Journal of Digitovation and Information System

http://jdiis.de/index.php/jdiis

Integrated Cyber Resilience in Banking: Examining the Role of Technology, Human Expertise, and Regulation

Khawla Elkhoundafi*

Institut Mines-Telecom Business School, France

Abstract

This research explores the integration of technological safeguards, regulatory frameworks, and employee-based practices to enhance cyber resilience within a large French banking institution. Drawing on qualitative insights from structured interviews with professionals involved in cyber resilience projects, the analysis identifies key operational strategies implemented to prepare for, respond to, and recover from cyber incidents. A thematic evaluation reveals the coordination of secure infrastructure systems, encrypted recovery procedures, and structured human intervention mechanisms supported by periodic training and simulation exercises. The findings also highlight how compliance with evolving regulatory requirements such as the Digital Operational Resilience Act (DORA) shapes organizational preparedness and communication protocols. Despite the institution's progress in implementing proactive frameworks, challenges remain in managing activity prioritization, anticipating attack forms, and maintaining clarity in interdepartmental responsibilities. The study contributes to resilience theory in cyber governance by underscoring the value of integrated frameworks that include technical, human, and regulatory perspectives. The analysis is grounded in a single institutional context and the implications offer practical relevance for financial institutions seeking to align operational continuity with adaptive cyber preparedness. Future research should expand on these findings through comparative analysis across institutional contexts and include quantitative evaluation of incident response outcomes.

Keywords

Cyber Resilience; Cybersecurity; Human Expertise; Regulatory Frameworks; French Banking

Article Information

Received 05 January 2025
Revised 31 March 2025
Revised 30 April 2025
09 May 2025
Accepted 20 May 2025

https://doi.org/10.54433/JDIIS.2025100048
ISSN 2749-5965

1. Introduction

In an increasingly interconnected financial environment, cyber resilience has become a strategic necessity for banking institutions. Cyber resilience refers to an organization's capacity to anticipate, withstand, recover from, and adapt to adverse cyber events (Linkov et al., 2023). As banking institutions continue to adopt advanced technologies such as cloud computing, artificial intelligence (AI), and blockchain, they are simultaneously exposed to evolving cyber risks that challenge traditional security frameworks (Almagribi & Putranto, 2025; Eshmawi et al., 2025). Financial institutions must protect vast amounts of sensitive customer data and ensure service continuity in the face of operational disruptions. The integration of cyber threat intelligence, both technical and behavioral, is particularly important in improving detection, prevention, and recovery capacities (Avrahami & Zwilling, 2025). Furthermore, human-centered approaches remain critical, as the effectiveness of cyber resilience frameworks depends not only on technological tools but also on the preparedness and awareness of personnel (Colabianchi, 2023). As cyber risks evolve, especially in data-intensive sectors such as banking, institutions are compelled to align their resilience strategies with emerging regulatory

*Corresponding author: e-mail addresses: khawlakhoundafi@gmail.com (K. Elkhoundafi) standards and technological trends (Okusi et al., 2025). The structure of banking systems inherently involves numerous external interfaces, including service providers, cloud platforms, and digital payment ecosystems. These interfaces increase exposure to external threats. Implementing a cyber resilience strategy entails classifying critical operations, applying tailored protection measures, establishing real-time breach detection mechanisms, and developing recovery protocols. These elements form the foundation for building adaptive systems that maintain operational capacity under disruptive conditions.

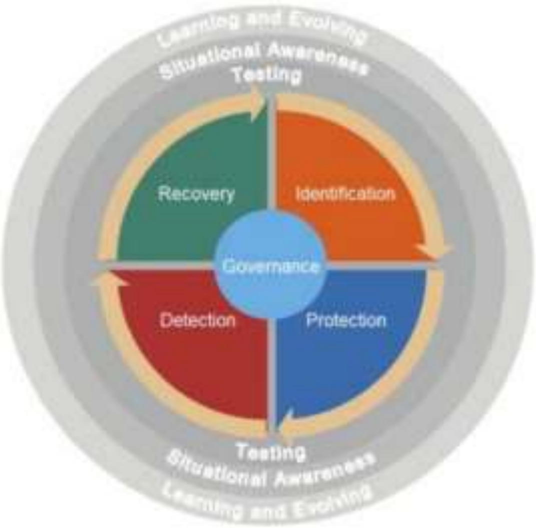

Figure 1. Cyber resilience guidance components

Resilience practices in the banking sector are not only technical but also organizational, ensuring continuity, trust, and compliance. The integration of cyber intelligence frameworks, automation, and secure authentication technologies such as Multi-Factor Authentication (MFA) and Artificial Intelligence (AI) applications has become more common. However, these tools alone cannot fully address emerging threats. Strategic implementation depends on training employees, reinforcing awareness, and aligning behaviors with institutional cybersecurity objectives (Avrahami & Zwilling, 2025). The role of human behavior and learning remains a key factor in supporting secure digital environments, particularly where human error can amplify the risks posed by technical vulnerabilities (Colabianchi, 2023). Equally important is regulatory compliance. National supervisory bodies such as the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) provide detailed frameworks to guide institutions in strengthening resilience. Ensuring that cyber resilience strategies comply with regulatory expectations requires coordinated efforts between cybersecurity and compliance departments. The failure to meet such expectations not only risks operational disruption but may also result in reputational and financial consequences (Okusi et al., 2025). This research focuses on how the integration of advanced technologies and human-centered practices can improve cyber resilience within the banking sector. The analysis is based on a case study of a major French banking institution currently developing a cloud-based solution designed to isolate client data in a secure environment outside the main information infrastructure. This initiative reflects a broader strategic shift in European banking toward more compartmentalized and resilient system architecture.

Given this background, the following research questions are explored:

- To what extent are current cyber resilience practices effective in countering evolving cyber threats?
- How can cyber resilience strategies be optimized to improve their implementation in the banking sector?

These questions are designed to examine both the technical and human dimensions of cyber resilience, while assessing the regulatory, organizational, and technological elements that contribute to its success.

2. Literature Review

. The reviewed literature offers a foundation for analysing how cyber resilience operates within banking institutions. Research highlights the importance of technological, regulatory, and human factors as integral components of institutional readiness. Table 1 summarises selected peer-reviewed articles related to the thesis scope. These were obtained through platforms including Google Scholar, Central Banking, Cairn, and ScienceDirect. The articles span the past decade, capturing relevant developments in cybersecurity and resilience within financial systems.

Table 1. Literature Review Table

Paper Title	**Objectives/Research Question**	**Theory/Model/Fra Mework**	**Methodology**	**Results**
(Tzavara & Vassiliadis, 2024)	To define cyber resilience and it difference from cyber security, also its components, framework and applications	NIST Cyber security framework's Impact	Literature review	The study emphasizes the importance of not only defending against cyber threats but also focusing on recovery, learning, and evolving from incidents.
(Kondratyeva et al., 2021)	To highlight the importance of information Technologies in maintaining the necessary level of security and improving the protection and resilience of banking systems	Paperless office technology (facilitation of electronic Interaction between banks and clients with minimization of paper usage) Deactualization risks and social engineering (client engagement and awareness), IS psychology, Regulatory and Supervisory Technology(optimize regulatory compliance)	Qualitative research	The implementation of IT represents an opportunity for banking industries to ensure their systems but it still new and result some failure and information leak
(Zimmermann & Renaud, 2019)	It proposes a new mindset that Recognizes the complexity, interconnectedness, and emergent qualities of socio- technical system, individuals are potential contributors to cyber security and focuses on improving factors that promote positive outcomes and resilience	Process and Simplify it), Biometric Identification based on unique human parameters like fingerprints, face) the socio-technical system: it is better to treat each member of the socio-technical system as an equal partner and leverage the strengths of each partner to create synergy	Quantitative research	It proposes a change in mentality that recognizes that errors and successes are an integral part of human work, and that the variability of human performance can contribute to both errors and successes.
(Khan et al., 2023)	To examine the use of biometric system in enhancing cyber resilience against threats of the banking sector	Different AI features, FinThech	Literature review	It is important for banks to integrate Biometrics identification into their security system to combat cyber threats but also adopting new technologies such AI.
(Dhashanamoorthi, 2021)	To determine the current and future use of AI, its benefits and challenges and how to overcome them by using ethical aspects, human intervention, education and regulation		Qualitative research	AI is transforming the cyber security and cybercrime prevention in the banking and financial sector by enhancing the efficiency, quality, and security of the services.
(Galinec & Steingartner, 2017)	To make the difference between	SD model: methodological	Quantitative research	Cyber Security is focused on

	cyber resilience and cyber security	framework for modelling and simulation of cyber resilience, modelling of socio- technical system involving human, organization and technological components		protecting IT systems,deal with known threats, cyber resilience ensure business continuity and stricung to save-to-fail, deal with unknown and unexpected threats
(Dupont, 2019)	To explore the concept of cyber-resilience and its applicability to the online security of financial institutions	Collapse ladder model: visualizes the cascade of decisions in crisis management, it shows how these decisions can prevent and control or destabilizing and destruction	Qualitative research	Cyber security industry is a promoter of cyber resilience as the future of security. Integration of cyber resilience in several Cyber security standards
(Fenjan, 2025)	To highlight the growing importance of cyber resilience in the financial sector			Cyber resilience is significant in maintaining stability and functionality of cyber incidents The importance of managing technology, people and process
(Sharkov, 2016)	The transition from cyber security to cyber resilience in order to combat cyber threats		Qualitative research	Preparing organization s and nations for unknown unknowns with 3levels: information security, cyber security, and cyber resilience
(Vimal Mani, 2021)	To explain the implementation of cyber resilience steps in organization regarding some aspects	Did security architecture: if controls positioned in one layer fail, the controls positioned in the other layers will still ensure the safety and security of the organization	Qualitative research	Choosing The cyber resilience architecture that suit organization objectives, be aware of different cyber resilience measures, the contribution of its people is important to have a strong cyber resilience, having effective guidelines and cyber security standards
(Saha et al., 2025)	The importance of risk management in cyber security, which involves identifying, evaluating, and reducing risks to ensure the confidentiality, integrity, and availability of information systems	The Business Impact Analysis	Qualitative research	Best practices such as risk assessment, governance and leadership, regulatory compliance, incident response planning cyber security laws and regulations, raising employee awareness of security. encrypting sensitive data technology: machine

learning algorithms and AI analyze data to identify patterns and potential risks, Automated vulnerability scanning Tools identify system weaknesses, while threat intelligence platforms collect and disseminate information on threats, AI-based platforms streamline incident Response processes. Human factor**:** training, awarenes, implementing clear security policies, educating on secure telecommute ng practices, authentication, reviewing access permissions, setting up channels for reporting incidents, providing incentives for good practices, and communicat ing about emerging threats Zero trust, EDR, XDR, AI…. Future Technologies two-factor

Cyber resilience and cybersecurity are often conflated, though they refer to distinct constructs. Cybersecurity typically involves preventive and defensive tools, while cyber resilience encompasses preparation, resistance, recovery, and continuity in the aftermath of digital disruptions (Linkov et al., 2023). A resilience-focused organisation is structured to maintain critical operations even during security incidents (Muhammad & Siraj, 2025). The National Institute of Standards and Technology (NIST) outlines five stages: identify, protect, detect, respond, and recover. These stages guide organisations in structuring their resilience processes. Various actors are involved, including cybersecurity vendors, internal staff, and regulators. Each contributes to security through infrastructure protection, operational awareness, and adherence to compliance requirements.

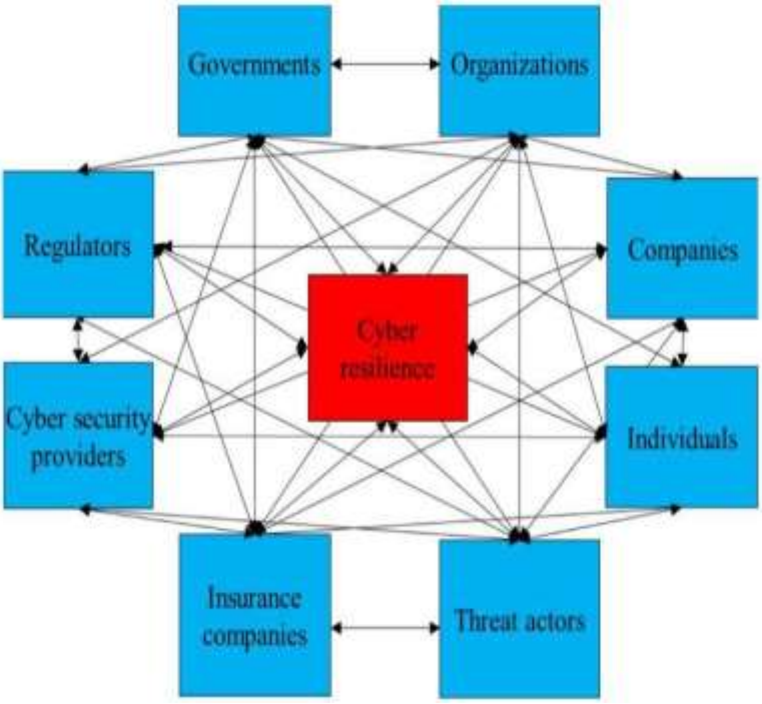

Figure 2. Actors Involved in Cyber Resilience

2.1. *Cybersecurity Technologies as Enablers of Resilience*

The adoption of cybersecurity technologies is central to achieving cyber resilience in banking. Cybersecurity operates as a support mechanism for resilience, contributing directly to detection and continuity systems (Dupont, 2019). With technologies such as machine learning, anomaly detection, and automation, banks gain the ability to respond rapidly to emerging threats (Adejumo & Ogburie, 2025). These tools support real-time fraud detection, user authentication, and network monitoring. Artificial intelligence systems also improve customer support efficiency and automate response processes. Cyber resilience is concerned not only with responding to known threats but also with adapting to new threat forms that may not fit existing patterns (citation needed). Banking institutions face ransomware, phishing, and data manipulation attacks that require flexible system design and risk response frameworks (Muhammad & Siraj, 2025). Resilience therefore involves continuous system adjustment and risk anticipation rather than just traditional defence.

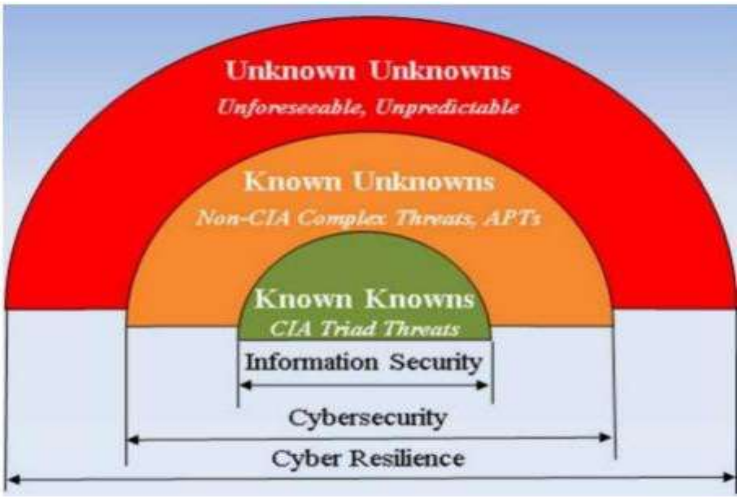

Figure 3. Cyber Resilience Model

2.2. *Integrating Human Factors into Resilience Strategies*

Technological systems alone cannot fully ensure resilience. Human participation in detecting, reporting, and managing incidents remains essential. Effective frameworks promote the ability to anticipate, monitor, respond, and learn from cyber events. Tools like biometric identification and secure digital channels depend on proper human interaction and oversight. Training programs ensure that staff can identify threats, follow response protocols, and contribute to security cultures(Galinec & Steingartner, 2017). Organisations are beginning to shift their view of employees from potential liabilities to contributors to resilience strategies. Investments in workforce education strengthen internal awareness and long-term sustainability. Humans are effective at tasks requiring decision-making under uncertainty, especially when threat conditions do not align with automated rule sets (Zimmermann & Renaud, 2019). By aligning human and technological resources, institutions improve their operational continuity and response performance across departments.

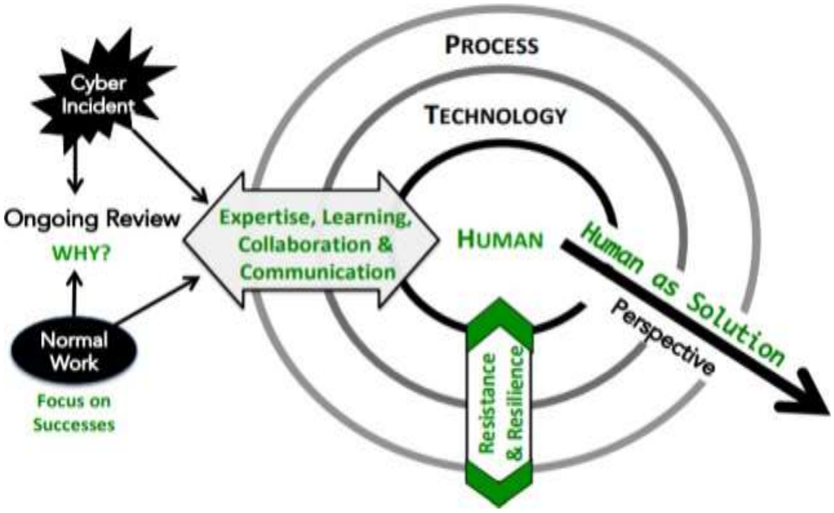

Figure 4. New Perspective of Human as a Solution

2.3. Regulatory Dimensions of Cyber Resilience

Regulatory bodies play a central role in establishing security benchmarks and resilience expectations for banks. Entities such as the European Banking Authority (EBA) and the Prudential Regulation Authority (PRA) provide operational guidance for regulated financial institutions. These frameworks shape how institutions structure their cyber response plans and evaluate incident recovery procedures. A tiered model of regulation has emerged, starting with awareness and leading to institutionalised resilience practices. For example, the Bank for International Settlements, in partnership with IOSCO, has issued resilience recommendations for financial market infrastructures. Similarly, the Basel Committee has developed comparative assessments to evaluate resilience maturity across jurisdictions (ENISA, 2021). These guidelines are designed to standardise recovery benchmarks and ensure transparent reporting mechanisms. In addition, regulators increasingly use consultations, assessments, and feedback loops to evaluate practical implementation across institutions. Such systems build accountability between governance structures and operational teams responsible for real-time resilience enforcement.

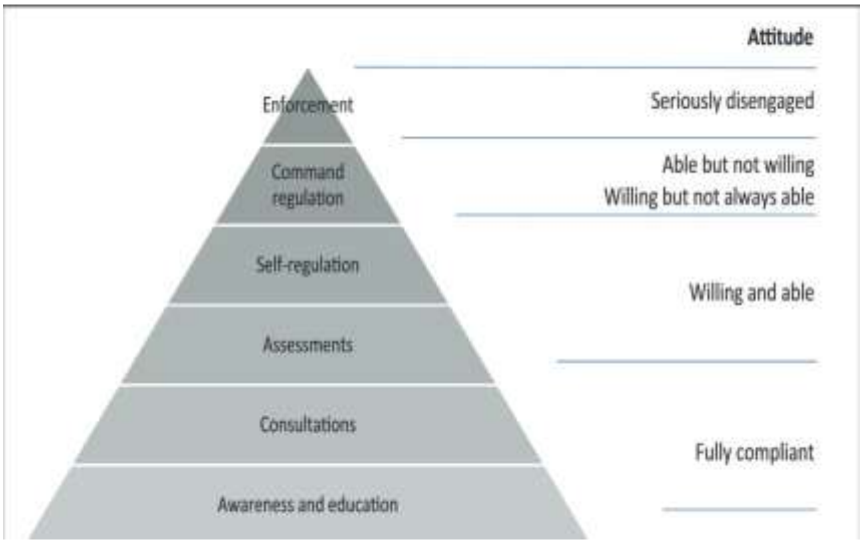

Figure 5. Cyber Resilience Regulatory Pyramid

The literature consistently identifies three core elements shaping cyber resilience in banking: technological capacity, human agency, and regulatory frameworks. While each area contributes to resilience independently, the greatest impact is observed when they function in an integrated and strategic manner. This interaction is captured in the following conceptual model.

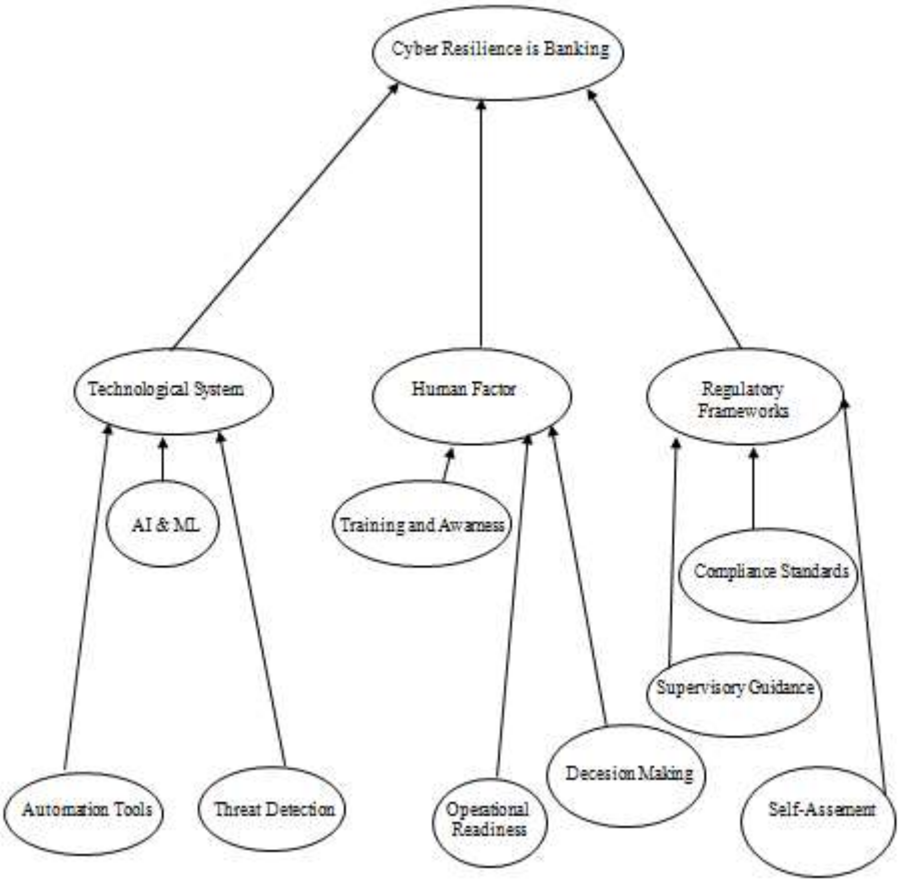

Figure 6. Factors Impacting Cyber Resilience in Banks

3. Methodology

3.1. Data Collection

This research employed a qualitative methodology to explore the interaction between cybersecurity technologies, employee involvement, and regulatory structures in shaping cyber resilience within a major French public bank. The qualitative approach allowed for in-depth insights from individuals with practical experience, which is essential when investigating organisational processes and perceptions (Denzin, 2018; Yin, 2018). The primary data was gathered through semi-structured interviews with professionals directly involved in the bank's cyber resilience project, which had been ongoing for over three years. A purposive sampling strategy was used to identify participants with operational knowledge and direct engagement in resilience-related activities. This included IS programme directors, IT support personnel, crisis managers, cybersecurity controllers, and analysts. A total of 11 participants took part in the interviews, all of whom were employees within the same institution. This sampling approach is commonly used in organisational research for its ability to capture relevant perspectives (Palinkas et al., 2015). The interviews were conducted via Microsoft Teams to accommodate participant availability. Questions were shared in advance to allow adequate preparation, and interviews were recorded using OBS software with full participant consent. All sessions were conducted in French to allow more fluent expression. Transcription and translation were completed before analysis to ensure fidelity and context accuracy. The project examined how technological solutions, human decisions, and regulatory practices functioned together to enhance the bank's resilience. The goal was not only to map existing practices but also to assess their alignment with evolving cyber threats and regulatory obligations. The interview protocol was structured around four key topics: (1) knowledge of cyber resilience, (2) strategies adopted in the project, (3) the role of human intervention and regulation, and (4) perceived effectiveness of implemented mechanisms.

Table 2. Job Descriptions of Interview Participants

ID	Job Position	Description
Resp-1	Customer Support/App	Leading the cyber resilience and the Data Vault cloud to meet the business need.
Resp-2	Relay point IT project manager	Project manager for cyber resilience; responsible for rebuild tests and implementation of technical security solutions on public cloud.
Resp-3	PCA & Crisis Management Responsible	Developing strategies to ensure continuity of critical operations during and after a crisis.
Resp-4	Customer Support Manager/AP	Monitoring production-related incidents within the designated IT perimeter for the past 5 years.
Resp-5	ITRM Research Officer	First-year Master's apprentice handling two cyber resilience construction projects.
Resp-6	IT Business Continuity Expert	Joined cyber resilience team to ensure recovery of IT systems during disruptions.
Resp-7	Data protection analyst	Over 15 years in the organization; currently working on data leakage prevention frameworks.
Resp-8	Customer support	Supporting cyber resilience project team (e.g., SWIFT) by testing total IS recovery plans.
Resp-9	IT service continuity management responsible	Risk and continuity management by overseeing reconstruction test processes.
Resp-10	IS program director	Managing IS projects with a focus on rapid and effective cyber attack response.
Resp-11	Cyber control REG ITRM	Working in REG cyber control team; responsible for cyber indicators and verifying security compliance.

3.2. Data Analysis

Following data collection, the transcripts were analysed using thematic analysis, a recognised method for extracting patterns and meaning from qualitative data in applied fields such as cybersecurity and organisational studies (Braun & Clarke, 2006; Nowell et al., 2017). Thematic coding was performed manually, involving multiple reviews of the translated transcripts. This iterative process helped identify repeated ideas and sub-themes that aligned with the central variables of the study. Themes were derived inductively but guided by the theoretical structure that informed the interview design. Codes were grouped based on how participants described technological tools (e.g., automation, data vaults, anomaly detection), human actions (e.g., risk management, training, decision-making), and the influence of internal and external regulation (e.g., compliance protocols, control indicators). Each transcript was compared across roles to account for variation in perspectives between management and operational teams. This form of comparative thematic analysis aligns with established best practices in qualitative cybersecurity research (Di Gravio et al., 2021; Dupont, 2019). To enhance reliability, analytical notes were documented throughout the coding process, and themes were reviewed across the dataset for coherence. The approach ensured that insights reflected the lived experiences and expert knowledge of professionals working within a live cyber resilience context. Steps such as repeated readings, code-revision cycles, and participant anonymity helped strengthen the credibility of the analysis (Guba & Lincoln, 1994).

4. Results

This section presents the analysis of interviews conducted with professionals involved in the cyber resilience project of a major French bank. The results are organised into thematic categories based on qualitative data collected from eleven participants. Each theme corresponds to a critical component of the bank's cyber resilience framework, supported by direct quotations and summarized into comprehensive tables.

4.1. Operational Cyber Resilience

Cyber resilience within the banking context extends beyond standard cybersecurity protocols to include business continuity, risk management, and the ability to resume operations during adverse conditions. Participants consistently highlighted that the concept has evolved into "operational cyber resilience," encompassing broader threats, including geopolitical instability and infrastructural disruptions. Participants emphasized the importance of maintaining continuity in operations during and after a cyber incident, with cyber resilience serving as a continuation of cybersecurity processes, not a replacement. The shift from passive protection to an integrated approach was a key strategic decision across departments.

Table 3. Selected Responses on Operational Cyber Resilience

Respondent	Responses
Resp-1	From now on, we no longer talk about cyber resilience but operational resilience, that is, we do not only talk about the cyber factor, but we also include geopolitical issues, hence the obligation to report a shock that has significantly impacted the organization.
Resp-3	Cyber resilience begins as soon as cybersecurity is completed, which is used to protect the information system, cyber resilience is the continuation/resumption of the cybersecurity process.

4.2. Cybersecurity Technologies and Strategic Response

The organization implemented a multi-layered strategic framework integrating technical tools, operational solutions, and human processes. Specific technologies such as encrypted data vaults, alternative payment interfaces, and cloud-based restoration systems were central to the plan. Each solution was designed with redundancy and isolation from the main infrastructure to reduce vulnerability during attacks.

Table 4. Selected Responses on Technologies and Strategies

Respondent	Responses
Resp-1	We have 3 levels of strategies... creating public cloud recovery tools that is separated from our IS that is encrypted and secure on which the procedures are stored (Datavault).
Resp-2	Data vault: secure and redundant vault for confidential documents and critical operational data... payments in any possible scenario.
Resp-3	To respond to and remediate cyberattacks, it is necessary to provide emergency devices to staff, to set up an alternative disconnected system that is not impacted by the attack.

The strategic planning phase involves identifying vital operational components including value chains, network architecture, and critical applications. Interviewees noted that business impact analysis (BIA) was used to classify and prioritise activities for response and recovery.

Table 5. Responses on Crisis Strategy Implementation

Respondent	Responses
Resp-2	The group strategies are based on two main phases: analysis... then production when a cyber resilience solution must be activated.
Resp-3	Adopting Business Impact Analysis... determine what we can keep, what is a priority and what can wait.
Resp-9	Identify the most important functions that absolutely must be rebuilt... have a survival plan.

4.3. Human Intervention and Training

Participants consistently affirmed the irreplaceable role of human involvement in cyber resilience processes. Employees were trained to respond to emergencies through simulations, manual backups, and compliance routines. Human intervention filled critical gaps where automation alone could not ensure resilience.

Table 6. Responses on Human Role in Cyber Resilience

Respondent	Responses
Resp-1	Human intervention is essential... crisis simulation exercises are regularly practiced.
Resp-3	Crisis management methodology, training the emine wheel... testing these solutions, repeat.
Resp-10	Manual processes must be very well established... trained to execute them.
Resp-11	Training employees, using strong passwords, reporting suspicious activity... essential role.

A broad range of simulation exercises and policy-driven human controls such as role-specific VPN access and phishing detection instead of it were practiced across teams.

4.4. Assessment of Strategic Effectiveness

Participants noted that while implementation is in progress, ongoing evaluation mechanisms are critical. Institutions used internal barometers, including the NIST Cybersecurity Framework, to assess the design, efficiency, and coverage of cyber control processes. Testing procedures include backup verification, simulation exercises, and control audits.

Table 7. Responses on Effectiveness of Strategies

Respondent	Responses
Resp-2	It is not possible to assess effectiveness yet... some corrections as the process progresses.
Resp-3	It is estimated that by 2024 it is possible to evaluate it.
Resp-10	Preparing for the worst... regularly test the solutions.
Resp-11	The barometer's controls have three axes: design-efficiency-perimeter.

These evaluations are aligned with continuous improvement principles and aim to reduce vulnerabilities by regular reassessments and simulations.

4.5. Challenges in Implementation

The implementation of a cyber resilience process presented various structural and procedural challenges. Participants cited the unpredictability of attacks and difficulties in defining critical priorities as major obstacles. Furthermore, the human factor introduces potential vulnerabilities, including inadvertent security gaps.

Table 8. Responses on Implementation Challenges

Respondent	Responses
Resp-1	Great difficulty in terms of hierarchy to define what is vital... different functions impact needs.
Resp-2	Adding loopholes to the system and constantly finding solutions.
Resp-7	We don't precisely control the contour of the risk... so there's a part of 'guessing'.
Resp-3	The process is long and complicated and requires direction and auditing.

Participants also highlighted the need for more sophisticated risk modelling to anticipate unknown threat vectors.

4.6. Regulatory Role and Influence

Regulation was described as a central pillar in the cyber resilience framework. Respondents frequently referred to the ECB, DORA regulation, and national cybersecurity policies as catalysts for strategic reform. The ECB provides guidance and enforceable requirements while DORA supports unified compliance across Europe, particularly in risk identification and response standardisation.

Table 9. Responses on Regulatory Role

Respondent	Responses
Resp-1	DORA regulations made it possible to evaluate the project... separate vital applications.
Resp-2	We receive instructions from the ECB to strengthen and secure our information system.
Resp-6	We have ECB, FCA regulators... they give recommendations to banks.
Resp-8	French government reminding of responsibility... banks discuss vulnerabilities and solutions.
Resp-7	The regulator has an essential role to play in catalyzing the remediation of systems.

The NIST framework is also actively used as a benchmark tool, supported by ECB recommendations and adapted internally for implementation. The findings above support the integrated model developed earlier in the research, showing how technologies, human competencies, and regulatory structures converge in cyber resilience planning and execution. Figure 3 provides a thematic Summary of Cyber Resilience

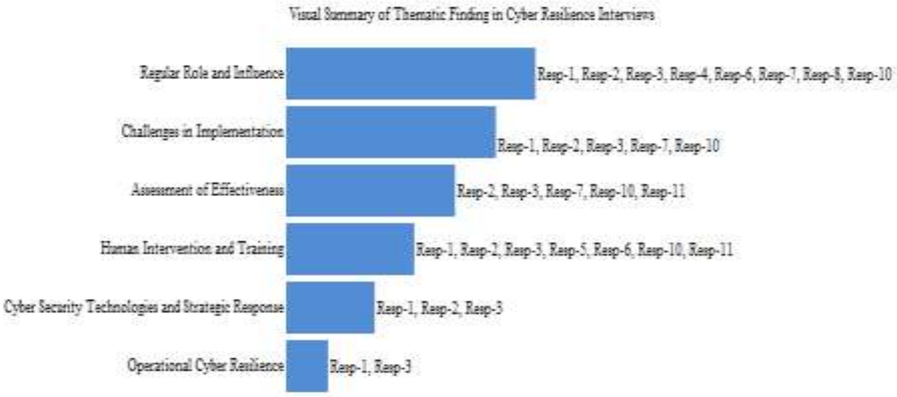

Figure 7. Thematic Summary of Cyber Resilience

Table 10. Key Findings of Cyber Resilience

Theme	Key Findings
Operational Cyber Resilience	Cyber resilience is now part of a broader concept of operational resilience, including business continuity and geopolitical risk response.
Cybersecurity Technologies and Strategic Response	Multiple layers of strategy (technical, operational, human) are implemented including cloud-based data vaults and emergency systems.
Human Intervention and Training	Human action is critical in responding to incidents, running simulations, securing operations manually, and applying best practices.
Assessment of Effectiveness	Effectiveness is tracked using control protocols like the NIST framework, annual rebuild tests, and department-level evaluation grids.
Challenges in Implementation	Difficulties include prioritisation of activities, unpredictable nature of threats, and human error introducing vulnerabilities.
Regulatory Role and Influence	Regulatory frameworks such as DORA and ECB guidelines guide formal expectations and compliance obligations across entities.

5. Discussion

The findings reveal a significant organisational shift toward operational resilience, which expands beyond traditional cybersecurity controls. Participants highlighted that resilience is no longer solely linked to technical defence mechanisms but encompasses the capacity to maintain essential services during and after disruptions. This view reflects established definitions of resilience in critical infrastructure research, where the objective is not only risk prevention but also system adaptability and recovery under pressure (Linkov et al., 2023; Seager et al., 2017). Within the examined bank, cyber resilience planning integrates recovery tools, crisis simulations, and alternative operating environments, indicating an evolving risk culture that accepts the inevitability of cyber incidents. Interviewed employees repeatedly pointed out that resilience planning began where static defence ends, with increased attention placed on scenarios involving system-wide outages and data integrity risks. This adaptive approach reflects recent institutional transformations where information systems must remain serviceable even when under attack, a principle which has grown more prominent in post-incident evaluations across the financial sector (Linkov et al., 2023; Seager et al., 2017). The results also confirmed the centrality of human intervention in implementing and sustaining cyber resilience practices. Respondents described extensive internal training, role-based simulations, manual process reactivation procedures, and access control protocols that ensure readiness in case of operational breakdown. Such findings are consistent with broader empirical studies that place human factors at the core of cyber defence effectiveness, particularly in layered security environments where staff are required to identify threats and respond promptly when automated systems are compromised (Parsons et al., 2023; Zimmermann & Renaud, 2019). The data emphasised that while technology enables faster detection and containment, the actual resolution and continuity tasks are often executed by trained staff. Moreover, multiple respondents acknowledged that the human factor could either enhance or compromise security efforts, depending on behaviour, training, and awareness levels. These insights align with prior literature warning against the overreliance on technical solutions without strengthening user-side vigilance and incident preparedness (Blyth & Kovacich, 2006; Kraemer & Carayon, 2007). The findings suggest that organisations still face challenges in embedding this human-technical synergy into daily operations without introducing new vulnerabilities.

In the regulatory dimension, most participants noted that frameworks such as the European Central Bank directives and the Digital Operational Resilience Act had played a structural role in shaping their organisation’s policies and control standards. These external guidelines provided the institutional legitimacy and urgency required to allocate resources, establish evaluation baselines, and prioritise mission-critical services. Interviewees mentioned the role of national bodies and industry-wide consultation platforms as key channels for translating regulatory objectives into practical implementation. The bank adopted regulatory instruments not only as compliance checklists but as a basis for ongoing performance assessment using tools like the NIST control grid. This reflects earlier research which argues that regulatory clarity combined with technical assessment tools supports better internal alignment between cybersecurity, IT continuity, and operational recovery teams (Kosmowski et al., 2022; Seager et al., 2017). The discussion across multiple departments also illustrated that the impact of regulation extended beyond formal documentation into shared risk understanding and incident accountability frameworks. While regulatory expectations are well communicated, the integration process remains complex, particularly where internal priorities and external controls do not always align, a tension well recognised in both industry assessments and academic commentary on cyber risk governance in financial systems (Wilson & Hash, 2003).

6. Implications

6.1. Theoretical Implications

This research provides empirical support for integrating cybersecurity technologies, human expertise, and regulatory frameworks as core components of cyber resilience in the banking sector. While previous studies have examined these elements independently, this thesis contributes to the literature by analysing their interdependence and operational relevance within a major European financial institution. The findings align with systems thinking approaches in cyber risk management, which emphasize the need to address socio-technical interactions to enhance digital resilience (Bada et al., 2019; Linkov et al., 2023). The inclusion of human factors in particular supports the broader theoretical argument that technological security alone is insufficient in managing cyber risk. The study expands resilience theory in digital environments by situating the banking context as one where operational continuity, rapid incident response, and institutional learning must operate in conjunction. This layered view of resilience, which includes proactive and reactive measures, contributes to existing frameworks for organizational cybersecurity maturity (Rocha et al., 2025).

6.2. Practical Implications

The findings present key practical insights for banks, policymakers, and technology leaders responsible for cybersecurity governance. The integrated approach observed within the participating institution highlights how operational strategies must be aligned with institutional structures to sustain resilience. For banking professionals, the results confirm the importance of continuous scenario-based training, data classification processes, and clearly assigned crisis response protocols. Investments in secure backup infrastructure and encrypted recovery solutions such as data vaults can offer critical redundancy in the event of a system failure. On a procedural level, the use of annual evaluation tools such as the NIST framework helps institutions maintain oversight of preparedness and adjust based on testing outcomes (NIST, 2020). For regulators, the study shows the value of maintaining adaptable legal standards such as the Digital Operational Resilience Act (DORA), which encourage not only compliance but ongoing internal assessment and communication across financial entities. Regulatory interventions should include proactive audits, cyber threat intelligence sharing, and regular enforcement assessments to ensure that minimum security standards are accompanied by actual organisational readiness.

7. Limitations and Future Research

The analysis is based on qualitative data gathered from one financial institution, which may limit the transferability of findings to other banking environments or financial service sectors. Although the interviews provided rich insights into internal procedures and challenges, the scope remains narrow and dependent on the perspectives of a limited sample of respondents. Additionally, the project's timeline restricted the capacity to observe long-term outcomes or evaluate the effectiveness of the strategies discussed. Confidentiality concerns also limited access to internal documentation, which may have affected the depth of validation. The dynamic and evolving nature of cyber threats further implies that solutions deemed effective at the time of writing may require reevaluation. While this thesis outlines a practical framework based on current organisational conditions, changes in threat vectors or regulatory policy may necessitate future adaptation. Future studies should adopt a comparative framework that includes multiple banks or financial institutions to assess how cyber resilience strategies vary across different regulatory environments and organisational structures. Mixed-method designs incorporating both qualitative insights and quantitative metrics would allow researchers to measure the statistical relationship between resilience strategies and incident outcomes such as data recovery time, financial loss reduction, or customer trust. There is also a need to explore the behavioural dimension of cyber resilience, particularly how employee attitudes, training compliance, and risk perception influence policy effectiveness (Puhakainen & Siponen, 2010). Investigating cross-functional collaboration between IT departments, crisis managers, and compliance officers would provide a deeper understanding of how coordination influences rapid incident response. Another emerging area for research includes assessing the scalability of resilience strategies among smaller financial institutions, which may face different resource constraints than major banking groups. Future work can also evaluate how artificial intelligence and automation affect resilience design and decision-making, especially in operational recovery and anomaly detection. Such extensions will contribute to a broader understanding of cyber resilience as both a technical and institutional practice.

References

Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews, 25*(03), 1542-1556. https://doi.org/10.30574/wjarr.2025.25.3.0909

Almagribi, A. B., & Putranto, B. P. D. (2025). Current Trends and Future Directions of Big Data in Commerce: A Bibliometric Analysis Based on Scopus. *Jurnal Sistem Informasi dan Ilmu Komputer, 8*(2), 57-74. https://doi.org/10.34012/jurnalsisteminformasidanilmukomputer.v8i2.6098

Avrahami, Z., & Zwilling, M. (2025). The impact of cyber threat intelligence (CTI) on employee behavior and skills and the implications for organizational cyber resilience. *International Journal of Information Security, 24*(4), 184. https://doi.org/10.1007/s10207-025-01096-y

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*. https://doi.org/10.48550/arXiv.1901.02672

Blyth, A., & Kovacich, G. L. (2006). IA and Software. In *Information Assurance: Security in the Information Environment* (pp. 191-212). Springer London. https://doi.org/10.1007/1-84628-489-9_14

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Colabianchi, S. (2023). *Humans in cyber resilience: managerial and operational opportunities* Sapienza University of Rome, Italy].

Denzin, N. K. (2018). *The qualitative manifesto: A call to arms*. Routledge.

Dhashanamoorthi, B. (2021). Artificial Intelligence in combating cyber threats in Banking and Financial services. *International Journal of Science and Research Archive, 4*(1), 210-216. https://doi.org/10.30574/ijsra.2021.4.1.0209

Di Gravio, G., Cantelmi, R., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions, 41*(3), 341-376. https://doi.org/10.1007/s10669-020-09795-8

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity, 5*(1), 1-17. https://doi.org/10.1093/cybsec/tyz013

Eshmawi, A. A., Aldrees, A., & Alharthi, R. (2025). Smart framework for industrial IoT and cloud computing network intrusion detection using a ConvLSTM-based deep learning model. *Frontiers in Computer Science, 7*. https://doi.org/10.3389/fcomp.2025.1622382

Fenjan, A. Z. (2025). Cyber Resilience and its Impact on Improving the Quality of Digital Financial Services: An Applied Study at the Jordanian National Cyber Security Center. *International Journal of Management and Organizational Research 4*(1), 143-150. https://doi.org/10.54660/IJMOR.2025.4.1.143-150

Galinec, D., & Steingartner, W. (2017). Combining cybersecurity and cyber defense to achieve cyber resilience. 2017 IEEE 14th International Scientific Conference on Informatics,

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of qualitative research, 2*, 105-117.

Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis. *IEEE Access, 11*, 80181-80198. https://doi.org/10.1109/ACCESS.2023.3298824

Kondratyeva, M. N., Svirina, D. D., & Tsvetkov, A. I. (2021). The role of information technologies in ensuring banking security. *IOP Conference Series: Materials Science and Engineering, 1047*(1), 012069. https://doi.org/10.1088/1757-899X/1047/1/012069

Kosmowski, K. T., Piesik, E., Piesik, J., & Śliwiński, M. (2022). Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. *Energies, 15*(10), 3610. https://doi.org/10.3390/en15103610

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics, 38*(2), 143-154. https://doi.org/10.1016/j.apergo.2006.03.010

Linkov, I., Ligo, A., Stoddard, K., Perez, B., Strelzoffx, A., Bellini, E., & Kott, A. (2023). Cyber Efficiency and Cyber Resilience. *Commun. ACM, 66*(4), 33–37. https://doi.org/10.1145/3549073

Muhammad, D., & Siraj, M. M. (2025). AI and Cybersecurity: Defending Data and Privacy in the Digital Age. *Journal of Engineering and Computational Intelligence Review, 3*(1), 25-35.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods, 16*(1), 1-13. https://doi.org/10.1177/1609406917733847

Okusi, O., Obiakor, I. J., & Adeloye, F. C. (2025). Designing resilient data risk management protocols for regulatory compliance and cyber incident response. *International Journal of Advance Research Publication and Reviews, 2*(7), 45-70. https://doi.org/10.55248/gengpi.6.0725.2419

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544. https://doi.org/10.1007/s10488-013-0528-y

Parsons, E. K., Panaousis, E., Loukas, G., & Sakellari, G. (2023). A Survey on Cyber Risk Management for the Internet of Things. *Applied Sciences, 13*(15), 9032. https://doi.org/10.3390/app13159032

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 757-778. https://doi.org/10.2307/25750704

Rocha, A., Alaba, F. A., Musa, H., Sousa, M. J., de Vasconcelos, J. B., & Pereira, R. (2025). Cybersecurity Maturity Models: A Systematic Literature Review. Countering Hybrid Threats Against Critical Infrastructures, Dordrecht.

Saha, S., Siddiki, M. S., Mondal, R. S., Bhuiyan, M. N. A., & Kamruzzaman, M. (2025). Risk assessment of cyber security in the banking sector. *Journal of Business and Management Studies, 7*(4), 208-218. https://doi.org/10.32996/jbms.2025.7.4.12

Seager, T. P., Clark, S. S., Eisenberg, D. A., Thomas, J. E., Hinrichs, M. M., Kofron, R., Jensen, C. N., McBurnett, L. R., Snell, M., & Alderson, D. L. (2017). Redesigning Resilient Infrastructure Research. Resilience and Risk, Dordrecht.

Sharkov, G. (2016). *From Cybersecurity to Collaborative Resiliency* Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Vienna, Austria.

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security, 23*(3), 1695-1719. https://doi.org/10.1007/s10207-023-00811-x

Vimal Mani, C. (2021). Demystifying the Implementation of Cyberresilience Programs. *ISACA Journal, 3*(1), 1-10.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication, 800*(50), 1-39.

Yin, R. K. (2018). *A book review: Case study research and applications* (6th ed ed.). Sage, Publication Inc.

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005