JAGDISH SHETH SCHOOL OF MANAGEMENT

AACSB Accredited, Formerly IFIM Business School

AACSB ACCREDITED

RESEARCH INCUBATION

EXTENDED ABSTRACT

INDUSTRY: BANKING

SUBMITTED BY: Cluster - 43

BANDUCHODE BHAVAN
2022JULB02072

DEVESH SENGER
2022JULB02053

LOKESWAR REDDY NALLASIDDU
2022JULB01086

PRAJWAL ARUN NAGPURE
2022JULB01064

SHEETAL SINGH PARMAR
2022JULB01142

Contents

Abstract

This research investigates the dynamic interplay between consumer involvement and the adoption of digital banking in the Indian banking sector, with a specific focus on cybersecurity in the process of digitalization. In the midst of India's rapidly evolving banking landscape, the study explores the unique aspects of consumer behavior and digital banking practices. Utilizing a mixed-methods approach that combines quantitative and qualitative data, the research aims to offer a comprehensive understanding of this intricate relationship.

The findings underscore the importance of in-branch communication, the evolution of roles among branch staff, customer-centric initiatives, and the modernization of bank branches. These factors emerge as crucial elements influencing the adoption of digital banking. Importantly, the study provides practical insights aimed at assisting banks in adapting to shifting consumer preferences while navigating the challenges of digitalization, with a specific emphasis on ensuring cybersecurity and safety in the digital banking space.

Introduction and objectives

With over 100 banks and 96,000 branches, the Indian banking sector is one of the biggest in the entire globe. Although private sector banks (PVBs) are gaining market share, public sector banks (PSBs) still dominate the sector. The banking sector in India is changing due to technology. Banks are making investments in online and mobile banking, as well as other digital platforms. As a result, more and more clients are choosing to conduct their banking transactions online. Technology is another tool used by fintech businesses to offer cutting-edge financial services and products. Traditional banks are under pressure from this to innovate and enhance their consumer offers. To keep up with the evolving financial environment and to safeguard customers, the Reserve Bank of India (RBI) is proposing new laws.

Context of the Banking Industry

The context of the banking industry refers to the current conditions, challenges, and trends that shape the industry's landscape. Here's an overview of the context of the banking industry:

- **Technological Advancements**: The banking industry has witnessed significant technological advancements in recent years. The proliferation of digital banking, mobile apps, online payment systems, and blockchain technology has transformed the way banks operate and interact with customers.

- **Changing Customer Expectations:** Customers now expect more convenient, personalized, and efficient banking services. They prefer the flexibility of conducting transactions and managing their finances online, which has increased the demand for digital banking solutions.

- **Regulatory Changes:** Regulatory bodies worldwide have introduced new regulations and compliance requirements to ensure financial stability and protect consumers. These regulations have had a profound impact on banking operations, including risk management and data security.

- **Fintech Disruption:** The rise of financial technology (fintech) companies has disrupted traditional banking models. Fintech firms offer innovative and agile solutions, challenging established banks in areas like payments, lending, and wealth management.

- **Cybersecurity Concerns:** With the increased use of digital technologies, banks are more susceptible to cyber threats. Ensuring robust cybersecurity measures is critical to protect customer data and maintain trust.

- **Global Economic Conditions:** Economic factors, such as interest rates, inflation, and geopolitical events, have a direct impact on the banking industry. Banks must adapt to changing economic conditions to manage risks effectively.

- **Sustainability and ESG (Environmental, Social, and Governance):** There's a growing emphasis on sustainability and ESG considerations in banking. Banks are under pressure to incorporate ethical, social, and environmental factors into their business strategies and investment decisions.

Research Objectives

Below mentioned are some of the focus points for this report focusing on digitalization of banking mainly on cybersecurity in Banking:

- Impact of Digital Payment Platforms on Financial Frauds.
- Incidence of Cyberattacks on India's Banking Industry.
- Evolution of Cybersecurity in the Banking Industry.
- Understanding Patterns and Life Cycle of Cyber Threats.
- Evaluation of Banks' Cyber Defense Systems.
- Recommendations for Strengthening Cybersecurity in Banking

Distinctiveness of the Study

Indian Banking Sector Focus:

The study's distinctiveness lies in its specific focus on the Indian banking sector, providing insights into the unique challenges and dynamics of cybersecurity within this rapidly evolving landscape.

Mixed-Methods Approach:

The use of a mixed-methods approach, combining both quantitative and qualitative data, adds depth to the research. This comprehensive methodology allows for a nuanced understanding of the relationship between consumer involvement and digital banking adoption in the context of cybersecurity.

Real-time Incidents and Global Context:

The incorporation of real-time incidents, such as the reported 40,000 cyberattacks on India's banking industry, enhances the study's relevance. It places the research within the broader global context of cyber threats, showcasing the immediacy and significance of the cybersecurity challenges faced by Indian banks.

Historical Perspective:

The inclusion of a historical perspective, tracing cybersecurity incidents in the banking sector back to 1970, adds depth and context. This historical lens provides a foundation for understanding the evolution of cyber threats and the corresponding advancements in cybersecurity measures.

Practical Insights for Banks:

The study's distinctiveness lies in its practical orientation, offering insights that banks can directly apply. By emphasizing factors like in-branch communication, role transformation of branch staff, and customer-centric initiatives, the research goes beyond theoretical analysis to provide actionable recommendations for banks navigating digitalization and cybersecurity challenges.

Adaptation to Changing Consumer Preferences:

The study stands out by addressing the need for banks to adapt to changing consumer preferences, especially in the context of digitalization. It recognizes the importance of understanding and responding to consumer behavior as a key element in ensuring the successful adoption of digital banking practices while maintaining a strong focus on cybersecurity.

Keywords

The keywords for the study report focusing on the evolving dynamics of consumer involvement and the adoption of digital banking in the Indian banking sector keeping in view for cybersecurity in banking might include:

- Digital Banking Adoption
- Cybersecurity Challenges
- Indian Banking Sector
- RBI Financial Stability Report
- Consumer Involvement
- Mixed-Methods Research
- Cyber Threats
- Financial Frauds
- Digital Payment Platforms
- Global Hackers
- Cyberattacks on Banks
- Historical Cybersecurity Incidents
- Evolution of Cybersecurity
- In-branch Communication
- Role Transformation
- Customer-centric Initiatives
- Modernization of Bank Branches
- Changing Consumer Preferences
- Practical Insights for Banks
- Adaptation to Digitalization

Literature Review

Previous Research Trends

Certainly! The digitization of the banking sector has been a dynamic field with several notable trends. Let's see some of these trends:

- **Artificial Intelligence (AI):** AI is revolutionizing banking by enabling personalized customer experiences, chatbots for customer service, and predictive analytics for risk management.
- **Contactless Payments**: With the rise of mobile wallets and NFC technology, contactless payments have become more prevalent. These methods enhance convenience and security for customers.
- **Neo banks:** Neo banks, also known as digital-only banks, are disrupting the traditional banking landscape. They offer streamlined services, lower fees, and innovative features, appealing to tech-savvy customers.
- **Blockchain Technology:** Blockchain has the potential to transform various banking processes, including secure transactions, identity verification, and supply chain finance.
- **Biometric Technology:** Biometrics like fingerprint and facial recognition are enhancing security in digital banking. They provide a seamless and secure authentication experience.
- **Cryptocurrencies:** While still evolving, cryptocurrencies like Bitcoin have sparked interest in the financial industry. Banks are exploring their applications and regulatory implications.
- **Robotic Process Automation (RPA):** RPA automates repetitive tasks, improving efficiency and reducing errors in banking operations.
- **Customer Experience Focus:** Banks are increasingly prioritizing customer experience. User-friendly interfaces, personalized services, and seamless digital journeys are critical for retaining and attracting customers.
- **Financial Inclusion:** Digital banking can bridge gaps by reaching unbanked populations through mobile banking and digital wallets. It accelerates financial inclusion.
- **Impact of FinTech**: The collaboration between traditional banks and FinTech startups is driving innovation. FinTech solutions are reshaping payment systems, lending, and investment services

Specific Focus of the Study

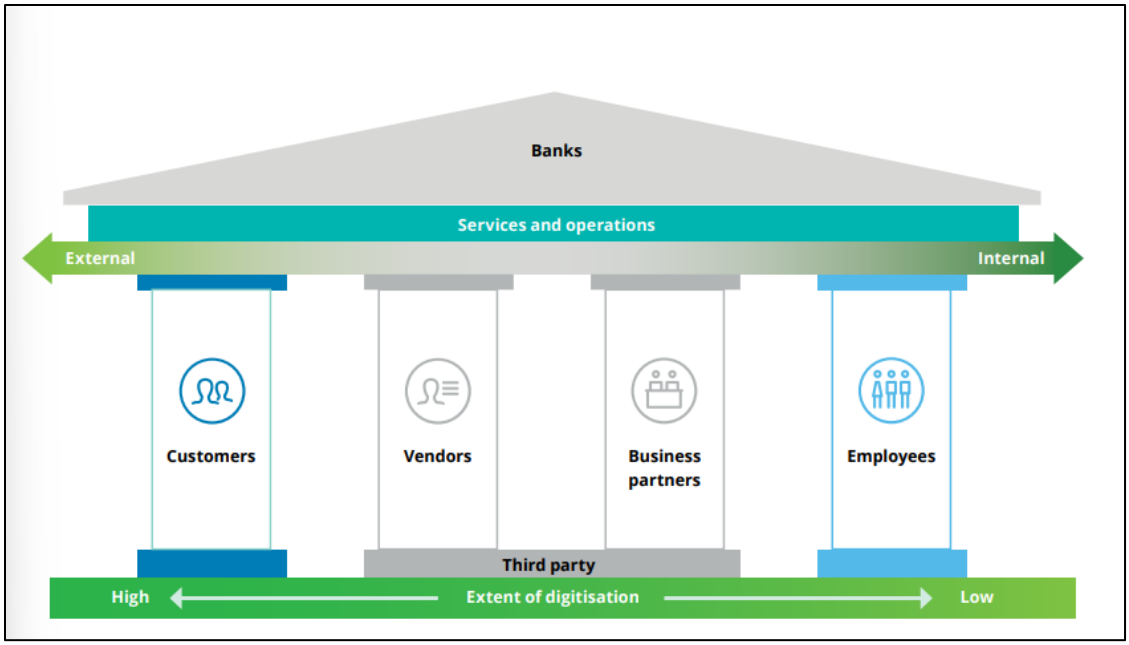


Figure 1 Digitalization Process

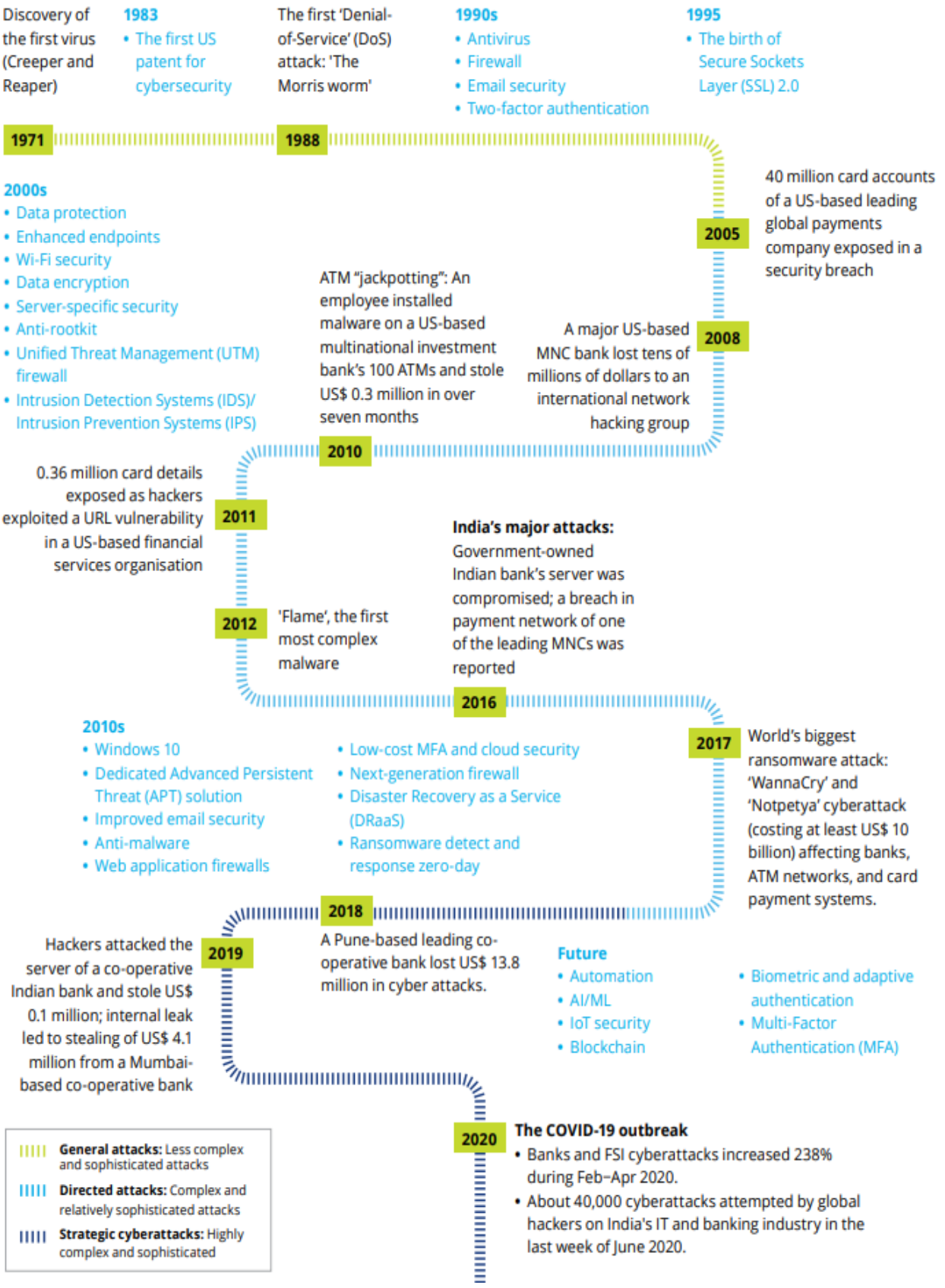
Banks' foremost agenda in board rooms has been the digitization of voluminous confidential data and banking processes (not limited to payments). This urgency has put the spotlight on digital technologies, such as cloud, Artificial Intelligence (AI), analytics, Internet of Things (IoT), and Machine Learning (ML).

With technology transformation, confidential information will be saved in remote servers and ubiquitous. Higher digitization and remote operations will lead to increased vulnerabilities and open up opportunities for cybercriminals, exposing banks to breaches or hacking. Banks need to be mindful of the following challenges while dealing with cyber threats.

Overview on Cybersecurity in Banking Sector

The evolution of cyber threats; cyberattacks in the financial industry; and cybersecurity.

In July 2020, the RBI flagged cybersecurity concerns, highlighting a surge in cyber threats targeting India's banking industry. The national security advisor noted a substantial rise in financial frauds linked to increased reliance on digital payment platforms post-COVID-19. Global hackers attempted over 40,000 cyberattacks on India's banks in a five-day period in late June. Cybersecurity challenges are not new; since 1970, banks globally have faced escalating threats, intensifying with rapid digitization. This evolution emphasizes the constant need for enhanced cybersecurity measures, driven by the imperative to understand and counter individual cyberattacks and their intricate patterns, sophistication, and life cycle.


Discovery of the first virus (Creeper and Reaper)
1971
1983
• The first US patent for cybersecurity
The first 'Denial-of-Service' (DoS) attack: 'The Morris worm'
1988
1990s
• Antivirus
• Firewall
• Email security
• Two-factor authentication
1995
• The birth of Secure Sockets Layer (SSL) 2.0
2000s
• Data protection
• Enhanced endpoints
• Wi-Fi security
• Data encryption
• Server-specific security
• Anti-rootkit
• Unified Threat Management (UTM) firewall
• Intrusion Detection Systems (IDS)/ Intrusion Prevention Systems (IPS)
2005
40 million card accounts of a US-based leading global payments company exposed in a security breach
ATM "jackpotting": An employee installed malware on a US-based multinational investment bank's 100 ATMs and stole US$ 0.3 million in over seven months
2008
A major US-based MNC bank lost tens of millions of dollars to an international network hacking group
2010
0.36 million card details exposed as hackers exploited a URL vulnerability in a US-based financial services organisation
2011
2012
'Flame', the first most complex malware
India's major attacks:
Government-owned Indian bank's server was compromised; a breach in payment network of one of the leading MNCs was reported
2016
2010s
• Windows 10
• Dedicated Advanced Persistent Threat (APT) solution
• Improved email security
• Anti-malware
• Web application firewalls
• Low-cost MFA and cloud security
• Next-generation firewall
• Disaster Recovery as a Service (DRaaS)
• Ransomware detect and response zero-day
2017
World's biggest ransomware attack: 'WannaCry' and 'Notpetya' cyberattack (costing at least US$ 10 billion) affecting banks, ATM networks, and card payment systems.
2018
A Pune-based leading co-operative bank lost US$ 13.8 million in cyber attacks.
2019
Hackers attacked the server of a co-operative Indian bank and stole US$ 0.1 million; internal leak led to stealing of US$ 4.1 million from a Mumbai-based co-operative bank
Future
• Automation
• AI/ML
• IoT security
• Blockchain
• Biometric and adaptive authentication
• Multi-Factor Authentication (MFA)
2020
The COVID-19 outbreak
• Banks and FSI cyberattacks increased 238% during Feb–Apr 2020.
• About 40,000 cyberattacks attempted by global hackers on India's IT and banking industry in the last week of June 2020.
General attacks: Less complex and sophisticated attacks
Directed attacks: Complex and relatively sophisticated attacks
Strategic cyberattacks: Highly complex and sophisticated

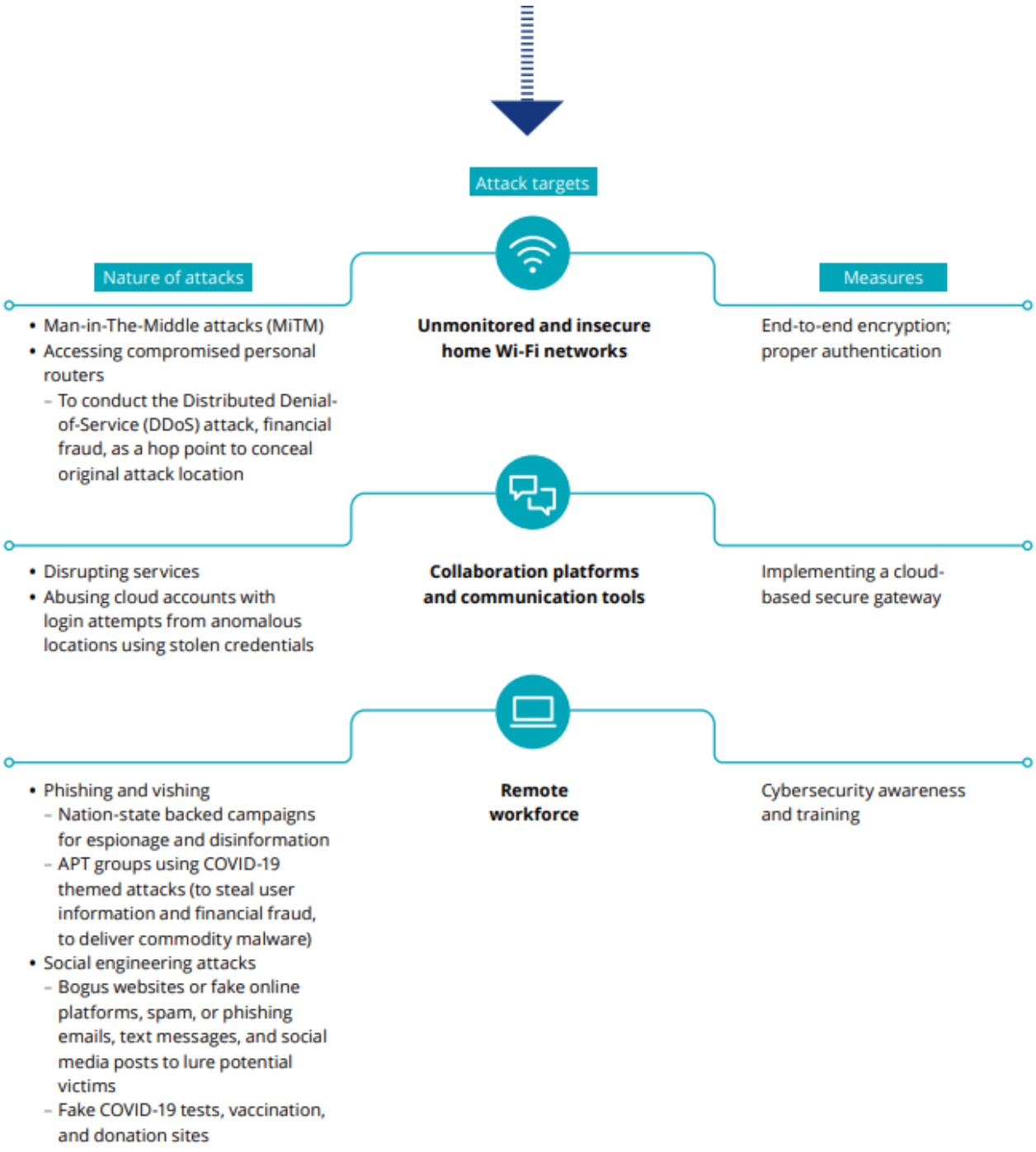


Figure 2 Cybersecurity Evaluation

Cyber related challenges of Digitization in Banking Sector

In banking boardrooms, the key agenda is digitizing vast amounts of confidential data and banking processes. This shift highlights the role of technologies like cloud, AI, analytics, IoT, and ML. While this

transformation securely stores information on remote servers, it also raises vulnerabilities, exposing banks to increased cyber threats and potential breaches.

- **Cybercrime Sophistication:**
    - Traditional threats like armed robbery now pale in comparison to sophisticated cybercrimes.
    - Cyber risks have evolved beyond data leakage and access control issues, encompassing activities such as stealing card data, reprogramming ATMs, and employing sophisticated software for money laundering.

- **Data Management Challenges:**
    - Banks, handling large amounts of Personally Identifiable Information (PII), face increased cybersecurity risks.
    - Adoption of cloud and IoT for data transfers requires efficient data management to address privacy concerns and comply with regulations.
    - Key issues include data sharing mechanisms, data life cycle management, and defining data ownership rules.

- **Legacy System Limitations:**
    - Banks' IT architecture, a mix of legacy systems and newer applications, poses challenges in adapting to the speed and mobility requirements of modern banking.
    - Integration of core applications with newer technologies exposes legacy systems to novel and evolving security threats.

- **Securing Third-Party Services:**
    - Banks are reliant on third-party vendors and alliance partners, introducing potential vulnerabilities.
    - The cybersecurity of third-party services becomes the responsibility of banks, necessitating robust security measures.

- **Compromised Network and Devices Exposure:**
    - Increased virtual connectivity to banks' networks through personal devices post-COVID-19 raises cybersecurity risks.
    - Managing threats arising from multiple access points, used by both employees and customers, is a challenging task for banks.

- **Shortage of Cybersecurity Professionals:**
    - Despite the growing demand and complexity of cyber risks, there is a global shortage of skilled cybersecurity professionals.
    - India, in particular, faces a challenge of insufficient skilled professionals in the cybersecurity sector.

- The increasing complexity of cyber risks is likely to lead to a shortage of skilled professionals in banks.

Methodology

Dimensions of cybersecurity banks have to be aware of

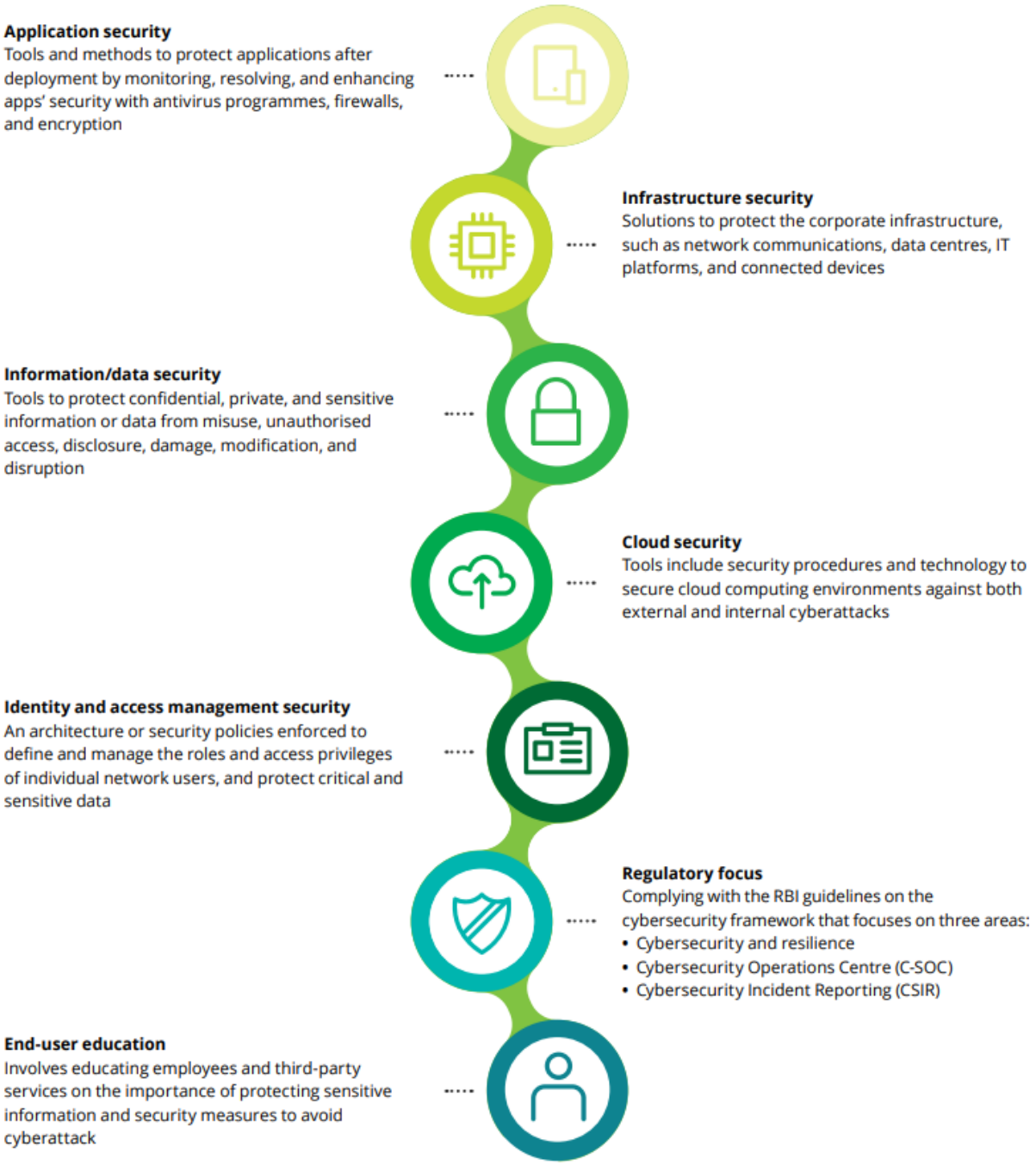


Figure 3 Dimensions of Cybersecurity threats

Results

The results of the research report on the dynamic interplay between consumer involvement, digital banking adoption, and cybersecurity in the Indian banking sector are summarized below:

- **Consumer Behavior and Digital Banking Adoption:**
    - In-branch communication, role evolution among branch staff, customer-centric initiatives, and modernization of bank branches are identified as crucial factors influencing the adoption of digital banking.
    - The study highlights the need for banks to adapt to shifting consumer preferences in the rapidly evolving banking landscape.

- **Cybersecurity Challenges in Digitalization:**
    - The report recognizes the urgency for banks to digitize confidential data and processes, emphasizing the integration of technologies like cloud, AI, analytics, IoT, and ML.
    - Increased digitization and remote operations lead to heightened vulnerabilities, exposing banks to cyber threats and potential breaches.

- **Cybersecurity Challenges of Digitization:**
    - Cyber threats have evolved beyond traditional issues, encompassing activities such as stealing card data, reprogramming ATMs, and employing sophisticated software for money laundering.
    - Challenges include data management issues, legacy system limitations, securing third-party services, compromised network exposure, shortage of cybersecurity professionals, and governance compliance.

- **Evolution of Cyber Threats:**
    - The examination of this timeline offers valuable insights into the methods, tactics, and strategies employed by cybercriminals, facilitating a comprehensive understanding of the persistent threats faced by the banking industry.
    - Furthermore, the immediacy and significance of contemporary cybersecurity challenges are accentuated by recent incidents highlighted in the report. Specifically, the disclosure of over 40,000 reported cyberattacks targeting India's banks serves as a stark reminder of the ever-present and evolving risks faced by financial institutions.
    - Recent incidents, such as over 40,000 reported cyberattacks on India's banks, underscore the immediacy and significance of cybersecurity challenges.

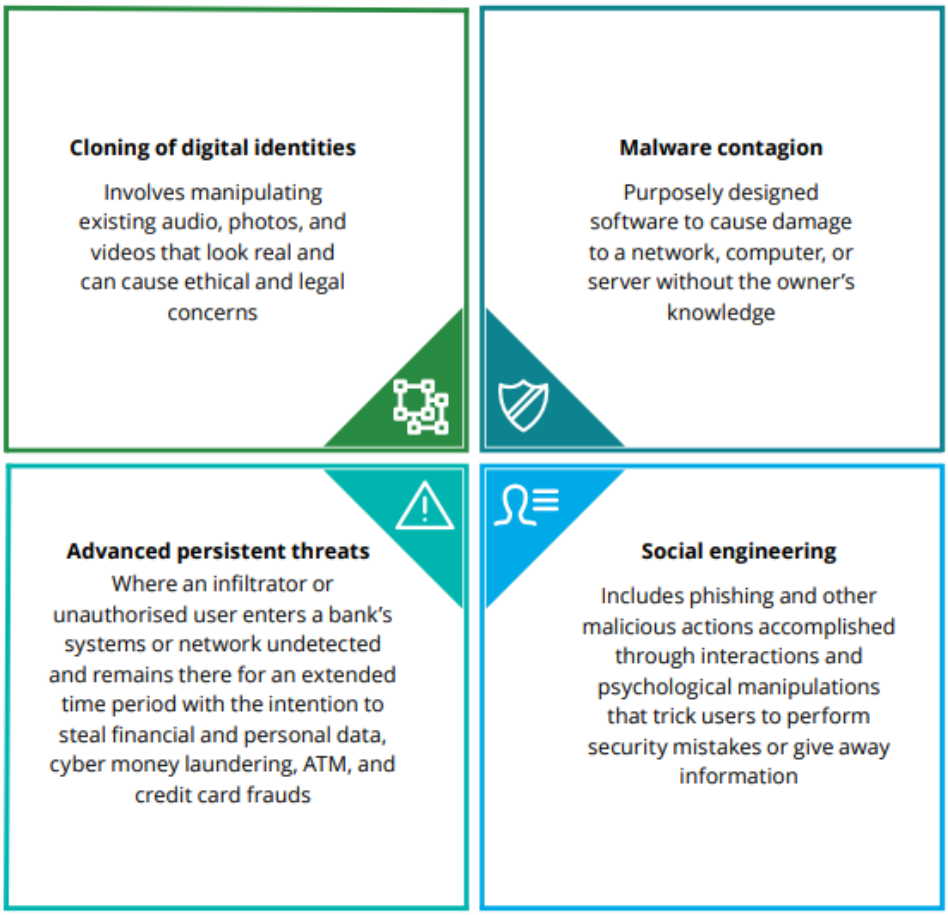


Figure 4 cyber threats challenges

- **Methodology and Recommendations:**
  - The recommended methodology includes continuous threat assessment, cybersecurity maturity assessments, and integration with fraud risk and financial crime reporting.
  - Recommendations for addressing cyber threats include prioritizing cybersecurity assessment, tightening access to third-party services, adopting advanced technology solutions, securing remote access control, contracting or outsourcing cybersecurity capabilities, and raising awareness through training.

Discussion

In the realm of consumer behavior and the adoption of digital banking, the research underscores the significance of maintaining a human touch in the digital era. The emphasis on in-branch communication and the evolution of roles within the banking staff highlights the importance of personalized interactions even as the industry embraces digitalization. The study aligns with the industry's imperative to cater to shifting consumer preferences by providing digital banking experiences that are both convenient and tailored to individual needs.

Concerning cybersecurity challenges in the process of digitalization, the research highlights the urgency for banks to undergo digitization while concurrently grappling with the complex interplay of innovation and security. The integration of advanced technologies, as emphasized in the study, underscores the dual challenge faced by industry. Moreover, the acknowledgment of heightened vulnerabilities underscores the imperative for robust cybersecurity measures to safeguard against potential breaches and cyber threats in the face of escalating digital operations.

Examining challenges specific to the digitization of banking processes, the research emphasizes the need for adaptive cybersecurity strategies, recognizing complexities such as data management issues and a shortage of cybersecurity professionals.

The historical perspective on cyber threats reveals the increasing sophistication of attacks, with the reported 40,000 cyberattacks emphasizing the constant threat, necessitating proactive cybersecurity measures.

In terms of methodology and recommendations, the research aligns with industry best practices, advocating for continuous assessment, integration with fraud risk reporting, and a comprehensive approach addressing both technical and human aspects of cybersecurity.

Conclusion

In the face of imminent cyber challenges, banks are compelled to adopt technologies like mobile, cloud, remote access, and IoT not merely as a choice but as a necessity to sustain and thrive in a post-pandemic business landscape. This transformative digitization, however, introduces an expanded attack surface, demanding a recalibration of strategies by bank executives to address ever-evolving cyber risks while simultaneously achieving overarching business goals. To create a resilient infrastructure for the future, banks must prioritize and invest in cyber defense initiatives. The impetus for this transformation lies in the hands of executives and board members who must set goals, allocate budgets, and drive the acceleration of cyber capabilities to match the rapid pace of digital transformation. Leadership decisions will determine the degree of agility, the pace of infrastructure change, and the collaborative efforts essential for building the cybersecurity landscape of the future.

The principles and generalizations

The principles inferred from the results are:

- **Adaptability in Digital Banking Adoption:**

  - Successful digital banking adoption hinges on adaptability. In-branch communication, role evolution, and modernization respond to shifting consumer preferences.
- **Dual Challenge of Digitization and Cybersecurity:**
  - Digitization and advanced technologies pose a dual challenge, demanding innovation and robust cybersecurity measures to address heightened vulnerabilities.
- **Evolutionary Nature of Cyber Threats:**
  - Cyber threats have evolved since 1970, emphasizing the need to understand the methods and strategies employed by cybercriminals over time.
- **Immediacy and Significance of Cybersecurity Challenges:**
  - The disclosure of over 40,000 reported cyberattacks underscores the immediate and significant contemporary cybersecurity challenges.
- **Holistic Approach to Cybersecurity:**
  - The recommended methodology advocates for a holistic approach, emphasizing continuous assessment, maturity assessments, and integration with fraud risk reporting.
- **Strategic Prioritization in Addressing Cyber Threats:**
  - Prioritizing cybersecurity assessment, tightening access, adopting advanced technology solutions, securing remote access, and raising awareness reflects a strategic and multifaceted approach to cybersecurity.

Exceptions

While the research report provides valuable insights into consumer behavior, digital banking adoption, and cybersecurity challenges in the Indian banking sector, there may be exceptions or factors not explicitly covered by the report. Here are potential exceptions or areas where additional considerations may be needed:

Regional Variances:

The report focuses on the Indian banking sector in a broad context. However, there might be regional variances within India that are not thoroughly explored. Different regions may exhibit unique consumer behaviors and cybersecurity challenges that are not adequately addressed in the report.

Size and Type of Banks:

The report broadly covers the banking sector, but exceptions could arise based on the size and type of banks. Larger, multinational banks may face different challenges compared to smaller, regional banks. Similarly, private sector banks and public sector banks may have distinct dynamics that are not explicitly differentiated in the report.

Government Policies and Regulations:

The report touches on regulatory changes but may not delve deeply into the specific impact of government policies and regulations on digital banking and cybersecurity. Different policy environments could result in varied challenges and opportunities for banks.

Customer Education and Awareness:

While the report emphasizes the need for banks to adapt to shifting consumer preferences, it might not extensively cover the role of customer education and awareness. Exceptional cases could involve banks with successful strategies in educating customers about digital banking security, potentially influencing consumer behavior positively.

Collaboration with Fintech Companies:

The report briefly mentions fintech disruption but may not explore in-depth the collaborative efforts between traditional banks and fintech companies. Exceptional cases might involve successful partnerships that mitigate cybersecurity challenges and enhance digital banking experiences.

Recommendations to address cyber threats.

The significant and imminent dangers that cyber criminals pose to banks cannot be overstated. Consequently, it is imperative for banks to establish a strong security threat monitoring system through the integration of cutting-edge solutions.

- **Prioritizing Cybersecurity Assessment:**
    - Continuous threat assessment using a risk-based approach.
    - Conducting cybersecurity maturity assessments.
    - Bridging identified gaps.
    - Integrating cyber risk assessment with fraud risk and financial crime reporting.
- **Tightening Access to Third-Party Services:**
    - Prioritizing access to services for alliance partners and vendors.
    - Restricting or controlling third-party access to core infrastructure.
    - Exploring contractual modifications to monitor third-party access to banking infrastructure.
- **Adopting Advanced Technology Solutions:**
    - Creating multiple lines of defense in the security ecosystem.
    - Utilizing defense options like zero-trust architecture, advanced endpoint security systems, AI-enhanced cybersecurity, and develops.
- **Securing Remote Access Control:**

- Enabling server-based computing and digital workspaces.
- Deploying zero clients and thin clients.
- Reviewing remote connectivity solutions and security governance.
- Implementing advanced authentication and authorization measures.
- Defining the scope of services requiring secured access.

- **Contracting or Outsourcing Cybersecurity Capabilities:**

  - Addressing shortages of cybersecurity professionals through third-party security providers.
  - Considering outsourcing various cybersecurity functions, including security operations and insider threat detection.

- **Raising Awareness Through Training:**

  - Implementing formal training programs on cyber threats and cybersecurity practices for employees.
  - Employing diverse methods to educate employees.
  - Cultivating a cybersecurity culture at every level, viewing it as a continuous process.
  - Bolstering Security Through Threat Identification and Response Competencies:

  - Integrating modern and evolving security infrastructure during digitization.
  - Embedding security, confidentiality, and policy checks into DevOps decisions and actions.

References

- Reserve Bank of India, RBI releases the financial stability report, July 2020, July 24, 2020, https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=50122

- Bank Quest, “Cyber security in banks”

- Data Security Center of India, “India Cybersecurity Services Landscape - A Global Hub in the Making”, May 21, 2020, https://www.dsci.in/content/India-Cybersecurity-Services-Landscape

- PTI, “Financial frauds rising due to dependence on digital payment platforms: NSA Ajit Doval”, Money Control, September 19, 2020,

- https://www.moneycontrol.com/news/india/financial-frauds-witnessing-a-spike-due-to-dependence-on-digital-payment-platforms-ajit-doval-5859641.html

- Deloitte Report in part 1 of digitization of banking sector focusing on Cybersecurity issues.