TATA COMMUNICATIONS

TATA

Decoding SEBI's AI Cybersecurity Advisory: What financial institutions must prioritize now!

Preparing for AI-accelerated cyber threats and continuous cyber resilience

Cyber Security Services by Tata Communications

TATA COMMUNICATIONS

Executive Summary

AI is changing the speed and scale of cyber threats.

The latest cybersecurity advisory issued by SEBI reflects a growing need for stronger cyber resilience across the financial ecosystem. As financial institutions become more connected through digital platforms, APIs, cloud environments, vendors, and third-party applications, cyber risks are also becoming more interconnected.

AI-assisted tools have the potential to accelerate vulnerability discovery and exploitation. This reduces the time available for organizations to detect risks, respond to incidents, and protect critical systems.

SEBI's advisory highlights the need for:

- Continuous vulnerability management
- Faster patching and hardening
- Stronger SOC monitoring
- AI-assisted security operations
- API security
- Third-party risk visibility
- Zero Trust approaches
- Continuous cyber resilience

The broader message is clear.

Cyber resilience can no longer rely only on periodic reviews and isolated controls. Organizations need stronger visibility, continuous monitoring, faster response capabilities, and more adaptive security operations to manage evolving threats.

Financial institutions that modernize early will be better positioned to improve resilience, maintain trust, and strengthen operational readiness in an increasingly complex threat landscape.

TATA COMMUNICATIONS

Why this advisory matters?

Financial institutions today operate in highly connected digital environments.

Banks, exchanges, fintech platforms, cloud providers, vendors, and service partners are deeply integrated across the financial ecosystem. This improves operational efficiency and customer experience. At the same time, it also increases cyber risk exposure.

A weakness in one part of the ecosystem can potentially affect multiple connected environments.

This is one of the key reasons why SEBI's advisory is important.

The advisory reflects a broader industry concern that AI may significantly accelerate how vulnerabilities are identified and potentially exploited. As attack cycles become shorter, organizations may have less time to assess exposure, validate risks, and respond effectively.

Traditional cybersecurity models built around periodic assessments and reactive processes are now under pressure.

This signals a broader shift toward continuous and operational cyber resilience.

Organizations will need:

- Better operational visibility
- Faster response capabilities
- Continuous monitoring
- Stronger vulnerability management
- Better coordination across interconnected environments

The SEBI advisory also highlights the growing importance of:

- Continuous SOC operations
- Third-party risk visibility
- API security
- Security automation
- Zero Trust principles
- AI-assisted cyber resilience

TATA COMMUNICATIONS

5 Priorities financial institutions should focus on

1. Continuous Vulnerability Management

Security assessments can no longer remain periodic. Organizations need continuous visibility into vulnerabilities, faster patching cycles, and stronger hardening practices to reduce exposure.

2. AI-Augmented SOC Operations

Security operations teams need stronger monitoring, better alert prioritization, integrated threat intelligence, and faster response capabilities to manage evolving threats more effectively.

3. API Security

APIs continue to expand the attack surface across digital financial ecosystems. Strong authentication, visibility, controlled access, and continuous monitoring are becoming critical.

4. Third-Party Risk Visibility

Financial institutions increasingly depend on vendors, cloud environments, fintech platforms, and external service providers. Cyber resilience now requires stronger visibility and governance across the ecosystem.

5. Zero Trust and Security Hardening

Identity-led security, least privilege access, segmentation, and secure configurations are becoming essential for reducing attack surfaces and limiting unauthorized access.

Cyber resilience is no longer periodic. It must become continuous, adaptive, and operationally embedded.

TATA COMMUNICATIONS

How Tata Communications can help

Tata Communications helps enterprises strengthen cyber resilience through integrated security capabilities designed to improve visibility, accelerate response, and support continuous security operations.

Our Cyber Security capabilities Include

We work with enterprises to help

- Improve threat visibility
- Strengthen security operations
- Enhance monitoring capabilities
- Support vulnerability management
- Improve operational resilience
- Build more adaptive security frameworks

As cyber risks continue to evolve, organizations need stronger operational coordination, intelligence-driven security operations, and continuous resilience strategies to protect increasingly connected digital environments.

→ **Use the following 'Cyber Resilience leadership discussion guide' for practical discussion** areas for security, risk, and technology teams.

TATA COMMUNICATIONS

From Insight to Action

The next 5 slides provide ready-to-use discussion templates for security and IT teams to address the key priorities outlined in SEBI's advisory.

1. Move from periodic assessments to continuous vulnerability management
2. Strengthen SOC capabilities for AI-driven threats
3. Treat API security as a core security priority
4. Improve visibility into third-party and ecosystem risks
5. Accelerate Zero Trust and security hardening initiatives

TATA COMMUNICATIONS

Cyber resilience leadership discussion guide: Move from periodic assessments to continuous vulnerability management

Why this matters

AI-assisted threats can reduce the time between vulnerability discovery and exploitation. We may no longer have long remediation windows to identify, validate, and patch risks. We need stronger visibility, faster patching, and continuous validation of vulnerabilities across our digital environment.

Discussion questions

- Do we have continuous visibility into vulnerabilities across our critical systems and applications?
- How quickly can we patch or virtually patch critical vulnerabilities?
- Are we prioritizing vulnerabilities based on business impact and exposure?
- Do we have visibility into open-source dependencies and internet-facing assets?
- Are our vulnerability assessments periodic or continuous?
- How effectively are we coordinating vulnerability management across teams?

Current observations

-
-
-
-

Potential gaps

-
-
-
-

Priority actions

-
- .s

Key Stakeholders

1.
2.
3.
4.
5.

TATA COMMUNICATIONS

Cyber Resilience Leadership Discussion Guide: Strengthen SOC capabilities for AI-driven threats

Why this matters

Security operations teams are dealing with larger attack surfaces, faster-moving threats, and increasing alert volumes. AI-assisted attacks may further increase the speed and complexity of cyber incidents. We need stronger monitoring, better visibility, and faster response capabilities across our security operations.

Discussion questions

- Do we have continuous visibility across our systems, users, applications, and networks?
- Are we effectively analyzing both high-priority and low-priority SOC alerts?
- How quickly can we detect, investigate, and respond to incidents?
- Are our SIEM and SOAR capabilities integrated effectively?
- Do we have the right level of automation across our SOC operations?
- Are our threat intelligence capabilities helping improve detection and response?

Current observations

-
-
-
-

Potential gaps

-
-
-
-

Priority actions

-
-

Key stakeholders

1.
2.
3.
4.
5.

TATA COMMUNICATIONS

Cyber resilience leadership discussion guide: Treat API security as a core security priority

Why this matters

APIs are becoming central to digital financial services. They support customer applications, partner integrations, internal platforms, and digital ecosystems. As API usage grows, so does the attack surface. We need stronger visibility, authentication, monitoring, and governance across our APIs.

Discussion questions

- Do we have a continuously updated inventory of our APIs?
- Do we have visibility into unmanaged or shadow APIs?
- Are strong authentication and authorization controls consistently enforced?
- Are we monitoring API traffic for unusual activity or abuse?
- Are rate limiting and access controls implemented effectively?
- How frequently are API security assessments conducted?

Current observations

-
-
-
-

Potential gaps

-
-
-
-

Priority actions

-
-

Key stakeholders

1.
2.
3.
4.
5.

TATA COMMUNICATIONS

Cyber Resilience Leadership Discussion Guide: Improve visibility into third-party and ecosystem risks

Why this matters

We operate in a highly interconnected ecosystem involving vendors, cloud providers, fintech platforms, software providers, and external service partners. A weakness in one connected environment can potentially affect multiple parts of the ecosystem. We need stronger visibility, governance, and coordination across third-party relationships.

Discussion questions

- Do we have clear visibility into the cyber risks associated with our vendors and partners?
- How frequently are third-party security assessments conducted?
- Are patching and vulnerability management expectations clearly defined with vendors?
- Do we have visibility into third-party access to critical systems and data?
- How effectively do we coordinate incident response with external partners?
- Are we continuously monitoring third-party cyber risks?

Current observations

-
-
-
-

Potential gaps

-
-
-
-

Priority actions

-
-

Key Stakeholders

1.
2.
3.
4.
5.

TATA COMMUNICATIONS

Cyber Resilience Leadership Discussion Guide: Accelerate Zero Trust and security hardening initiatives

Why this matters

Traditional perimeter-based security models are becoming less effective in distributed digital environments. We need stronger identity validation, access control, segmentation, and system hardening to reduce attack surfaces and limit unauthorized access.

Discussion questions

- Are least privilege principles consistently enforced across users and systems?
- Do we have strong visibility into privileged access across our environment?
- How effectively are we implementing Zero Trust or ZTNA initiatives?
- Are unnecessary services, default accounts, and unused access pathways regularly removed?
- Do we have clear segmentation across critical systems and environments?
- How frequently are hardening standards reviewed and validated?

Current observations

-
-
-
-

Potential gaps

-
-
-
-

Priority actions

-
- .s

Key stakeholders

1.
2.
3.
4.
5.

TATA COMMUNICATIONS

Financial institutions that strengthen cyber resilience today will be better prepared to manage the next generation of AI-driven cyber threats.`

Engage with Tata Communications to Strengthen Cyber Resilience

tatacommunications.com

www.tatacommunications.com | @tata_comm

http://tatacommunications-newworld.com | www.youtube.com/tatacomms