# **Initial cybersecurity risk scenarios developed for ACRB**

1. Inadequate Firewall Protection: Legacy firewall fails to detect modern-day threats, allowing attackers easy ingress.
2. Employee Insider Threat: Disgruntled employee intentionally leaks confidential client data to competitors.
3. Mobile Banking App Flaw: Vulnerability in the bank's mobile app allows unauthorized access to client accounts.
4. Physical Security Breach: Unauthorized person gains access to the bank's data center due to lax security checks.
5. Obsolete Encryption Standards: Older, now-cracked encryption methods are still in use, putting data transmissions at risk.
6. Third-party Vendor Weakness: A software vendor's weak security allows backdoor access to the bank's systems.
7. Lax BYOD Policy: An employee's infected personal device connects to the bank network, spreading malware.
8. Ransomware Lockdown: Critical bank data is encrypted by ransomware, with attackers demanding payment.
9. Ineffective Incident Response: Delayed response to a detected threat results in greater damage and data loss.
10. Unpatched Software Exploit: Known vulnerabilities in unpatched software get exploited, compromising data.
11. Cloud Misconfiguration: Incorrectly configured cloud storage buckets expose sensitive bank data to the public.
12. IoT Vulnerability: Smart devices in bank premises are hacked, serving as entry points for attackers.
13. Weak Password Policies: Employees using easily guessable passwords lead to unauthorized account access.
14. Social Engineering Attack: An attacker impersonates bank staff to gather sensitive information from clients.
15. Legacy System Exploitation: Continued use of outdated systems becomes an easy target for cybercriminals.
16. DDoS Attack: Bank's online services are disrupted, causing downtime and loss of business.
17. Database Injection Attack: Attackers exploit vulnerabilities to manipulate and steal data from bank databases.
18. VPN Exploit: A vulnerability in the bank's VPN allows unauthorized remote access.
19. Misleading SSL Certificates: Users are tricked into accessing fake bank websites, compromising their credentials.
20. AI-driven Attack: Advanced AI tools predict the bank's security responses and effectively bypass them.
21. Mismanaged User Access Rights: Employees have more access than needed, increasing the potential data breach scope.
22. ATM Malware: Local ATMs infected with malware, stealing card data from bank customers.
23. Keylogging Software: Malicious software records keystrokes, capturing passwords and sensitive data.
24. Man-in-the-middle Attack: Attackers intercept and manipulate communication between the bank and its clients.
25. Data Destruction: Cyberattack results in the deletion of critical bank financial records.
26. Malicious Insider Collaboration: Employees collaborate with external actors for financial gain, compromising bank operations.
27. Uncontrolled Use of Shadow IT: Employees use unsanctioned software, introducing vulnerabilities.
28. Data Misuse by AI Algorithms: AI tools misinterpret data, causing faulty financial predictions and decisions.
29. Inadequate Audit Trails: Lack of proper logging allows malicious activities to go undetected.
30. Unsecured API Endpoints: Weak security on bank's APIs allows unauthorized data access.
31. Mobile Device Data Leak: Lost/stolen employee mobile devices give attackers access to bank's internal communication.
32. Outdated Backup Protocols: Old backup methods don't secure data properly, leading to potential breaches.
33. Insecure Wireless Networks: Wi-Fi networks at bank branches are exploited due to weak encryption.
34. Uncontrolled Admin Privileges: Too many employees have admin rights, widening the threat landscape.
35. Voice Phishing (Vishing): Scammers use phone calls to extract sensitive info from unsuspecting bank clients.
36. Malicious Chatbots: Customer support chatbots are hacked to mislead customers.
37. Compromised Biometric Data: Biometric authentication data gets exposed, jeopardizing multifactor authentication.
38. Hardware Tampering: Physical tampering of bank's servers’ results in data compromise.
39. Insecure Code Deployment: Software deployed without proper security checks introduces vulnerabilities.
40. Client-side Scripting Attack: Client web browsers are targeted to steal session cookies.
41. Malicious Firmware Updates: Hardware devices receive rogue updates, causing malfunctions and data leaks.
42. Data Exfiltration via Printers: Networked printers are used as points to siphon out data.
43. Weak Security Training Programs: Employees are ill-prepared for modern threats due to outdated training.
44. Exploitation of Virtual Assistants: Voice-activated assistants on devices leak confidential conversations.
45. Rogue Mobile Banking Apps: Fake banking apps on app stores deceive users into compromising their data.
46. Inadequate Network Segmentation: Attack on one network segment easily spreads due to lack of isolation.
47. Webcam Surveillance: Webcams on bank's premises get hacked, compromising physical security.
48. Insufficient Data Masking: Sensitive data is insufficiently masked during testing, leading to potential leaks.
49. Clickjacking Attacks: Users are tricked into clicking hidden links, compromising their banking session.
50. Cryptojacking Malware: Bank's computer resources are hijacked to mine cryptocurrency, degrading performance.
51. Endpoint Protection Failure: Devices accessing the bank network lack adequate security, leading to potential breaches.
52. Spoofed Internal Communications: Attackers mimic internal email addresses, spreading misinformation or malware.
53. Server Room Environment Anomaly: Unmonitored temperature or humidity spikes damage server equipment.
54. Outdated Security Certificates: Expired SSL/TLS certificates erode trust and expose data in transit.
55. Blind Spots in Network Monitoring: Parts of the bank's network lack monitoring, allowing stealthy cyberattacks.
56. Digital Skimming Attacks: Attackers capture client data during online transactions.
57. Weakness in Two-Factor Authentication: 2FA mechanisms get bypassed due to flaws or social engineering.
58. Watering Hole Attack: Websites frequented by bank employees are compromised to target the bank's network.
59. Insufficient Patch Management: Delays in updating critical software leave systems vulnerable.
60. Third-party Data Handling Mishaps: External partners mishandle ACRB's sensitive data due to lax protocols.
61. Cryptographic Weakness: laws in cryptographic methods expose encrypted data.
62. Session Hijacking: Attackers take over user sessions to gain unauthorized access.
63. Data Hoarding: Employees or systems accumulate excessive data, amplifying breach impacts.
64. Post-breach Data Sale: Stolen bank data is sold on the dark web, leading to secondary attacks.
65. Unregulated Use of USB Drives: USB devices introduce or extract malicious content.
66. Customer Data Modification: Unauthorized changes to customer financial data lead to monetary losses.
67. Resource Exhaustion Attack: System resources are overloaded, causing service outages.
68. Misleading Domain Names: Domains resembling ACRB's lure customers into giving away their data.
69. Fileless Malware Attack: Malware residing in memory evades traditional detection mechanisms.
70. IoT Device Eavesdropping: Internet-connected devices capture and transmit confidential conversations.
71. Supply Chain Software Compromise: Software sourced from vendors contains pre-installed malware.
72. Remote Desktop Protocol (RDP) Exploits: RDP vulnerabilities provide backdoors for unauthorized access.
73. Exposure from Previous Breaches: Data from old breaches is used to launch new, targeted attacks.
74. Machine Learning Model Manipulation: ACRB's AI models are tampered with, leading to flawed outcomes.
75. DNS Cache Poisoning: Users are redirected to malicious websites when accessing ACRB's site.
76. Fraudulent Account Creation: Automated bots create fake accounts for money laundering.
77. Customer-facing Application Bugs: Flaws in user applications expose or compromise client data.
78. Misconfigured Security Groups: Incorrect permissions give users undue access to sensitive systems.
79. Misdirected Emails: Emails containing sensitive data are accidentally sent to the wrong recipients.
80. Misuse of Corporate Social Media: ACRB's social media accounts are hijacked, spreading false information.
81. Exploits via Obsolete Hardware: Old, unsupported hardware serves as a gateway for cyberattacks.
82. Proxy Server Manipulation: Bank's proxy servers are compromised, exposing user activities.
83. Digital Certificate Compromise: Stolen or forged certificates erode the trust of online platforms.
84. Unintended Data Sharing: Cloud configurations inadvertently expose data to unauthorized users.
85. Cross-site Scripting (XSS) Attack: Malicious scripts are injected into webpages viewed by bank users.
86. Data Backdoor Exfiltration: Hidden paths in systems allow data theft without detection.
87. Mobile Device Man-in-the-middle Attack: Banking apps on mobile devices get intercepted, compromising transactions.
88. Improper Data Sanitization: Old hardware, like hard drives, is discarded with retrievable data.
89. Inadequate Intrusion Detection Systems: IDS fails to identify new or sophisticated breach attempts.
90. Automated Teller Machine (ATM) Firmware Attack: Rogue firmware updates on ATMs compromise card data.
91. Malicious Insider Collaboration with External Threats: Employees secretly work with cybercriminals for data theft.
92. Shared Service Vulnerabilities: Shared IT services between branches have flaws, allowing lateral movement by attackers.
93. Replay Attacks: Authentic data transmissions are maliciously retransmitted or delayed.
94. Security Misinformation Among Staff: Employees follow outdated or misleading security advice.
95. Personal Device Compromise at Work: Personal apps or data on employee devices lead to corporate data exposure.
96. Wearable Tech Vulnerabilities: Smartwatches or fitness trackers used by staff are targeted for data interception.
97. Client-side Security Flaws: Bank's client applications lack adequate local security controls.
98. Compromised Virtual Environments: Virtualized IT environments in the bank are infiltrated.
99. Unauthorized Database Snapshot: Malicious snapshots of databases are taken for offline attacks.
100. Lack of Redundancy in Security Systems: Single points of failure in security infrastructure led to prolonged exposure.