XECURITYPULSE

2025

HOW MILLIONS WERE COMPROMISED: WHAT TELECOM AUDITS COULD HAVE PREVENTED

XECURITYPULSE

TABLE OF CONTENTS

XECURITYPULSE

XECURITYPULSE

ABOUT THE AUTHOR

TAHA SAJID, CISSP, MSC

FOUNDER OF XECURITY PULSE

Taha Sajid is a leading voice in cybersecurity, known for his deep expertise in telecom security, zero trust architecture, AI, and blockchain technologies. As the Founder of Xecurity Pulse and a Principal Architect, he has helped shape security frameworks that strengthen digital infrastructure against modern threats.

With a career that spans enterprise, telecom, and government sectors, Taha has advised on and implemented cybersecurity strategies across complex environments. His work in Privileged Access Management (PAM), Identity and Access Management (IAM), and emerging security solutions has positioned him as a trusted expert in the field.

He is also a published author and co-author of the Blockchain Security Handbook, where he explores the challenges and solutions around securing decentralized systems. In addition to his technical achievements, Taha actively mentors professionals through EB1A coaching and contributes to global security programs as an Infosec Board Member.

Recognized with multiple industry awards, Taha continues to influence the future of cybersecurity through both innovation and leadership.

XECURITYPULSE

ABSTRACT

Telecom networks power global communication, yet many providers overlook one of the most critical elements of cybersecurity: the security audit. This whitepaper explores what happens when telecom operators skip regular audits and highlights the hidden consequences that can accumulate over time.

From misconfigurations that go undetected to legacy systems left exposed, the absence of structured auditing can leave telecom networks open to targeted attacks and systemic failures. Threat actors often take advantage of weak points in signaling systems, outdated firmware, or gaps in access controls that audits are designed to uncover.

We examine real-world scenarios where a lack of auditing led to major service disruptions, data breaches, and regulatory scrutiny. The paper also outlines how these oversights affect long-term trust, financial stability, and national infrastructure.

Through this analysis, the whitepaper offers practical guidance on how telecom providers can prioritize and implement effective audit programs. The goal is to provide decision-makers with a clear understanding of the risks involved and how to move toward a more secure, monitored environment that keeps pace with evolving threats.

XECURITYPULSE

INTRODUCTION

Telecom networks carry the world's conversations, transactions, and critical infrastructure traffic. As technology evolves, these systems grow more connected, layered, and exposed. With every upgrade, expansion, and integration, the potential entry points for attackers increase.

Security in telecom is not just about firewalls or encryption. It's also about knowing what's happening inside the network, where the weaknesses are, and whether controls are still effective. That's where telecom security audits come in. They help identify gaps in configuration, access, and policy before attackers do.

In many cases, organizations delay or skip audits due to time, cost, or operational pressure. This creates blind spots across the network. These blind spots are often exploited through outdated protocols, mismanaged access, or unmonitored interfaces. Once a vulnerability is used, the damage can spread quickly and silently.

This paper explores what happens when security audits are ignored or treated as a secondary task. It looks at the practical risks, operational impacts, and the broader consequences for service providers, regulators, and users. The goal is to understand why audit programs are more than a checkbox and how they fit into the larger strategy of telecom cybersecurity.

XECURITYPULSE

UNDERSTANDING THE ROLE OF SECURITY AUDITS IN TELECOM

Telecom systems rely on constant availability, complex architecture, and trusted communication. Security audits help verify whether these systems are protected, managed, and aligned with evolving risks.

2.1 WHAT IS A TELECOM SECURITY AUDIT?

A telecom security audit is a structured review of systems, configurations, and processes that affect the security of network operations. It involves evaluating the setup and controls of core network components, such as base stations, routers, switches, signaling systems, and interconnection points.

Key areas of review include password policies, remote access permissions, firewall rules, signaling traffic paths, and software patch levels. The audit also inspects third-party integrations, cloud-based systems, and identity management practices across the environment. The purpose is to spot hidden risks, confirm that security controls are working as expected, and uncover any deviations from internal or external standards.

2.2 WHY SECURITY AUDITS ARE CRITICAL IN TELECOM

Telecom networks are large, layered systems with hardware, software, and services running across many physical and virtual nodes. These networks often have older components still in use alongside newer technologies like 5G or containerized microservices. When these systems aren't reviewed regularly, vulnerabilities can stay unnoticed. A small configuration error or an unmonitored port may expose a wide area of the network. Attackers often search for these unnoticed gaps and use them to access core network functions or customer data. Audits help prevent these scenarios by forcing a detailed check on critical paths, especially those tied to signaling protocols, management interfaces, and internal APIs. Without this visibility, issues grow quietly until they lead to outages or breaches.

2.3 STANDARDS AND REGULATORY EXPECTATIONS

Security audits in telecom are not just technical best practices. In many regions, they are required by law or by regulatory authorities.

The ISO/IEC 27011 standard provides guidance for managing information security in telecom environments. It aligns with ISO/IEC 27001 but adapts the controls for telecom-specific contexts, like mobile switching centers and transmission networks.

GSMA publishes guidelines for mobile network security, including areas such as interconnection, SIM provisioning, and subscriber privacy. These documents help operators follow common practices across different countries and vendors.

Local laws and regulators often build on these frameworks. For example, the FCC in the United States may require periodic reporting and risk assessments, while in countries like India, the TRAI enforces audit requirements tied to licensing agreements. Data privacy laws such as GDPR also place additional pressure on telecom operators to document their security practices and prove compliance.

Audits are one way providers show that they understand their risks and are taking steps to manage them. They are also one of the first things regulators or partners review after a breach or service failure.

XECURITYPULSE

WHAT HAPPENS IF YOU SKIP A TELECOM SECURITY AUDIT

Telecom networks that go without regular audits become harder to manage and easier to exploit. Small issues that are easy to miss often grow into serious security gaps.

3.1 INCREASED VULNERABILITY TO CYBERATTACKS

Unaudited networks often carry risks that remain hidden until attackers find them. Outdated firmware, for example, may contain known exploits that remain unpatched for years. Legacy protocols like SS7 still run in the background of many mobile networks, exposing subscriber data and enabling location tracking or message interception.

Hardcoded credentials are another common issue. When systems are deployed and left untouched, default usernames and passwords often stay active across large segments of the network. This opens the door to lateral movement once a single point is breached.

Many networks also skip verification of trust boundaries. Without checks in place, devices and services that should be isolated can interact freely, making it easier for an attacker to move from a public-facing system to a critical internal one.

3.2 REAL-WORLD CASE STUDIES: BREACHES DUE TO NEGLECTED AUDITS

In several mobile networks, attackers have exploited SS7 flaws to intercept text messages used in two-factor authentication. These issues had been documented for years, but without audits, the vulnerabilities remained active and unnoticed.

SIM-swapping attacks have occurred in environments where identity verification systems were misconfigured. In one case, a mobile provider failed to validate API access between internal tools and third-party apps. Attackers used this gap to reassign phone numbers and bypass SMS verification.

Some 5G testbeds have also exposed management interfaces online without authentication. These were often meant to be temporary environments but were never reviewed or removed. In one example, researchers found dozens of unsecured endpoints tied to telecom prototypes running on public cloud infrastructure.

3.3 OPERATIONAL AND FINANCIAL IMPACT

A breach in a telecom network usually leads to immediate service disruption. Depending on the target, this can affect voice calls, internet access, or internal signaling functions. Restoring these services takes time, especially if the source of the issue is unknown or spread across multiple systems.

Regulatory agencies often respond to telecom breaches with investigations, which may include heavy fines or audits imposed by third parties. In many countries, telecom operators are required to report such incidents within a fixed time, which can increase reputational damage.

Customer trust also takes a hit. People rely on telecom providers for basic communication. When that trust breaks, customers may leave the network or reduce their usage. In competitive markets, even short-term damage can result in long-term revenue loss.

On top of this, the cost of forensics, patching, and legal support adds to the overall impact. All of this is far more expensive than what it would have taken to run regular audits in the first place.

XECURITYPULSE

HOW CYBERCRIMINALS EXPLOIT AUDIT GAPS IN TELECOM

Attackers often target areas that go unchecked during day-to-day operations. Without audits, these weak points stay active for years and serve as easy entry paths.

4.1 EXPLOITING LEGACY SYSTEMS

Many telecom networks still rely on legacy systems that were never designed with modern security in mind. Interfaces like SNMPv1 or Telnet are sometimes still used in production for device management. These protocols transmit data in plain text and often have weak or no authentication. Attackers scan for these interfaces across public IP ranges. Once found, they can extract device configurations, change routing settings, or disrupt network services.

In some cases, these systems are tied to critical signaling functions or customer data platforms. Lack of audit routines means these outdated tools stay online even when they are no longer needed. They are rarely logged or monitored, which gives attackers time to explore without detection.

4.2 INSIDER THREATS AND UNMONITORED ACCESS

Insiders present a risk when permissions are too broad or left unchecked. Contractors or former employees may still have access to internal tools or management systems long after their engagement ends.

Without regular audits, identity and access records often become outdated. Privileged accounts are not reviewed, and access logs are never analyzed. This creates a quiet opportunity for insiders to steal data, modify configurations, or create backdoors.

In some cases, access is granted through shared accounts that are never rotated. If a breach happens, it becomes difficult to trace activity back to a specific individual. Audit gaps make it easier for these events to stay hidden until long after the damage is done.

4.3 LATERAL MOVEMENT AND PIVOTING FROM TELECOM NETWORKS

Telecom systems often sit at the edge of multiple industries. From government to banking, many organizations rely on these networks for core connectivity.

Attackers who breach a telecom system can use it as a starting point to move into other targets. They can monitor enterprise traffic, inject malicious commands into signaling paths, or exploit shared interconnects to access downstream clients.

Once inside, attackers might use compromised routers, DNS records, or messaging gateways to escalate privileges elsewhere. In some attacks, telecom systems have been used to reach military communication nodes or intercept credentials passed over unencrypted channels.

Audit trails are the only way to catch this kind of movement early. Without them, these attacks often continue unnoticed across multiple sectors.

XECURITYPULSE

LONG-TERM CONSEQUENCES FOR NEGLECTING SECURITY AUDITS

When security audits are ignored, the damage doesn't end with a single breach. It affects trust, reputation, and even national security in ways that are difficult to repair.

5.1 TRUST EROSION AMONG STAKEHOLDERS

Telecom providers handle sensitive data and critical services. If they experience repeated breaches or fail to explain security lapses, customers begin to look for alternatives. Large enterprise clients may move contracts elsewhere. Even business partners and technology vendors may question the reliability of future collaborations.

This shift isn't just about brand image. In many cases, long-standing relationships break down due to poor security practices that went unchecked for too long. Once that trust is lost, it rarely returns.

5.2 REPUTATIONAL AND REGULATORY FALLOUT

Privacy laws like GDPR and CCPA place direct accountability on organizations that collect or process personal data. If a breach is tied to poor oversight or missing controls, regulators can impose heavy penalties. These penalties may include both fines and required operational changes.

Telecom regulations in many countries require periodic risk assessments and security reviews. Failing to follow them can lead to suspension of licenses or public disclosure of audit results. Even in less regulated markets, public backlash often pushes telecom companies to spend more on crisis management than they would have on prevention.

News coverage, legal exposure, and loss of investor confidence all pile onto the aftermath. Some companies spend years trying to rebuild credibility after a serious security lapse.

5.3 NATIONAL SECURITY RISKS

Telecom infrastructure supports more than everyday communication. It also underpins emergency response, military logistics, and critical public services. A vulnerability in these systems can disrupt national operations or expose government communications.

In some regions, foreign adversaries have used telecom weaknesses to track political figures, intercept classified exchanges, or map network topologies for future use. These threats are difficult to contain once the system has been breached.

Security audits help identify these weak links early. Without them, telecom providers may unknowingly become a gateway for larger national threats. The consequences of this go far beyond business risk.

XECURITYPULSE

IMPLEMENTING A PROACTIVE SECURITY AUDIT PROGRAM

A proactive audit program helps detect vulnerabilities before they become problems. Regular reviews prevent minor issues from escalating into major risks that can harm your telecom network and reputation.

6.1 KEY AUDIT COMPONENTS FOR TELECOM SECURITY

Security audits should cover several areas, each addressing a different aspect of the network's health.

- **Penetration Testing:**

Penetration testing simulates real-world attacks to uncover weaknesses in your network. These tests help identify vulnerabilities in systems, protocols, and configurations before attackers can exploit them.

- **Identity and Access Audits:**

Review user roles and permissions to ensure that only authorized individuals have access to sensitive data or systems. This includes checking for inactive accounts, inappropriate access levels, and misconfigured access control settings.

- **Signaling Security Checks (e.g., SS7, Diameter):**

Older signaling protocols like SS7 and Diameter are still widely used in telecom networks, but they are prone to exploitation. Regular checks can identify vulnerabilities in these protocols, such as unauthorized message interception or traffic rerouting.

- **Cloud and Container Security:**

For modern telecom networks, security extends to cloud infrastructure and containerized environments. Audits should assess cloud service providers, containerized applications, and network boundaries to ensure proper security measures are in place.

6.2 RECOMMENDED AUDIT FREQUENCIES AND TRIGGERS

Audits should be carried out regularly and after specific events.

- **Regular Audits:** Quarterly or annual audits are recommended to maintain ongoing visibility into network security. These reviews provide enough time to detect minor issues before they turn into major vulnerabilities.

- **Event-Triggered Audits:** Additional audits should be triggered after any significant event, such as system upgrades, changes in network architecture, or after a security breach. These audits ensure that new changes haven't inadvertently opened up new risks or vulnerabilities.

6.3 TOOLS AND SOLUTIONS THAT STREAMLINE TELECOM AUDITS

Several tools can simplify and speed up the audit process.

- **Nessus:** Nessus is commonly used for vulnerability scanning. It helps identify security flaws across a wide range of network devices and services.

- **Wireshark:** Wireshark is a packet analyzer that helps telecom teams monitor and capture network traffic. It can be especially useful for identifying malicious activity or weaknesses in data transmission.

- **5G Penetration Frameworks:** As 5G networks expand, specialized penetration testing tools have been developed to assess the unique security risks these networks pose. These tools help ensure 5G systems are as secure as possible.

- **SIEMs (Security Information and Event Management):** SIEMs aggregate and analyze data from different security systems. By leveraging real-time monitoring and event correlation, SIEMs help detect unusual activities and potential threats before they escalate.

- **Orchestration Platforms:** Orchestration platforms help automate security monitoring, making it easier to manage large-scale networks. These platforms integrate various tools and workflows, simplifying the audit and response process.

XECURITYPULSE

RECENT TELECOM SECURITY INCIDENTS

Several high-profile attacks in recent years have revealed the growing security gaps in telecom networks. These cases show how overlooked vulnerabilities can quickly escalate into major disruptions and data loss.

SK TELECOM BREACH (APRIL 2025)

In April 2025, South Korea's largest mobile carrier, SK Telecom, faced a serious cybersecurity breach. The attack targeted the Home Subscriber Server (HSS), a core element of mobile communication networks. Hackers deployed malware that may have accessed sensitive SIM-related data, including IMSI, IMEI, and USIM authentication keys. While the company stated no personal information such as birth dates or bank account details was leaked, the full scale of the exposure is still under investigation. This incident revealed how critical backend systems, if left unchecked, can become entry points for deep network compromise, even in technically advanced markets.

OPTUS DATA LEAK (2022)

Australian telecom company Optus was breached in 2022 due to an unauthenticated API endpoint left exposed online. Hackers were able to access data of more than 10 million customers, including license numbers, addresses, and phone numbers. The breach sparked a national conversation around API security, data retention policies, and corporate accountability. It was later revealed that basic security testing and audit procedures could have flagged the exposed endpoint before it was exploited.

HOW MILLIONS WERE COMPROMISED:
WHAT TELECOM AUDITS COULD HAVE PREVENTED

XECURITYPULSE

IRANIAN MOBILE NETWORK DISRUPTION (2022)

In late 2022, Iran's telecom infrastructure was disrupted by a coordinated cyberattack that affected mobile and internet services across the country. The attack reportedly bypassed internal defenses by exploiting poor network segmentation and weak logging mechanisms. The lack of real-time monitoring made detection and containment slow. This case showed how insufficient visibility into internal systems can turn localized attacks into nationwide service outages.

TELETALK BANGLADESH ADMIN ACCESS EXPLOIT (2023)

In 2023, Teletalk, Bangladesh's state-owned telecom provider, experienced a breach involving stolen administrative credentials. The attackers gained access to backend systems and disrupted billing services. Investigations revealed that the provider lacked proper Privileged Access Management (PAM) controls and failed to implement multi-factor authentication for high-level accounts. A routine security audit would have highlighted these gaps, helping to secure administrative access points and protect internal assets.

XECURITYPULSE

ROLE OF NECAS AND SCAS IN MITIGATION

The Network Equipment Security Assurance Scheme (NECAS) and the Security Compliance Assurance Scheme (SCAS) have emerged as vital frameworks for telecom cybersecurity. These standards offer a structured way for telecom vendors and operators to evaluate and strengthen their infrastructure security.

NECAS focuses on the security of network equipment such as routers, switches, and base stations. It enforces standardized testing for known vulnerabilities, secure software updates, and firmware integrity. Adopting NECAS ensures that telecom providers aren't blindly integrating hardware into their networks without assurance of its security posture.

SCAS complements this by providing a broader compliance framework that covers the operational lifecycle of telecom networks. It assesses security across areas such as configuration management, incident response, access control, and software patching. SCAS audits can uncover misconfigurations or outdated software that attackers often exploit.

Together, NECAS and SCAS offer a comprehensive approach to telecom security, closing the gaps left by ad hoc security practices. By integrating these schemes into their regular audit routines, telecom providers can significantly reduce exposure to both known and emerging threats.

HOW MILLIONS WERE COMPROMISED: WHAT TELECOM AUDITS COULD HAVE PREVENTED

XECURITYPULSE

FUTURE-PROOFING TELECOM THROUGH CONTINUOUS AUDITING

As telecom networks become more complex, traditional security audits must evolve to address the growing risks. Continuous auditing helps ensure long-term security, providing ongoing visibility into potential threats and compliance gaps.

9.1 CONTINUOUS MONITORING VS. PERIODIC AUDITING

While periodic audits have served telecom security well in the past, they are no longer enough on their own. Point-in-time audits can miss emerging threats that develop in between review periods. Continuous monitoring, on the other hand, provides real-time insights into network activity, making it easier to detect irregularities or unauthorized access as they happen.

With continuous monitoring, data is constantly reviewed and assessed for security risks. This approach offers faster response times, reduces the chances of undetected vulnerabilities, and helps maintain compliance with ever-changing regulations.

9.2 INTEGRATING AI/ML INTO TELECOM SECURITY POSTURE

Machine learning (ML) is becoming an integral part of modern telecom security. AI-driven tools can analyze vast amounts of network traffic and behavior patterns, identifying unusual activity that might otherwise go unnoticed in manual audits.

ML models can learn typical network behavior over time and flag deviations that might indicate a breach or misconfiguration. By automating this process, telecom providers can stay ahead of new threats without relying on human intervention alone. This integration helps improve overall audit efficiency and effectiveness.

9.3 ZERO TRUST IN TELECOM: AUDIT AS THE FOUNDATION

The Zero Trust model operates on the principle of "never trust, always verify." It requires constant authentication and validation of every user, device, and network request, regardless of origin.

In a Zero Trust framework, continuous auditing plays a key role in maintaining security. Every access request is continuously monitored and reviewed, ensuring that permissions are always aligned with the principle of least privilege. This reduces the risk of unauthorized access and minimizes the potential impact of internal threats.

By tying auditing to Zero Trust, telecom providers can enforce tighter controls and keep their networks secure from both external and internal threats.

XECURITYPULSE

CONCLUSION & STRATEGIC RECOMMENDATIONS

Skipping security audits in telecom creates space for risk to grow unnoticed. What looks like a cost-saving decision in the short term can lead to deeper problems later, such as data breaches, disrupted service, and lost customer trust.

Security audits are meant to catch what regular operations overlook. They bring clarity, expose misconfigurations, and test whether systems hold up under pressure. Without them, vulnerabilities stay hidden until something breaks.

To move forward with fewer surprises, telecom operators should treat audits as part of their regular rhythm, not as a one-time fix. Continuous monitoring helps identify issues early and respond faster. Automation reduces errors and speeds up repetitive tasks, especially in complex environments. Adopting a model where no part of the network is blindly trusted helps close gaps attackers often exploit. And keeping teams updated through regular training ensures that people stay sharp and prepared for new threats.

Telecom environments are complicated. Having the right support makes a difference. Xecurity Pulse helps telecom providers, vendors, and national regulators build and maintain secure networks. From detailed architecture reviews to 5G security testing and implementation plans, they bring field-tested experience to real-world telecom security.

Audits are more than reports. When done right, they prevent damage, protect uptime, and create space for confident growth. The choice is not whether to audit. It is when, how often, and who to trust with the process.

XECURITYPULSE

REFERENCES

- **The Importance of Performing a Telecom Audit**
  - https://verityit.com/the-importance-of-performing-a-telecom-audit-saving-money-increasing-efficiency-and-staying-competitive/

- **Security Audits:** ***A Comprehensive Overview***
  - https://auditboard.com/blog/what-is-security-audit/

- **Simplifying Telecom Security:** ***What You Need to Know***
  - https://www.lifecycle-software.com/resources/simplifying-telecom-security

- **Cyber Security Audit:** ***Why Your IT Department Should Not Fear It Network Security?***
  - https://www.grandmetric.com/cyber-security-audit-reasons-to-do-it/

- **Network Security Audit:** ***A Comprehensive Overview in 2025***
  - https://qualysec.com/network-security-audit/

- **Elevating Telecom Security:** ***The Role of Penetration Testing***
  - https://www.p1sec.com/blog/elevating-telecom-security-the-role-of-penetration-testing

XECURITYPULSE

2025

THANK YOU!

XECURITY-PULSE

SUPPORT@XECURITYPULSE.COM

HTTPS://XECURITYPULSE.COM/