ACCG8086

Cyber Security, Governance Frameworks and Ethics

MACQUARIE University
SYDNEY·AUSTRALIA

Cybersecurity Roadmap Report

Name	Muntasir Md Nafis
Student ID	48312932
Session	02, 2025
Submission Date	13th September 2025

Table of Contents

Executive Summary:

This report analyzes two major cybersecurity breaches at Coinbase which are the 2023 phishing attack and the 2025 insider bribery case through the lens of the NIST Cybersecurity Framework (CSF). These incidents demonstrate that vulnerabilities at Coinbase arose not only from technical lapses but also from weaknesses in governance and organizational culture.

The analysis applies the CSF's five functions which are Identify, Protect, Detect, Respond, and Recover,showing how stronger risk assessments, awareness training, contractor oversight, and centralized monitoring could have mitigated both breaches. Governance frameworks such as ISO 27014 and COBIT emphasize accountability, while policy structures and cultural factors such as psychological safety and supervisory responsibility ensure consistent enforcement and reporting.

In synthesis, resilience at Coinbase requires more than compliance. Effective security emerges when technical safeguards, governance clarity, and cultural reinforcement operate together. By adopting the CSF as a living framework aligned with its mission of trust and transparency, Coinbase can strengthen long-term resilience and safeguard its reputation in global finance.

Introduction:

Cryptocurrency exchanges have become prime targets for cybercriminals due to their fast, global, and irreversible transactions. Coinbase, the world's third-largest exchange, is particularly attractive to adversaries because it manages billions in assets for millions of customers worldwide (Novinson, 2025). Its size and visibility make it an ideal case study to examine how human and technical weaknesses combine to create vulnerabilities.

Coinbase defines its purpose through its mission "to increase economic freedom in the world" by making cryptocurrency accessible for all. Its vision is "to build a trusted, user-friendly platform that brings crypto and Web3 into mainstream finance, empowering both individuals and institutions" (Coinbase, Our mission, strategy and culture, 2025) (Coinbase, About Coinbase, 2025). Coinbase's value statement emphasizes trust, transparency, compliance, and customer

security. Because these values place trust and security at the center of Coinbase's identity, any breach directly undermines its mission and reputation.

Two major incidents highlight these risks. In 2023, a phishing campaign tricked a Coinbase employee through SMS and a follow-up phone call, exposing limited employee data. In 2025, overseas contractors were bribed to leak customer records, leading to a $20 million extortion attempt. Together, these cases illustrate unintentional insider threats and malicious insider threats.

This report investigates the breaches, develops a cybersecurity roadmap for Coinbase using the NIST CSF framework, and critically evaluates how the organization could have responded differently. It applies key concepts which are CIA triad and ethics, security governance frameworks such as ISO 27014 and COBIT, policies and enforcement, and people, culture, psychological safety, and supervisory roles.

Case Study Overview:

Coinbase is a valuable case study because its recent breaches directly tested its mission, vision, and values. The company's mission is "to increase economic freedom in the world," and its vision is to "build a trusted, user-friendly platform that brings crypto and Web3 into mainstream finance." Its value statement emphasizes trust, transparency, and regulatory compliance, with security as a foundation of its services (Coinbase, About Coinbase, 2025) (Coinbase, Our mission, strategy and culture, 2025). However, the incidents of 2023 and 2025 demonstrated how gaps in governance and culture threatened these principles.

The 2023 phishing incident exposed Coinbase to unintentional insider threats. Attackers sent fraudulent SMS messages to employees urging them to log in, and one employee entered their credentials into a fake page. The campaign escalated into a phone call from an attacker posing as IT support, who attempted to gain deeper access (Coinbase, Social engineering – A Coinbase case study, 2023) (Toulas, 2023). Although the attacker obtained limited employee contact data, Coinbase's security controls, which included multi factor authentication and its Computer

Security Incident Response Team (CSIRT), prevented further compromise. Analysts linked the attack to the 0ktapus campaign, which had previously targeted Okta and Twilio (Montalbano, 2023). This incident illustrates how unintentional insider mistakes can create entry points for attackers, reinforcing the importance of governance frameworks and cultural practices that encourage quick reporting and escalation.

In contrast, the 2025 breach revealed the dangers of malicious insiders and weak contractor oversight. Criminals bribed overseas support staff to extract customer data, ultimately affecting more than 69,000 users (Lakshmanan, 2025) (Whittaker, 2025). The stolen information included names, addresses, masked banking details, government IDs, balances, and transaction histories. Attackers demanded a $20 million ransom, but Coinbase refused and instead launched a $20 million bounty for information leading to arrests (Vardai, 2025) (Kapko, 2025). This response aligned with Coinbase's value of transparency but exposed significant governance gaps in vendor management and access control.

The consequences of these breaches were significant. The 2023 incident had limited impact but highlighted the inevitability of human error. The 2025 breach, however, carried projected remediation and reimbursement costs of $180–$400 million (Whittaker, 2025). Coinbase responded with transparency blogs, reimbursements, stricter withdrawal verification, a new U.S. support hub, and stronger insider-threat monitoring. These actions underscored security as a shared responsibility between leadership, employees, and contractors. Together, the incidents show that governance gaps and cultural weaknesses magnify risks, framing the need for a structured cybersecurity roadmap based on the NIST CSF.

Cybersecurity Roadmap – NIST CSF v1.1

Introduction to the NIST CSF

The NIST Cybersecurity Framework (CSF) version 1.1 provides a flexible, risk-based structure to improve organizational resilience, making it highly relevant to Coinbase as both a financial and technology platform (NIST, 2018). Its five core functions are Identify, Protect, Detect, Respond, and Recover which form an adaptable roadmap that integrates governance, culture, and technical safeguards. Studies confirm its strengths and challenges in regulated sectors, stressing its suitability for financial institutions (Salas-Riega, 2025) (Adebola, 2025). This roadmap applies NIST CSF directly to Coinbase's breaches, aligning with concepts on governance frameworks, policy enforcement, and organizational culture to create a holistic defense.

Identify

The first step in strengthening Coinbase's cybersecurity posture is proper identification of risks, stakeholders, and governance structures. According to the NIST CSF's Business Environment (ID.BE), organizations must define their role in the supply chain and clarify mission-critical dependencies ((NIST), 2018). Coinbase is both an exchange and custodian of customer data.

The 2025 insider breach demonstrated that overseas contractors were weak points in this supply chain, aligning with ID.BE-4, which emphasizes mapping dependencies and critical functions (Lakshmanan, 2025) (Whittaker, 2025). In parallel, Governance (ID.GV) requires clear policies and alignment of cybersecurity responsibilities across internal teams and external partners ((NIST), 2018). Coinbase's failure to prevent insider bribery shows gaps in ID.GV-2, as roles and oversight of contractors were not adequately managed (Lakshmanan, 2025).

Risk assessment is another pillar of identification. The phishing attack in 2023 showed that even trained employees can fall victim to smishing, aligning with ID.RA-3 and ID.RA-4, which focus on documenting internal and external threats and evaluating potential business impacts (Toulas, 2023) (Coinbase, Social engineering – A Coinbase case study, 2023) (Montalbano, 2023). Similarly, the extortion attempt highlighted the need for ID.RA-5, requiring prioritization of threats and vulnerabilities (Whittaker, 2025).

Finally, Supply Chain Risk Management (ID.SC) is particularly relevant, as Coinbase depends heavily on outsourced support centers. Weak contractual safeguards and monitoring mechanisms violated ID.SC-3 and ID.SC-4, where third-party risk processes should ensure contractors meet cybersecurity obligations ((NIST), 2018) (Kapko, 2025). Strengthening these areas will create the foundation for the Protect function.

Protect

After identifying risks, the next step is to put protective safeguards in place to stop attackers from exploiting weaknesses. The phishing attack against Coinbase in 2023, which started with a fake SMS and follow-up phone call, showed how quickly a single mistake can put sensitive data at risk (Coinbase, Social engineering – A Coinbase case study, 2023) (Toulas, 2023).

To address this, the NIST Cybersecurity Framework highlights the need for Access Control. Subcategories such as PR.AC-1, PR.AC-4, PR.AC-6, and PR.AC-7 call for strong identity management, least-privilege access, and multi-factor authentication. For Coinbase, this means enforcing hardware-token MFA for all employees and contractors and regularly reviewing who has access to critical systems.

Another area is Awareness and Training. Subcategories PR.AT-1, PR.AT-3, and PR.AT-4 stress that all users, partners, and executives must understand their security responsibilities. This aligns with Coinbase's need to embed scam-awareness prompts, encourage training participation, and reward protective behaviors.

Finally, Protective Technology (PR.PT-1, PR.PT-4) emphasizes audit logging and network protection. If such monitoring had been stronger, the 2025 bribery scheme involving contractors could have been detected earlier. Studies confirm training and CSF adoption strengthen defenses. (Hussain Aldawood, 2020), and organizations that apply the CSF effectively strengthen their defenses (Adebola, 2025). Together, governance reforms and cultural reinforcement build a much stronger protective layer against phishing, bribery, and insider threats.

Detect

Detection is critical because protective measures alone cannot guarantee safety. In 2023, Coinbase's SIEM and CSIRT flagged anomalies within ten minutes of a phishing attempt, preventing escalation (Montalbano, 2023). This reflects the value of DE.AE-1 and DE.AE-2, which require establishing baselines of network activity and analyzing anomalies.

For Coinbase, implementation means expanding anomaly libraries, integrating phishing playbooks into detection tools, and simulating attack scenarios to sharpen analyst responses. The 2025 breach showed months-long contractor data leaks, violating DE.AE-3 and DE.AE-4.(Kapko, 2025). To implement these, Coinbase should centralize logs from internal and outsourced systems, deploy automated correlation engines, and mandate business-impact scoring of anomalies in real time.

DE.CM-1 and DE.CM-7 stress continuous monitoring and detection of unauthorized access. Coinbase must extend monitoring to third-party endpoints and require privileged access dashboards for managers. Finally, DE.DP-1 and DE.DP-4 highlight governance, defining roles for detection and requiring incident escalation reports to leadership. Research supports these reforms: blockchain traceability can track insider misuse, while continuous monitoring is a governance requirement (Salas-Riega, 2025). Together, these implementations make detection proactive and prepare Coinbase for faster, coordinated response.

Respond

A timely and coordinated response decides whether an incident remains contained or spirals into crisis. In the 2023 phishing case, Coinbase's CSIRT contained the attack quickly, but uncertainty slowed communication. In contrast, the 2025 insider bribery breach revealed weaknesses in escalation and stakeholder coordination (Kapko, 2025).

The NIST CSF emphasizes Response Planning (RS.RP-1), which requires predefined playbooks. For Coinbase, this means scenario-based plans for smishing, phishing, and insider extortion, complete with legal, regulatory, and customer communication steps ((NIST), 2018). Communications (RS.CO-1 to RS.CO-5) stress clarity and coordination. Coinbase must ensure staff know their roles, report incidents promptly, and share updates with law enforcement and regulators.

The CSO's promotion of tabletop exercises reflects RS.AN-1, where detection notifications feed into rehearsed responses (Novinson, 2025). Finally, Improvements (RS.IM-1, RS.IM-2) call for lessons learned to be embedded into future responses. Transparent engagement with stakeholders, already evident in 2025, must become institutionalized. By reinforcing governance clarity and cultural accountability, Coinbase can ensure responses are swift, credible, and resilient.

Recover

Recovery is more than technical restoration; it is about restoring trust and demonstrating resilience. The 2025 insider bribery breach, which led to remediation costs of $180–400 million, showed how inadequate recovery planning can magnify financial and reputational risks (Whittaker, 2025).

The NIST CSF highlights Recovery Planning (RC.RP-1), which requires a structured plan executed during or after incidents. For Coinbase, this means embedding recovery metrics into Board-level dashboards so that progress is tracked alongside prevention and detection ((NIST), 2018). Improvements (RC.IM-1, RC.IM-2**)** stress that lessons must be incorporated into future strategies.

Coinbase's decision to reimburse affected users and to launch a $20 million bounty not only mitigated harm but also aligned recovery with cultural values of transparency and accountability (Vardai, 2025). Finally, Communications (RC.CO-1 to RC.CO-3) require managing public relations, repairing reputation, and updating stakeholders. By pairing governance reforms with cultural reinforcement, Coinbase can use recovery not just to repair damage but to strengthen its mission and values (Salas-Riega, 2025) (Adebola, 2025).

The NIST CSF roadmap for Coinbase shows that resilience depends on integrating technical safeguards, governance frameworks, and cultural reforms. The 2023 smishing attack and 2025 insider bribery breach revealed how governance gaps and cultural weaknesses amplified risks, underscoring the need for accountability, psychological safety, and vigilance. More than a compliance tool, the CSF serves as a living framework that aligns Coinbase's mission of trust and transparency with long-term resilience.

Critical Evaluation

The purpose of this evaluation is to examine how the NIST Cybersecurity Framework (CSF) could have prevented Coinbase's major breaches in 2023 and 2025. Rather than retelling events, the focus is on how the Identify, Protect, Detect, Respond, and Recover functions provide safeguards that, if properly implemented, would have reduced the likelihood and impact of these incidents. Governance frameworks such as ISO 27014 and COBIT, policy structures including EISP, ISSP, and SysSP, and cultural reforms such as psychological safety and supervisory accountability are used to strengthen the analysis. Together, these elements demonstrate that resilience requires not only technical solutions but also cultural and organizational alignment.

2023 Phishing and Smishing Attack

The 2023 phishing attack exposed Coinbase to an unintentional insider threat when one employee fell victim to an SMS scam followed by a vishing call (Coinbase, Social engineering – A Coinbase case study, 2023) (Toulas, 2023). The NIST CSF provides several safeguards that could have prevented escalation. Under *Identify* (ID.RA-3, ID.RA-4), risk assessments should have classified smishing as a high-likelihood threat, regularly updated through threat libraries. Coinbase underestimated this vector, leaving staff unprepared. The Protect function highlights awareness and training (PR.AT-1 to PR.AT-4), where It shows that regular awareness programs reduce susceptibility to social engineering (Hussain Aldawood, 2020). And it further demonstrates that phishing evolves constantly, requiring scenario-based training and testing. Policy reinforcement through SysSPs could have mandated routine phishing simulations and strict escalation rules. Access control (PR.AC-6) is also crucial; enforcement of hardware-token MFA would have prevented credential misuse (Salahdine, 2019).

On the detection side, CSF calls for anomaly detection (DE.AE-1, DE.AE-2) and continuous monitoring (DE.CM-1). Coinbase's SIEM eventually flagged suspicious behavior, but if detection thresholds had been tied to KPIs such as "time-to-escalation," response could have been faster. Governance frameworks like COBIT and ISO 27014 emphasize board accountability for awareness and incident reporting, ensuring management prioritizes these safeguards. Finally, cultural reforms psychological safety and a supportive communication climate would have encouraged immediate reporting, rather than employees hesitating due to fear of blame. In short, the phishing breach was not inevitable; it revealed weaknesses in governance oversight and cultural reinforcement that CSF subcategories directly address.

2025 Insider Bribery and Extortion Breach

The 2025 insider bribery case demonstrated the risks of weak contractor oversight and poor supply chain governance. Attackers bribed overseas support staff to exfiltrate customer data,

leading to an extortion attempt of $20 million (Lakshmanan, 2025) (Kapko, 2025). The CSF's Identify function highlights supply chain risk management (ID.SC-3, ID.SC-4), which requires mapping dependencies and ensuring contractors meet security obligations. Weak contracts and minimal monitoring created exploitable gaps. In Protect, least-privilege access (PR.AC-4) and protective technology (PR.PT-1) would have reduced insider opportunities, limiting contractors to task-specific data.

The Detect function was notably absent in this case. DE.AE-3 and DE.AE-4 emphasize correlating event data and determining business impact. Coinbase lacked centralized logging across third-party endpoints, allowing bribery to persist for months. Detection processes (DE.DP-4) also require escalation protocols to leadership—another area that failed (Hou, 2020). Under Respond, predefined playbooks for insider bribery and extortion (RS.RP-1) would have guided legal, regulatory, and customer communication, ensuring faster coordination. Novinson notes that tabletop exercises reinforce this readiness (Novinson, 2025), but Coinbase had not rehearsed insider-extortion scenarios. Finally, Recover requires structured planning (RC.RP-1) and continuous improvement (RC.IM-1). Embedding recovery KPIs into board dashboards could have reduced remediation costs, which reached $180–$400 million (Whittaker, 2025).

Governance reforms under ISO 27014 would have clarified contractor roles within the organizational security framework. ISSPs could have mandated monitoring obligations for vendors, while SysSPs would define exact access levels for support staff. Culturally, Concepts of leadership tone and supervisory accountability would have helped establish shared responsibility. If contractors had been included as part of the security culture, rather than outsiders, the likelihood of bribery acceptance would have been reduced.

Balancing Culture and Technology

Both breaches illustrate that technical safeguards alone are insufficient without cultural and governance reinforcement. Technology such as hardware-token MFA, anomaly detection, and blockchain traceability can block attacks, but its effectiveness depends on people and oversight. Aldawood demonstrates that awareness improves behavior (Hussain Aldawood, 2020), while Khan explains why unintentional insider errors occur without systemic safeguards. Hussain shows how technology can trace misuse (Hussain Aldawood, 2020), and Salahdine emphasizes evolving social engineering tactics requiring updated defenses (Salahdine, 2019). Together, these studies support the case that CSF is a flexible skeleton, but its strength comes from cultural "muscle" and governance "nerves" that direct action. By embedding ISO 27014 principles of accountability, enforcing clear policies at all levels, and fostering a culture of psychological safety and vigilance, Coinbase can make CSF implementation sustainable and effective.

In evaluating Coinbase's breaches, both the 2023 phishing attack and the 2025 insider bribery incident could have been avoided if the NIST CSF had been fully applied. Failures stemmed not

only from technical lapses but also from cultural hesitation, poor governance, and weak policy enforcement. The critical lesson is that resilience arises when technical safeguards, governance structures, and culture work in concert. For Coinbase, aligning its mission of trust and transparency with CSF-driven reforms ensures that future incidents are less likely to escalate into crises, and that recovery efforts reinforce, rather than undermine, its reputation.

Conclusion

This report analyzed Coinbase's 2023 phishing incident and 2025 insider bribery breach using the NIST Cybersecurity Framework (CSF) version 1.1. The cases showed that weaknesses arose not only from technical gaps but also from insufficient governance and cultural shortcomings, which conflicted with Coinbase's mission of trust and transparency.

The NIST CSF's five functions illustrated how lapses in one area created broader vulnerabilities. In 2023, stronger awareness and access controls could have mitigated the phishing attempt, while in 2025, weak contractor oversight and delayed detection enabled insider bribery to escalate. These failures underscored that resilience depends on integrating governance, clear policy enforcement, and cultural reinforcement with technical safeguards.

Governance frameworks such as ISO 27014 and COBIT emphasize accountability; enterprise and system-specific policies ensure consistent enforcement; and cultural factors, including psychological safety and supervisory responsibility, sustain vigilance across all levels of the organization.

In synthesis, the analysis shows that effective security arises from the interaction of culture, governance, and technology. For Coinbase, applying the NIST CSF as a living framework provides a pathway to align security with organizational values, ensuring that resilience, trust, and transparency remain central to its long-term strategy.

References

(NIST), N. I. (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1.

Adebola, K. (2025). The Role of NIST Cybersecurity Framework in the Adoption of Could-Native Technologies in the Financial Service Sector . *International Journal of Computer Engineering and Technology(IJCET) , 16*(3), 490-512.

Coinbase. (2023). *Social engineering – A Coinbase case study*. Retrieved September 2025, from Coinbase Blog: https://www.coinbase.com/en-au/blog/social-engineering-a-coinbase-case-study

Coinbase. (2025). *About Coinbase*. Retrieved September 2025, from Coinbase: https://www.coinbase.com/en-au/about

Coinbase. (2025). *Our mission, strategy and culture*. Retrieved September 2025, from Coinbase: https://www.coinbase.com/en-au/blog/our-mission-strategy-and-culture

Hou, X. L. (2020). Insider Threat Detection Using Blockchain-Based Traceability in Digital Transactions. *Sensors, 20(18)* , 5297.

Hussain Aldawood, T. A. (2020, February). Does Awareness of Social Engineering Make Employees More Secure? *International Journal of Computer Applications , 177*, 45-49.

Kapko, M. (2025). *Coinbase flips $20M extortion demand into bounty for info on attackers*. Retrieved September 2025, from CyberScoop: https://cyberscoop.com/coinbase-cyberattack-extortion-counter-reward/

Lakshmanan, R. (2025). *Coinbase agents bribed, data of ~1% users leaked; $20M extortion attempt fails*. Retrieved September 2025, from The Hacker News: https://thehackernews.com/2025/05/coinbase-agents-bribed-data-of-1-users.html

Montalbano, E. (2023). *Coinbase crypto exchange ensnared in 'Oktapus'-related smishing attack*. Retrieved 2025 September, from DarkReading: https://www.darkreading.com/cyber-risk/coinbase-crypto-exchange-ensnared-oktapus-smishing-attack

Novinson, M. (2025). *Coinbase CSO: Crypto security demands fast, flexible defense*. (D. Today, Producer) Retrieved September 2025, from DataBreach Today: https://www.databreachtoday.com/coinbase-cso-crypto-security-demands-fast-flexible-defense-a-29210

Salahdine, F. a. (2019). Social engineering attacks: A survey. *Future Internet , 11(4)* , 89 .

Salas-Riega, J. R.-V.-S.-R. (2025). Cybersecurity and the NIST Framework: A Systemic Review of it's Implementation and Effectiveness Against Cyber Threats . *International Journal of Advanced Computer Science and Applications , 16*(6).

Toulas, B. (2023). *Coinbase cyberattack targeted employees with fake SMS alert*. Retrieved September 2025, from BleepingComputer: https://www.bleepingcomputer.com/news/security/coinbase-cyberattack-targeted-employees-with-fake-sms-alert/

Vardai, Z. (2025). *Coinbase faces $400M bill after insider phishing attack*. Retrieved September 2025, from Cointelegraph: https://cointelegraph.com/news/cyber-criminals-steal-coinbase-customer-data-20-m-ransom

Whittaker, Z. (2025). *Coinbase says customers' personal information stolen in data breach*. Retrieved September 2025, from TechCrunch: https://techcrunch.com/2025/05/15/coinbase-says-customers-personal-information-stolen-in-data-breach/