	Engineering Department	Vincent Zhou
3	HR Department	Marley Willyoung
4	InfoSec Department (Technical/Business)	Vincent Zhou

TABLE II
RISK MANAGEMENT PLANNING TEAM MEMBERS

Roles and Responsibilities

Each RMPT member has a specific function in the risk assessment process. Table III summarizes their responsibilities.

1. Establishing the Context

1.1. Threat Review

1.1.1. Overview

In our initial analysis we identified eight major threats impacting Verizon's wireless infrastructure. These threats reflect evolving attack methods used against telecommunications providers, often leveraging a mix of technical exploits and social engineering.

SIM Swapping Attacks exploit weak identity-verification processes at customer service centers, allowing attackers to seize control of subscriber accounts. Once access is gained, fraudsters bypass two-factor authentication (2FA) and escalate intrusions into financial and personal data.

Insider Threats & Social Engineering continue to be leading concerns, as privileged employees with access to network systems may be coerced, bribed, or manipulated into granting unauthorized access. External attackers also use phishing and pretexting tactics to exploit Verizon's customer service workflows.

SS7 & Diameter Exploits target vulnerabilities in Verizon's core signaling protocols, enabling adversaries to intercept calls, track subscriber locations, or inject fraudulent messages that disrupt authentication mechanisms.

	Role	Responsibilities
1	**InfoSec Department**	• Leads risk assessment and ensures compliance with NIST SP800-53 • Coordinates cross-departmental security strategy • Defines security controls for identified risks • Documents and validates mitigation measures
2	**Engineering Department**	• Conducts system vulnerability analysis • Performs penetration testing and risk modeling • Identifies hardware/software security flaws • Assesses impact of technical risks on infrastructure
3	**HR Department**	• Evaluates insider threats and social engineering risks • Enforces personnel security policies and access controls • Implements security awareness training • Assists in compliance with employment-related security regulations
4	**Technical/Business Role)**	• Maps threats to business impact and risk tolerance • Analyzes financial and operational risk exposure • Develops risk treatment (mitigation, transfer, acceptance) • Aligns cybersecurity policies with business objectives

TABLE III
RMPT ROLES AND RESPONSIBILITIES

Home Gateway Vulnerabilities stem from Verizon-issued routers and IoT devices with outdated firmware, default credentials, or weak security configurations. These gateways can be hijacked for data interception, botnet activity, or local network compromise.

Advanced Persistent Threats (APTs) leverage stealthy intrusion techniques, often exploiting zero-day vulnerabilities to infiltrate Verizon's infrastructure undetected. These attackers, often state-sponsored, establish long-term footholds to exfiltrate sensitive data or disrupt services.

Supply Chain Attacks introduce risk through third-party software and hardware dependencies, where compromised vendors inject malicious code or backdoors into Verizon's network environment.

Ransomware & Extortion attacks continue to evolve, shifting from simple encryption-based tactics to multi-stage extortion models where attackers steal data before locking critical systems.

Distributed Denial-of-Service (DDoS) attacks remain a major operational threat, overwhelming Verizon's core infrastructure with large-scale traffic floods, causing service outages and degraded performance for customers.

1.1.2. Top Identified Threats

For this risk assessment, the RMPT selected the following key threats for deeper evaluation. These threats were prioritized based on their impact on Verizon's critical infrastructure, likelihood of occurrence, and historical significance in past incidents:

- **SIM Swapping** – High-severity risk due to potential for account takeovers affecting customer trust and regulatory liability.

- **SS7 & Diameter Exploits** – Threatens network availability and subscriber privacy, impacting authentication and service continuity.
- **Home Gateway Vulnerabilities** – Targeting Verizon's customer-premises equipment (CPE) creates large-scale exposure points.
- **Advanced Persistent Threats (APTs)** – Long-term intrusion risks from sophisticated actors seeking deep network penetration.
- **Supply Chain Attacks** – Increasing reliance on third-party vendors amplifies potential entry points for embedded malware or firmware compromises.
- **Ransomware & Extortion** – Major financial and operational disruption risk, compounded by data theft and ransom demands.

1.2. Additional Factors

Verizon's risk exposure is influenced by external and internal factors that increase the likelihood and severity of security incidents. These factors shape the threat landscape, impacting Verizon's ability to maintain network integrity, protect customer data, and comply with regulatory mandates.

- **Intellectual Property Risks:** Verizon holds a vast portfolio of patents, proprietary network designs, and trade secrets, stored in cloud collaboration platforms (Office 365, SharePoint) and internal repositories (GitHub Enterprise). Threat actors, including nation-state cyber groups, may attempt to exfiltrate source code or steal R&D data through phishing attacks, insider threats, or software supply chain infiltration.
- **Regulatory & Compliance Pressures:** Verizon operates under strict U.S. and international regulations (FCC, GDPR, CCPA, PCI DSS, ISO 27001) that govern data security, privacy, and consumer protection. Failure to meet compliance requirements may result in regulatory fines, lawsuits, or reputational damage. Recent regulatory trends emphasize zero-trust architectures, AI-driven threat detection, and cross-border data sovereignty, further complicating global compliance efforts.

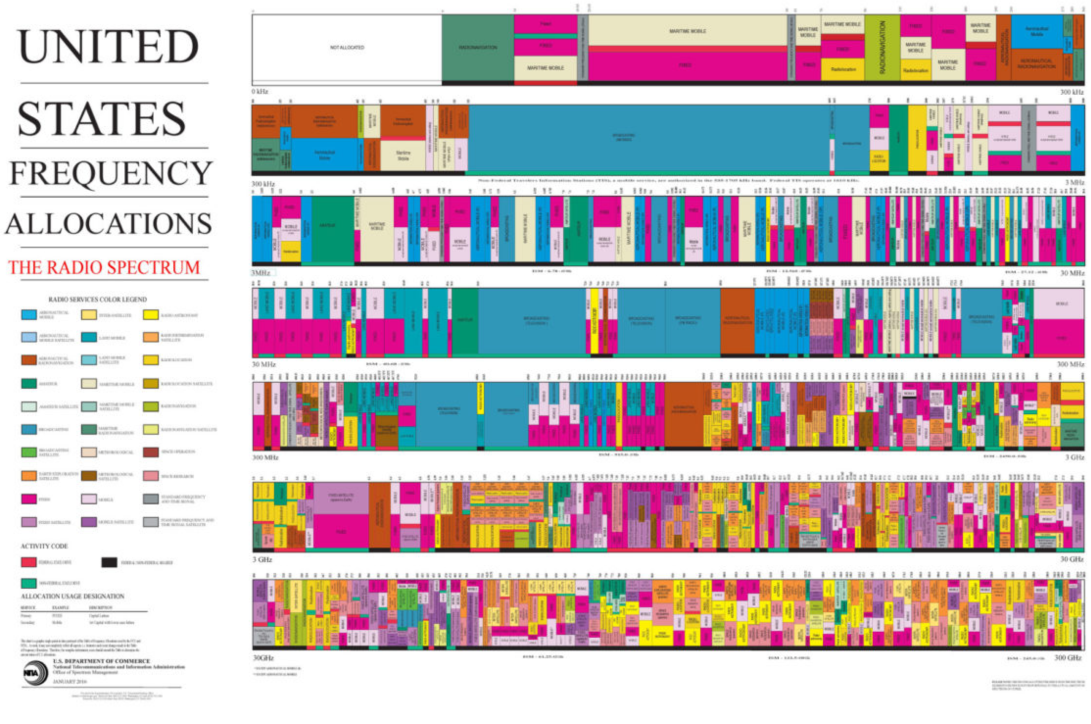

Fig. 3. FCC Frequency Allocation Chart detailing U.S. spectrum usage.

- **5G Expansion & Infrastructure Complexity:** The deployment of 5G Standalone (5G SA) networks introduces new attack surfaces, including service-based architectures (SBA), network slicing, and multi-access edge computing (MEC). Legacy SS7/Diameter vulnerabilities remain exploitable, while emerging threats such as 5G signaling fraud, API abuse, and AI-driven DDoS attacks require adaptive security strategies and automated mitigation tools.
- **Supply Chain Dependencies & Third-Party Risk:** Verizon relies on third-party vendors for software, hardware, and cloud services, increasing the risk of supply chain attacks. Adversaries may introduce backdoors in firmware, trojanized software updates, or exploit weak vendor authentication mechanisms. High-profile incidents, such as the SolarWinds compromise, highlight the need for software bill of materials (SBOM) tracking, vendor risk assessments, and runtime supply chain monitoring.
- **Operational Constraints & Workforce Challenges:** Verizon faces budgetary limitations, security talent shortages, and complex patch management cycles that hinder rapid threat mitigation. Zero-day vulnerabilities in network hardware (e.g., routers, SDN controllers), delayed security patch rollouts, and misconfigurations in multi-cloud environments (AWS, Azure, GCP) increase residual risk. Additionally, insider threats, exacerbated by remote work and hybrid IT environments, require enhanced behavioral analytics and anomaly detection.
- **Advanced Persistent Threats (APTs) & Nation-State Cyber Activity:** Telecommunications providers are frequent targets of APTs seeking espionage, surveillance capabilities, and infrastructure disruption. Adversaries exploit zero-day vulnerabilities, phishing campaigns, and advanced malware (e.g., modular implants in telecom core networks) to persist in high-value systems. Verizon's role in critical national infrastructure (CNI) makes it a strategic target for state-sponsored attacks.
- **Evolving Threat Landscape & Emerging Attack Techniques:** Threat actors are leveraging AI-driven malware, deepfake social engineering, adversarial machine learning (ML) techniques, and quantum computing threats to bypass traditional security controls. Verizon must anticipate automated AI-powered phishing campaigns, enhanced ransomware-as-a-service (RaaS) models, and post-quantum cryptographic risks to maintain security resilience.
- **Cloud & Virtualization Security Challenges:** As Verizon expands its multi-cloud infrastructure (AWS, Azure, GCP) and virtualized network functions (VNF) using Kubernetes, OpenStack, and NFV architectures, security challenges arise in container misconfigurations, identity federation (OAuth, SAML) exploits, and data sovereignty issues. The increasing reliance on cloud-based 5G core deployments requires continuous security monitoring, hardened APIs, and zero-trust enforcement.

1.3. Critical Information Assets

Based on the threats identified, the RMPT classified Verizon's most critical information assets, selecting those that are highly valuable and vulnerable to exploitation. These assets represent high-priority targets for cyber adversaries due to their role in customer data protection, network security, and infrastructure integrity.

1.3.1. Customer Identity & Payment Data (PII, PCI, Account Credentials)

Asset 1: Personally Identifiable Information (PII) such as customer names, addresses, phone numbers, and Social Security Numbers, along with Payment Card Industry (PCI) data including credit card details and banking credentials, are stored in Verizon's billing systems and authentication platforms. A breach can result in financial fraud, identity theft, and regulatory non-compliance under frameworks such as PCI DSS, CCPA, and GDPR. Attackers often exploit weak authentication, credential leaks, and phishing attacks to gain access to this sensitive data [2].

1.3.2. Verizon Core Telecom Signaling & Authentication Systems (SS7, Diameter, 5G SA Core)

Asset 2: Signaling and authentication protocols, including SS7, Diameter, and 5G Service-Based Architecture (SBA) Core, are critical for call routing, SMS transmission, and subscriber verification. Vulnerabilities in SS7 allow attackers to intercept SMS-based two-factor authentication (2FA), track subscriber locations, or manipulate authentication requests. Diameter exploits can lead to fraudulent session hijacking, while weaknesses in 5G SBA may introduce new attack vectors against network authentication and subscriber identity integrity [2].

1.3.3. Employee & Insider Privileged Access Systems (HR, IAM, Customer Support)

Asset 3: Internal Identity and Access Management (IAM) systems, HR databases, and customer service tools such as Verizon Enterprise Center (VEC) and VZOne grant privileged access to employees and contractors. Compromising these systems allows attackers to manipulate customer accounts, execute fraudulent SIM swaps, or exfiltrate sensitive internal communications. This category also includes access to confidential business documents, pricing agreements, internal policies, and trade secrets. Social engineering tactics, business email compromise (BEC), and credential theft remain primary attack methods [2].

1.3.4. Software Source Code & Research Repositories (Internal R&D, Patents, Proprietary Systems)

Asset 4: Proprietary software source code, research and development (R&D) documentation, and patent-related materials are critical intellectual property stored in GitHub Enterprise, Bitbucket, Office 365, and SharePoint. These repositories contain proprietary algorithms, internal security protocols, and software development lifecycles (SDLC) artifacts. Unauthorized access can result in industrial espionage, source code tampering, and product vulnerabilities. Threat actors often use phishing attacks against developers, malicious insider activity, and repository misconfigurations to infiltrate these systems [2].

1.3.5. Network & Infrastructure Management Systems (Firewalls, SDN Controllers, Cloud Compute)

Asset 5: Core network administration consoles, including firewalls, software-defined networking (SDN) controllers, and cloud compute platforms (AWS, VMware vSphere, OpenStack), regulate Verizon's network traffic and security policies. Unauthorized access enables attackers to alter network routing, disable security protections, or establish persistent access for further exploitation. These systems are prime targets for advanced persistent threats (APTs) seeking long-term network infiltration [2].

1.3.6. Customer-Facing Web Services & APIs (MyVerizon, Billing, Self-Service Portals)

Asset 6: Verizon's customer account management platforms, including MyVerizon, online billing services, and self-service APIs, handle sensitive customer interactions. API vulnerabilities, authentication flaws, and credential stuffing attacks allow unauthorized access to customer accounts, enabling financial fraud, identity theft, and unauthorized modifications to service plans. Attackers frequently exploit OAuth token misconfigurations and exposed API keys to escalate access [2].

1.3.7. Verizon-Issued Customer Premises Equipment (CPE) & Home Gateways (Fios, 5G, IoT)

Asset 7: Verizon-distributed hardware, including Fios routers, 5G gateways, and IoT-connected devices, relies on remote management protocols such as TR-069 and TR-369 for firmware updates and diagnostics. Unpatched firmware, default credentials, or supply chain compromises enable attackers to hijack devices for botnet deployment, execute man-in-the-middle attacks, or inject malicious DNS configurations. Large-scale exploitation of these devices can lead to widespread service disruptions and data interception [2].

1.3.8. Partner, Vendor, & Supply Chain Infrastructure (Third-Party Software, Billing Integrations)

Asset 8: Third-party software providers, billing platform vendors, and firmware suppliers form an extended risk surface. Supply chain attacks targeting Verizon's software dependencies can introduce malicious code into production environments, compromise vendor credentials, or exploit weak integrations with third-party services. Attackers increasingly leverage supply chain compromises to introduce persistent vulnerabilities that propagate across interconnected systems. This asset includes external billing processors, cloud service providers, and outsourced development teams [2].

1.4. Asset List Table

For reference throughout this report, please refer to the table below for the full names of the identified critical assets.

Asset #	Name
1	Customer Data
2	Verizon Core & Authentication
3	Insider Privileged Access
4	Source Code & Research
5	Network Management Systems
6	Web Services & APIs
7	Customer Premises Equipment (CPE)
8	Vendor & Supply Chain

TABLE IV
CRITICAL INFORMATION ASSET LIST

2. Key Considerations

Scope of the Risk Assessment

This risk assessment focuses on Verizon's wireless and network infrastructure, including:

- The eight critical information assets identified in Section VIII, spanning customer data, signaling protocols, insider access systems, source code repositories, network management, web services, CPE gateways, and supply chain dependencies.
- The operational and administrative processes that govern SIM provisioning, network routing, software development lifecycles (SDLC), and vendor integrations.
- Threat vectors affecting both legacy SS7/Diameter protocols and emerging 5G standalone (5G SA) architectures.

Any systems, tools, or processes not directly impacting the above assets (e.g., purely administrative HR workflows, standalone marketing platforms) are out of scope unless they interface with these high-value domains.

Assumptions and Constraints

- **Accurate Inventory:** All hardware, software, and virtual appliances pertaining to the in-scope assets are properly inventoried and documented.
- **Availability of Stakeholders:** Engineering, InfoSec, and HR departments can provide timely input regarding vulnerabilities, threat intelligence, and control effectiveness.
- **Compliance Requirements:** The assessment must adhere to NIST SP800-53 guidelines, meeting or exceeding relevant regulatory frameworks (FCC, GDPR, CCPA, PCI DSS, ISO 27001).
- **Resource Limitations:** Budgetary and scheduling constraints may limit the depth of certain vulnerability scans, penetration tests, or training programs.

- **Evolving Threat Landscape:** Zero-day exploits, novel attack techniques, and undisclosed hardware or software vulnerabilities may emerge, influencing residual risk beyond documented metrics.

Sources of Information Used

- **Verizon Internal Data:** Configuration baselines, incident logs, and network diagrams provided by the Engineering and InfoSec teams.
- **Previous Analysis:** Threat enumeration and preliminary vulnerability analysis conducted in the initial project phase, serving as the foundation for this risk assessment.
- **Verizon 2024 Data Breach Investigations Report (DBIR) [2]:** Industry trends, statistical data on breaches, and threat actor methodologies relevant to telecommunications providers.
- **NIST Special Publications (SP800-30, SP800-53):** Guidelines on risk assessment procedures, control selection, and risk treatment strategies.
- **Vendor Advisories and Security Bulletins:** Firmware vulnerability disclosures, application security patches, and upstream code dependency alerts from third-party providers.

3. Risk Assessment Process

3.0.1. Establish the Context

The context for this risk assessment, including Verizon's critical assets, external threats, and internal vulnerabilities, has been previously detailed in Establishing the Context Review of Identified Threats.

3.0.2. Identify Risk

The key risks Verizon faces have been outlined in Review of Identified Threats. The next steps involve analyzing the probability, impact, and ranking of each identified risk to guide mitigation strategies.

3.0.3. Analyze Risk

The analysis phase assigns numerical values to the likelihood and impact of each identified risk. Verizon's risk scoring model considers:

Risk Score Calculation:

$$\text{Risk Score} = \text{Likelihood (1–5)} \times \text{Impact (1–5)}$$

■

- **Likelihood (1–5):** Probability of occurrence based on past incidents and known vulnerabilities.
- **Impact (1–5):** Consequences if the threat materializes.
- **Residual Risk:** Level of risk remaining after existing security controls are applied.

3.0.4. Evaluate Risk

Risk evaluation categorizes threats into priority levels:

Risk Score	Category
16–25	Critical (Requires immediate remediation)
10–15	High (Strong mitigation recommended)
5–9	Moderate (Manageable with existing controls)
1–4	Low (No urgent action necessary)

TABLE V
Risk Evaluation Categories

4. Risk Analysis

4.0.1. Risk Calculation

Each threat is assigned an L-value and I-value using the following standardized criteria:

Likelihood Score	Description
1 – Rare	Less than once in 10 years, requires extreme conditions.
2 – Unlikely	Occurs once every 5–10 years, dependent on targeted attacks.
3 – Possible	Occurs once every 2–5 years, known exploits exist.
4 – Likely	Occurs annually, actively exploited in the industry.
5 – Certain	Occurs multiple times per year, persistent threats targeting Verizon.

TABLE VI
LIKELIHOOD SCALE

Impact Score	Description
1 – Minimal	No customer impact, less than $10,000 in losses.
2 – Low	Limited impact, affects fewer than 1,000 users, losses under $100,000.
3 – Moderate	Affects multiple services, legal consequences possible, losses up to $1M.
4 – High	Significant customer impact, regulatory violations, losses up to $10M.
5 – Catastrophic	Widespread service failure, lawsuits, regulatory fines, losses over $10M.

TABLE VII
IMPACT SCALE

Weighted Impact Score Calculation

$$I_w = (W_r \times I_r) + (W_p \times I_p) + (W_c \times I_c)$$

$$W_r + W_p + W_c = 1$$

where:

- I_w = Weighted impact score
- I_r = Revenue impact (scale 1–5)
- I_p = Profitability impact (scale 1–5)
- I_c = Compliance impact (scale 1–5)
- W_r = Weight for revenue impact (0.3)
- W_p = Weight for profitability impact (0.4)
- W_c = Weight for compliance impact (0.3)

The weighted impact score I_w remains a valid linear combination of the individual impact factors, preventing distortion in the ranking process.

4.0.2. Handling Uncertainty in Risk Estimates

Risk assessment inherently involves uncertainty. Historical attack frequency data may be limited, making it difficult to accurately predict future threats. Cyber threat landscapes evolve rapidly, introducing new vulnerabilities that may not have been previously considered. The effectiveness of security controls can vary, further impacting risk calculations.

Confidence Scoring Adjustment

Each risk score is adjusted based on intelligence confidence:

$$\text{Adjusted Risk Score} = (\text{Risk Score}) \times (1 \pm \text{Uncertainty Factor})$$

where the uncertainty factor is:

- 0% – High certainty (well-documented threats)
- 10% – Moderate certainty (known but evolving threats)
- 25% – Low certainty (emerging or zero-day threats)

For example, if a risk score of 20 has a 10% uncertainty factor:

$$20 \pm (20 \times 0.10) = 18 - 22$$

Threat Intelligence Correlation

Verizon aligns risk scores with DBIR trends [2] and external threat intelligence. If industry data indicates an increase in attack frequency, likelihood scores are dynamically adjusted to reflect emerging risks.

5. Results and Deliverables

Reference Table of Critical Assets:

Asset #	Name
1	Customer Data
2	Verizon Core & Authentication
3	Insider Privileged Access
4	Source Code & Research
5	Network Management Systems
6	Web Services & APIs
7	Customer Premises Equipment (CPE)
8	Vendor & Supply Chain

TABLE VIII
Critical Information Asset List

Threat #	Name
1	Compromises to Intellectual Property
2	Deviations in Quality of Service from Service Providers
3	Espionage or Unauthorized Access
4	Forces of Nature
5	Human Error or System Misconfiguration
6	Information Extortion (Ransomware)
7	Sabotage or Vandalism
8	Software Attacks (Malware, Exploits)
9	Technical Hardware Failures
10	Technical Software Failures
11	Technological Obsolescence
12	Theft (Data, Devices)

TABLE IX
THREAT REFERENCE TABLE

5.1. Information Asset and Classification Worksheet

Asset #	Examples	Sensitivity	Value
1	PII, PCI, Account Credentials	High	5
2	SS7, Diameter, 5G SA Core	High	5
3	HR systems, IAM, Customer Support	Medium	4
4	Source Code, R&D, Internal Collab	Medium	5
5	Firewalls, SDN Controllers, Cloud Compute	High	5
6	MyVerizon, Billing, Self-Service Portals	Medium	4
7	CPE, Fios, 5G Gateways, IoT	Medium	3
8	Third-Party Software, Billing Integrations	Medium	4

TABLE X
INFORMATION ASSET AND CLASSIFICATION WORKSHEET

5.2. Information Asset Value Weight Table Analysis

Asset #	Continuity	Legal	Reputation	Revenue	Total	Importance
1	5	5	5	5	20	High
2	5	4	5	5	19	High
3	4	4	4	4	16	High
4	3	4	4	4	15	Medium
5	5	4	5	5	19	High
6	4	3	4	4	15	Medium
7	3	3	3	3	12	Medium
8	4	4	3	4	15	Medium

TABLE XI
INFORMATION ASSET VALUE WEIGHT TABLE ANALYSIS

5.3. Threat Severity Weighted Table Analysis

Threat #	Likelihood (L)	Ease of Exploitation (E)	Detection Capability (D)	Total	Importance
1	4	4	4	12	High
2	2	2	3	7	Low
3	4	4	5	13	High
4	2	5	2	9	Medium
5	5	3	3	11	High
6	4	4	4	12	High
7	3	3	4	10	Medium
8	5	5	3	13	High
9	3	2	3	8	Medium
10	4	3	3	10	Medium
11	3	4	2	9	Medium
12	3	3	3	9	Medium

TABLE XII
THREAT SEVERITY WEIGHTED TABLE ANALYSIS

5.4. TVA (Threat-Vulnerability-Asset) Controls Worksheet

Threat #	Asset #	Vulnerability	Existing & Planned Controls
5	1	Employees mishandling customer PII or credentials	**Existing:** Basic security training, role-based access control (RBAC) **Planned:** Enhanced staff awareness programs, restricted privilege access, advanced identity verification measures
8	5	Unpatched SDN firewall vulnerabilities	**Existing:** Quarterly patch cycle, Intrusion Detection System (IDS) **Planned:** Automated patch deployment system, AI-driven threat detection, adaptive firewall rule enforcement
11	7	Legacy firmware in IoT devices	**Existing:** Vendor patch advisories, periodic security reviews **Planned:** Enforced automatic firmware updates, secure boot implementation, vulnerability scanning for IoT devices
3	3	Weak monitoring of insider activity	**Existing:** Role-based access control (RBAC), log retention and periodic audits **Planned:** Security Information and Event Management (SIEM) implementation, real-time insider threat detection alerts, behavioral analytics for privilege misuse detection
1	4	Unsecured software repositories, risk of source code exfiltration	**Existing:** Developer Two-Factor Authentication (2FA), private repositories for proprietary code **Planned:** Automated dependency scanning for third-party libraries, stricter pull request approval workflows, source code integrity verification through digital signatures

TABLE XIII
TVA CONTROLS WORKSHEET

5.5. Risk Ranking Worksheet

Threat #	Asset #	Threat Severity	Asset Importance	Final Risk Ranking
8	5	High (13)	High (19)	Critical
5	1	High (11)	High (20)	Critical
11	7	Medium (9)	Medium (12)	Medium
3	3	Medium (10)	High (16)	High
1	4	Medium (10)	Medium/High (15)	High
2	8	Low (7)	Medium (15)	Low/Medium

TABLE XIV
RISK RANKING WORKSHEET

Results

The Information Asset and Classification Worksheet classifies Verizon's eight critical assets based on sensitivity and operational value. Customer Data (Asset #1) and Network Management Systems (Asset #5) are identified as the highest-priority assets due to their role in authentication security, infrastructure control, and regulatory compliance under PCI DSS and CCPA. Insider Privileged Access (Asset #3) and Web Services (Asset #6) present moderate risk due to access control requirements and exposure to external threats. Customer Premises Equipment (Asset #7) and Vendor & Supply Chain Infrastructure (Asset #8) are lower-priority, with risks concentrated in third-party dependencies and endpoint vulnerabilities.

The Information Asset Value Weight Table Analysis assigns numerical weights to each asset based on continuity, legal compliance, reputation, and revenue impact. Customer Data (Asset #1) and Network Management Systems (Asset #5) score the highest, indicating primary areas for security investment. Insider Privileged Access (Asset #3) follows due to risks associated with internal misuse and regulatory exposure. Web Services (Asset #6) and Intellectual Property (Asset #4) remain significant but with lower immediate risk. Customer Premises Equipment (Asset #7) and Vendor & Supply Chain Infrastructure (Asset #8) present indirect security risks through external attack surfaces rather than direct exploitation.

The Threat Severity Weighted Table Analysis evaluates threat severity based on likelihood of occurrence, ease of exploitation, and detection capability. Software Attacks (Threat #8) and Insider Threats (Threat #3) score highest due to frequency, exploitability, and detection limitations, with total scores of 13. Human Error (Threat #5) is a major risk with a total score of 11. Lower-rated threats include Quality of Service Deviations (Threat #2) and Forces of Nature (Threat #4), which have limited cybersecurity impact. These rankings confirm that attack-driven and insider threats require immediate mitigation.

The TVA (Threat-Vulnerability-Asset) Controls Worksheet maps threats to vulnerable assets, identifying security gaps and necessary mitigations. Software Attacks (Threat #8) target unpatched firewalls and SDN vulnerabilities in Network Management Systems (Asset #5), requiring automated patching and AI-driven monitoring. Insider Threats (Threat #3) affect Privileged Access (Asset #3), necessitating stricter role-based access controls and real-time behavioral analytics. Technological Obsolescence (Threat #11) introduces risks in Customer Premises Equipment (Asset #7), requiring enforced firmware updates and phased hardware replacements.

The Risk Ranking Worksheet ranks threats based on severity and asset importance. Critical risks include Software Attacks (Threat #8) on Network Management Systems (Asset #5) and Human Error (Threat #5) affecting Customer Data (Asset #1), requiring immediate action. High-risk scenarios include Insider Threats (Threat #3) on Privileged Access (Asset #3) and Data Theft (Threat #12) targeting Customer Data (Asset #1), requiring enhanced access control and monitoring. Medium-risk items include Technical Software Failures (Threat #10) affecting Web Services (Asset #6), while lower-risk threats such as Forces of Nature (Threat #4) pose minimal cybersecurity impact.

Comparative Risk

High-Risk Assets and Threat Pairings

Customer Data (Asset #1) and Network Management Systems (Asset #5) have the highest risk exposure. Software Attacks (Threat #8) targeting Network Management Systems exploit vulnerabilities in SDN controllers, firewall configurations, and remote management interfaces. Insider Threats (Threat #3) and Data Theft (Threat #12) compromise Customer Data by exploiting weak identity verification, excessive user privileges, and credential reuse. Human Error (Threat #5) remains a leading cause of misconfigurations, exposing assets to further exploitation. Privileged Access Systems (Asset #3) are susceptible to credential compromise, session hijacking, and social engineering attacks, increasing the risk of unauthorized network infiltration. Mitigation requires zero-trust architecture expansion, automated access revocation, behavioral monitoring, and anomaly-based authentication.

Emerging Trends from Risk Assessment

Threat actors increasingly use AI-driven attacks, leveraging machine-learning-based phishing, adversarial malware, and automated reconnaissance. Credential stuffing and synthetic identity fraud bypass multi-factor authentication through behavioral mimicry. Software supply chain attacks target vendor firmware, dependency injection vulnerabilities, and signed update processes. Cloud-native 5G infrastructure increases the attack surface, exposing containerized workloads, service-based architecture (SBA) endpoints, and API management systems. Ransomware has evolved into persistent multi-stage extortion campaigns, integrating lateral movement techniques, data exfiltration, and coercion tactics. Zero-day exploits in telecom signaling protocols (SS7, Diameter, SIP) allow adversaries to intercept subscriber metadata, modify authentication requests, and hijack active sessions.

Benchmarking Against Industry Threat Trends

Verizon's threat landscape aligns with industry-wide cyber risk patterns observed in global telecom reports and the Verizon DBIR. Insider privilege misuse, business email compromise (BEC), and advanced persistent threats (APTs) are primary attack vectors. Compared to industry benchmarks, Verizon exhibits similar exposure to API security risks, misconfigured identity federation, and cross-platform authentication weaknesses. While its implementation of network segmentation and zero-trust policies mitigates some risks, security gaps persist in endpoint posture enforcement and real-time anomaly detection. The rapid adoption of software-defined networking (SDN) and multi-access edge computing (MEC) further increases the risk of attack propagation through lateral movement inside virtualized network functions.

Verizon's Risk Appetite vs. Residual Risk

Residual risk remains in unpatched vulnerabilities, unmonitored third-party integrations, and legacy system dependencies. Network infrastructure aging increases exposure to security gaps in older routing protocols, firmware inconsistencies, and weak cryptographic implementations. While Verizon's security strategy prioritizes risk reduction through automation and proactive mitigation, operational constraints limit full risk elimination. Risk acceptance thresholds must be recalibrated to account for emerging AI-enabled attack methodologies, regulatory compliance shifts, and real-time response automation. The current risk posture necessitates continuous assessment, adaptive threat intelligence integration, and predictive risk modeling to prevent high-impact security incidents.

Summary

Lessons Learned

The risk assessment confirms that high-severity threats target Verizon's network infrastructure, privileged access systems, and customer data. Software attacks, insider threats, and human error continue to be primary risks, with software supply chain vulnerabilities and misconfigurations increasing the attack surface. Existing security controls mitigate some threats, but gaps remain in real-time threat detection, endpoint security enforcement, and automated incident response. The effectiveness of Verizon's zero-trust architecture is dependent on continuous monitoring and access control enhancements. The growing reliance on third-party vendors introduces external risks, necessitating stricter vendor security assessments and runtime supply chain monitoring. The integration of AI-driven security mechanisms is critical for identifying and mitigating sophisticated attacks in real time [2], [5], [6].

The assessment identified software supply chain vulnerabilities and insider threats as the two most critical risks to Verizon's security posture. Software supply chain attacks present a significant risk due to the increasing reliance on third-party vendors for firmware, cloud services, and application dependencies. A compromise in a trusted vendor's software update or development pipeline could introduce undetectable backdoors, enabling persistent unauthorized access to critical systems. This risk is particularly concerning given the rise of sophisticated attacks leveraging open-source software dependencies and previously trusted vendors. Insider threats, while often overlooked compared to external cyberattacks, emerged as a major concern due to the potential for privileged employees or contractors to bypass existing security controls. This process revealed that Verizon's current access control measures may not adequately detect or prevent unauthorized data access by insiders, and the absence of continuous monitoring in some areas increases the risk of undetected data exfiltration. It was surprising that despite advanced perimeter defenses and authentication mechanisms, human factors and trusted relationships within the supply chain remain the largest potential points of failure, emphasizing the need for continuous security monitoring, zero-trust enforcement, and stricter vendor risk assessments.

Future Considerations

Mitigation strategies must prioritize advanced threat intelligence correlation, predictive risk modeling, and AI-enhanced anomaly detection. Expanding endpoint detection and response (EDR) capabilities will strengthen proactive defense against ransomware and data exfiltration attempts [9], [10]. Implementing secure-by-design principles in software development will reduce supply chain attack risks by ensuring software dependencies are continuously validated and monitored for vulnerabilities [1]. Strengthening security baselines for cloud-native 5G infrastructure and enforcing strict API access controls will mitigate risks associated with multi-access edge computing (MEC) and service-based architecture (SBA) vulnerabilities. Enhancing cryptographic security in legacy authentication protocols, including SS7 and Diameter, will prevent session hijacking and unauthorized subscriber tracking. Future assessments should incorporate adversarial penetration testing, continuous compliance validation, and automated remediation workflows to align with evolving regulatory requirements [7], [8], [11].

AI-driven cyber threats continue to evolve, with ransomware groups now leveraging machine learning for automated attack execution, real-time reconnaissance, and dynamic payload generation. The 2024 Data Breach Investigations Report (DBIR) highlights an increasing use of AI-assisted phishing campaigns, which employ large language models (LLMs) to generate highly targeted social engineering attacks with contextual awareness [2]. To counteract these trends, Verizon must integrate AI-powered phishing detection mechanisms, behavioral threat analytics, and identity-based deception techniques to mitigate fraudulent account takeover attempts. AI-assisted ransomware detection must incorporate real-time memory analysis, behavior-based threat scoring, and deep learning models capable of identifying polymorphic malware strains before encryption events occur.

Zero-trust security enforcement must extend beyond access controls to continuous authentication and dynamic trust scoring. Identity and access management (IAM) solutions should leverage AI-driven behavioral baselines to detect anomalous credential usage, privilege escalation attempts, and unauthorized session persistence. Risk-based authentication models should be implemented to evaluate access requests based on contextual factors, including device health, location profiling, and historical usage patterns. Integrating deception technologies into enterprise networks can further disrupt reconnaissance phases of adversaries, forcing attackers into controlled environments where their tactics can be analyzed and mitigated in real time.

Cloud security enhancements must focus on runtime monitoring, API security posture enforcement, and workload segmentation within virtualized environments. API abuse remains one of the fastest-growing attack vectors in cloud-native architectures, with adversaries exploiting misconfigured authentication mechanisms, overprivileged service accounts, and unvalidated input handling [2]. Implementing robust API gateway security, adaptive rate limiting, and automated API behavioral anomaly detection will be critical in preventing lateral movement within cloud environments.

Supply chain security must incorporate continuous software bill of materials (SBOM) validation, ensuring that third-party code dependencies are regularly scanned for vulnerabilities. Runtime integrity verification and real-time dependency tracking should be enforced across development pipelines to mitigate the risk of supply chain compromise. Firmware security hardening for customer-premises equipment (CPE) and IoT gateways must become a priority, requiring manufacturers to adopt secure firmware update mechanisms and cryptographic signing enforcement for software distribution [1].

Incident response automation must evolve to address AI-driven threats, with security orchestration, automation, and response (SOAR) platforms leveraging machine learning-based decision trees to automate containment workflows. AI-assisted forensic analysis can accelerate post-breach investigations by automatically correlating attacker indicators of compromise (IOCs) and mapping intrusion paths to the MITRE ATT&CK framework. Improving response efficiency through automated threat containment will reduce breach dwell times and minimize operational disruptions.

Future risk assessments should incorporate adversarial machine learning (ML) testing to evaluate the resilience of AI-driven security solutions. As attackers refine their techniques to evade AI-based detections, defensive models must be continuously tested against evolving adversarial inputs to maintain accuracy and reliability. Quantum-resistant cryptographic adoption should also be explored in preparation for the eventual emergence of quantum computing threats that could compromise current encryption standards.

Verizon must continuously refine its security posture through red teaming, purple teaming, and automated breach simulation exercises. These assessments will provide empirical data on the effectiveness of current security controls, allowing for continuous improvement in threat detection, response automation, and resilience against AI-assisted cyber threats.

References

[1] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to integrating forensic techniques into incident response,” National Institute of Standards and Technology (NIST), Tech. Rep. SP 800-86, 2006. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-86/final

[2] Verizon, “2024 data breach investigations report,” Online Report, 2024. [Online]. Available: https://www.verizon.com/business/en-gb/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf

[3] M. E. Whitman and H. J. Mattord, *Principle of Information Security*, 7th ed. Boston, MA: Cengage, 2023.

[4] T-Mobile US, Inc., “2022 data breach incident,” Online Disclosure, 2022. [Online]. Available: https://www.t-mobile.com/news/network/data-breach-2022

[5] National Institute of Standards and Technology (NIST), “Computer security incident handling guide,” Online, Aug 2012, gaithersburg, MD, USA. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/61/r2/final

[6] J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton, and J. Sweetnam, “Data integrity: Detecting and responding to ransomware and other destructive events,” Online, October 2020, gaithersburg, MD, USA. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-26.pdf

[7] N. I. of Standards and T. (NIST), “Guide for cybersecurity event recovery,” Online Report, 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-184.pdf

[8] IBM Security, “Cost of a data breach report 2024,” Online, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[9] CrowdStrike Security, “Ransomware and data exfiltration: Double extortion attacks,” Online, 2024. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/data-exfiltration-ransomware/

[10] CrowdStrike Endpoint Protection, “Ransomware detection & response: Endpoint security,” Online, 2025. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-detection/

[11] Microsoft, “Prepare for ransomware attacks with a backup and recovery plan,” Online Technical Guide, 2024. [Online]. Available: https://learn.microsoft.com/en-us/security/ransomware/protect-against-ransomware-phase1