Cybersecurity Checklist for For BFSI Navigating Rising Cyber Threats in GCC

paramount

Key Takeaways

1 Cyber attacks targeting banks in the GCC are rising, with over 150+ cyber incidents recorded in recent years, exposing critical financial infrastructure and customer data.

2 Digital banking ecosystems, including mobile apps, APIs, and third-party integrations, significantly expanded the attack surface for BFSIs.

5 Banks and financial institutions can reduce risk through phased cybersecurity implementation, continuous monitoring, automated threat detection, and strong response readiness.

4 A structured cybersecurity checklist helps banks prioritise crisis response, secure identity and data systems, and strengthen overall cyber resilience.

3 Common threats include DDoS attacks, credential theft, ransomware, destructive malware, and supply chain compromises.

Over the past few months, threat monitoring across the GCC region has recorded more than 150 cyber incidents affecting critical sectors. Banking and financial institutions appear at the top of the list, followed by, second only to government infrastructure. The reason is not difficult to understand.

Banks in the GCC operate some of the most digitally connected financial systems in the world. Customers use mobile banking apps, instant payment platforms, digital wallets, and online onboarding services for transactions. These innovations have transformed convenience. At the same time, they have created the cyber threat surface.

Today, a banking environment is rarely confined to a single network. It includes fintech partners, payment gateways, cloud infrastructure, third-party APIs, and customer-facing digital integration interfaces capability but also increases exposure.

As a result, this shift, cybersecurity is no longer a background technical process. It is now a function that has an impact on the stability of operations, customer trust, and public confidence in the financial system. A structured **cybersecurity checklist** can help banks address these evolving risks.

Before discussing how banks can respond to these issues, let's first examine the nature of the threats that define the regional landscape.

GCC banks face rising cyber threats due to increased digital connectivity, making strong cybersecurity essential for stability and trust.

Rising Cyber Incidents Across Critical Sectors in the GCC

Threat monitoring across the GCC has recorded 150+ cyber incidents in recent months affecting critical infrastructure sectors.

150+
Cyber Incidents
Across GCC Critical Sectors

Government Infrastructure
Most Targeted Sector

Banking & Financial Institutions
Second Most Targeted Sector

Other Critical Sectors
Energy | Telecom | Transportation

Financial institutions rank among the most frequently targeted sectors because they process high-value transactions and store sensitive financial data.

Types of Cyber Attacks Affecting BFSIs in GCC

Banks and financial institutions are particularly attractive targets for cyber attackers for several reasons.

FIRST
Banks process high-value digital financial transactions daily.

SECOND
They store highly sensitive customer and financial information.

THIRD
Their digital services are accessible and continuously available.

Top Attacks Targeting GCC BFSIS

Hacktivist Disruption Campaigns
Large-scale DDoS attacks overwhelm online banking portals, causing outages that damage reputation and disrupt operations

Credential Theft & Identity Attacks
Phishing and password attacks allow intruders to compromise, accounts, escalate privileges, and move within banking networks

Destructive Malware & Ransomware
Attacks that aim to disrupt banking systems by encrypting or damaging financial databases

Other Common Entry Points
- Remote access exploits targeting VPN gateways
- An-driven social engineering and phishing campaigns
- Supply chain compromises targeting fintech or technology partners
- Data exfiltration campaigns targeting customer records

Protecting identity security and entry points can mitigate up to 60% of attacks.

These characteristics make financial institutions especially vulnerable to multiple **types of cyber attacks** ranging from data theft to service disruption.

The major types of threats that are shaping the cyber landscape across the GCC include:

Hacktivist Disruption Campaigns

Hacktivist groups increasingly target financial infrastructure to create visible disruption and pressure institutions. In the GCC, these attacks have overwhelmed public facing banking systems using large scale **DDoS attacks**.

Online banking portals and payment services often become the primary targets. Even if data is not stolen, prolonged outages can damage operational resilience and customer trust.

Credential Theft and Identity Attacks

Many intrusions begin with something relatively simple. A phishing email captures employee credentials, or a password is reused across multiple platforms allowed password spraying across large numbers of accounts.

Once access is obtained, the attacker appears inside the network as a legitimate user. From there they may attempt to escalate privileges or move laterally between systems.

Destructive Malware and Ransomware

Threat intelligence also points to an increase in destructive malware. Some attacks have been carried out by ransomware groups, but several incidents involved attackers

Instead, the attacker attempts to damage systems or interrupt banking operations by targeting payment infrastructure or financial databases.

Other Common Entry Points

Beyond these primary attack types, security investigations frequently identify several additional entry points that attackers exploit to gain access to systems.

Common vectors include:

- Remote access exploits targeting VPN gateways
- An-driven social engineering attacks targeting employees
- Supply chain compromises affecting fintech or technology partners
- Data exfiltration campaigns targeting customer records

Research indicates that strengthening identity security and external attack surfaces can mitigate up to 60% of these attack vectors.

Understanding these threats and attack vectors is the first step in building cyber resilience. The next step is to ensure a structured **cybersecurity checklist becomes essential.**

Cybersecurity Checklist for BFSIs

Activate "Heightened Alert" Playbook
Implement change freeze, monitor critical systems, Establish 24x7 monitoring for anomalous activity, assets.

Activate Multi-Factor Authentication (MFA)
Mandate MFA on VPN, Remote access, Privileged accounts (VPN, SSH), Admin consoles, Cloud portals, "Crown-jewel" application protocols.

A structured response model helps banks and financial organisations organise their defences efforts in stages.

Review DDoS Mitigation Readiness
Confirm circulating carrier activation procedures, Confirm CDN, Ensure "always-on" for critical payment calls.

The checklist below outlines how institutions can move from urgent crisis response to structured hardening and long-term resilience.

Board & C-Suite Crisis Briefing
Confirm risk ownership, Assess operational disruptions, Define communication, Prepare authorities for network isolation scenarios.

Confirm CISO Incident Response Ownership
Ensure budget approvals, Activate emergency procurement, Monitor vendors, Verify SOC staffing levels and coverage.

Enterprise Credential Reset
Rotate high-risk, admin, and service credentials, Immediately invalidate stale sessions, Enforce re-authentication protocols.

Validate Remote Access Security
Audit VPN/Zero Trust access logs, Disable unused accounts, Block suspicious access, Review business logins.

Policy & Protocol Refresh
Update incident response playbooks, Accounts, Access Use Policy (AUP), Define communication standards for crisis mode.

Email & Phishing Hardening
Configure DMARC/DKIM/SPF strictly, Block suspicious domains, Pre-emptively block and URL reporting for risks.

Regulatory Notification (GDPR/Central Bank)
Map current analysis to GDPR, Central Bank, NCSC, CBB, CSR, DFSA, and CBD specific directives.

Vulnerability Management
Scan internet-facing assets daily, Prioritise critical CVEs, Patch critical systems, SLO/LLO within 24-48 hours.

Communication Strategy
Prepare templates, Coordinate with notification, customer communication, Establish regular updates, Provide staff alerts regarding threat levels.

Device Hardening
Disable USB/ removable media, Enforce critical system updates, Block macros, Integrate malware/ malware signatures, Enforce network hardening techniques.

Immediate Priority: Critical First Steps for Crisis Response & Strategic Oversight

The first priority during a period of heightened cyber threat activity is rapid stabilisation. At this stage, the focus is on reducing immediate exposure and ensuring that leadership teams have clear visibility into potential risks.

The immediate crisis response and governance measures include:

Immediate Crisis Response

- Confirm risk ownership and operational disruptions. Define communication and authorities for network isolation scenarios.
- **Confirm CISO Incident Response Ownership**
  Ensure budget approvals, Activate emergency procurement, Monitor vendors, Verify SOC staffing levels and coverage.
- **Enterprise Credential Reset**
  Rotate high-risk, admin, and service credentials, Immediately invalidate stale sessions, Enforce re-authentication protocols.
- **Validate Remote Access Security**
  Audit VPN/Zero Trust access logs, Disable unused accounts, Block suspicious access, Review business logins.
- **Activate "Heightened Alert" Playbook**
  Implement change freeze, monitor critical systems, Establish 24x7 monitoring for anomalous activity, assets.
- **Activate Multi-Factor Authentication (MFA)**
  Mandate MFA on VPN, Remote access, Privileged accounts (VPN, SSH), Admin consoles, Cloud portals, "Crown-jewel" application protocols.
- **Review DDoS Mitigation Readiness**
  Confirm circulating carrier activation procedures, Confirm CDN, Ensure "always-on" for critical payment calls.

Governance & Leadership

- **Board & C-Suite Crisis Briefing**
  Confirm risk ownership, Assess operational disruptions, Define communication, Prepare authorities for network isolation scenarios.
- **Policy & Protocol Refresh**
  Update incident response playbooks, Accounts, Access Use Policy (AUP), Define communication standards for crisis mode.
- **Communication Strategy**
  Prepare templates, Coordinate with notification, customer communication, Establish regular updates, Provide staff alerts regarding threat levels.
- **Regulatory Notification (GDPR/Central Bank)**
  Map current analysis to GDPR, Central Bank, NCSC, CBB, CSR, DFSA, and CBD specific directives.

High Priority: Hardening Defenses Across Identity, Network & Data Layers

Once immediate risks are addressed, attention shifts toward strengthening the technical foundations of the organisation's cybersecurity posture.

This stage focuses on closing the gaps that attackers commonly exploit after gaining initial access. Identity systems, endpoints, and network architectures become central areas of attention. At this stage, **measures include:**

Identity & Endpoint Defense

- **Privileged Access Management (PAM)**
  Implement Just-in-Time (JIT) access, Vault credentials for admins, Enforce session recording for critical infrastructure access.
- **Endpoint Hardening & Protection**
  Deploy EDR/XDR agents, Block lateral movement, Isolate infected systems, Ensure real-time malware capabilities are active.
- **Vulnerability Management**
  Scan internet-facing assets daily, Prioritise critical CVEs, Patch critical systems, SLO/LLO within 24-48 hours.
- **Device Hardening**
  Disable USB/ removable media, Enforce critical system updates, Block macros, Integrate malware/ malware signatures, Enforce network hardening techniques.

Threat Intelligence Integration

- **Network Segmentation** Isolate critical systems (core banking, SWIFT, and payment gateways), Restrict east-west traffic with strict firewall rules.
- **DDoS Protection & Web Security** Pre-arrange scrubbing with ISP/ Cloud provider, Deploy API Gateways with rate limiting for all public portals.
- **Encryption & Key Management** Encrypt data-in-transit (TLS 1.3+), Encrypt data-at-rest (AES-256), Rotate SSH and encryption keys regularly.
- **Data Loss Prevention (DLP)** Monitor sensitive data movement, Block unauthorized policies on USB/Cloud/Email, and insider threats to prevent exfiltration.
- **Centralized Logging & SIEM** Retain identity, VPN, DNS, and firewall logs for 12 months, Ensure real-time ingestion to SIEM for threat hunting.

Focus Area: Supply Chain Security, Recovery Planning & GCC Compliance

Even with strong technical defenses in place, banks and financial organisations must prepare for the possibility that incidents will still occur. The final layer of the framework therefore focuses on operational resilience and recognition risk.

At this stage, the measures include:

Incident Response & Continuity

Tested IR Playbooks
Verify specific playbooks for Ransomware, Wiper Malware, and DDoS scenarios. Update legal/PR/regulatory communication matrices.

Backup Integrity & Restoration
Ensure immutable/offline backups for core banking & payments. Conduct quarterly restore tests for critical databases.

Business Continuity Failback
Define manual workarounds (paper/offline) for critical payment/clearing processes. Confirm alternate channels (SMS/Voice) for customer notification.

Threat Intelligence Integration
Subscribe to GCC-specific threat feeds (Aftermarket of IOCs/TTPs, intra SIEM/SOAR. Conduct periodic threat hunting.

Tabletop Exercises (TTX)
Conduct crisis simulation workshops with executive leadership and operational teams to test decision-making speed.

Threat Intelligence Integration

Critical Vendor Tiering
Identify and tier vendors supporting critical functions (MSPs, Fintech, Cloud). Review SLAs for incident notification timelines.

Supply Chain Mapping
Map dependencies for SWIFT, Core Banking, and API partners. Identify non-redundant nodes for geopolitical conflict zones.

Regional Compliance Alignment
Map incident reporting to NCSC, CBB, Aligin with UAE NESAF, DFSA, CSR, DIFC, and CBD specific directives.

Audit Trail & Evidence
Maintain rigorous documentation of all security controls and incident response actions for audits and post-incident review.

SWIFT & Payment Security
Implement SWIFT CSP (Customer Security Controls Framework (CSCF). Enforce strict segmentation for payment zones.

Cybersecurity Implementation Roadmap for BFSIs

Financial institutions should implement cybersecurity improvements through a phased roadmap.

PHASE 1
Involves assessing internal facing systems and identifying critical exposed assets.

PHASE 2
Involves crisis simulation exercises so that leadership teams can practice cyber incident decision-making.

PHASE 3
Involves strengthening incident response capabilities and ensures that forensic capabilities are operational.

PHASE 4
Involves continuous monitoring supported by threat intelligence integration and security operations.

How Paramount Supports Cybersecurity Programs in BFSIs

Paramount provides cybersecurity services designed specifically for regional financial institutions and helps institutions implement a structured cybersecurity checklist to strengthen protection across critical systems. Key capabilities include:

Rapid Security Readiness Assessment:
A focused exposure review across internal facing assets, identity infrastructure, and endpoint defenses to identify immediate security gaps. Includes:

- External attack surface discovery and vulnerability assessment
- Identity security posture review, including MFA enforcement and privileged access management
- Endpoint protection
- Endpoint Detection and Response (EDR) tuning aligned with active threat actor techniques

Crisis Simulation Tabletop Exercises:
Interactive cyber tabletop exercises for executive and operational teams, simulating ransomware, wiper malware, and DDoS attacks. Includes:

- Executive decision-making stress testing during simulated incidents
- Validation of incident response playbooks and escalation workflows

Incident Response Readiness:
Dedicated incident response support with predefined service levels to enable rapid containment and minimise operational impact.

- 24x7 response readiness with a four-hour remote response SLA
- Forensic readiness assessment to support investigation and evidence preservation

Third Party Risk Management and MSR:
Strengthening visibility across vendor ecosystems with continuous monitoring and threat detection. It includes:

- Vendor risk tiering and supply chain mapping
- 24x7 SOC monitoring and threat hunting
- Security monitoring aligned with GCC regulatory frameworks such as DORA and NCA.

Final Thoughts

Cyber threats targeting financial institutions continue to evolve in scale and sophistication. Banks that implement a structured cybersecurity checklist and maintain continuous monitoring across critical systems can significantly better positioned to protect cyber attacks and maintain operational resilience.

Connect with Paramount to assess your cybersecurity posture and strengthen security across digital banking platforms, payment systems, and financial infrastructure.