Zaperon

WHITEPAPER

SEBI Cybersecurity Compliance Made Easy With Zaperon



Introduction

The Indian securities market is experiencing a boom, but this growth comes with the risk of increased cyberthreats. According to a recent report by CERT-In (Indian Computer Emergency Response Team), cyberattacks on Indian financial institutions have surged by 300% in the past three years and the top motive for such attacks is stealing of confidential information. This alarming trend highlights the critical need for robust cybersecurity measures.

The **Securities and Exchange Board of India (SEBI)** regulates India's securities markets, ensuring investor protection, promoting fair trading practices, and fostering market transparency. SEBI is also securing IT infrastructure of its regulated entities from cyberattacks by implementing stringent cybersecurity guidelines that require meticulous adherence.

300%

Increase in cyberattacks on Indian financial institutions in last 3 years

Source: CERT-in Report



SEBI Rolls Out Revised IT Governance and Cybersecurity Guidelines for Financial Sector

SEBI-regulated entities need to implement an enhanced cybersecurity and cyber resilience framework, as per guidelines released by the market regulator on June 27, 2024. The framework adheres to the five essential functions of cybersecurity outlined by NIST (National Institute of Standards and Technology): Identify, Protect, Detect, Respond, and Recover.

KEY COMPONENT OF CYBERSECURITY AND CYBER RESILIENCE FRAMEWORK



1. CYBER RISK GOVERNANCE AND MANAGEMENT FRAMEWORK

Establishes processes for identifying, assessing, & managing cyber risks within SEBI-regulated entities.



2. DATA CLASSIFICATION AND LOCALIZATION

Categorizes data into 'Regulatory' & 'IT/Cybersecurity' categories, requiring 'Regulatory Data' to be stored in India while allowing flexibility for 'IT/Cybersecurity Data'.



3. SECURITY OPERATIONS CENTRE (SOC)

Mandates the setup of a SOC for continuous monitoring & response to cyber threats, with periodic evaluations of its effectiveness.



4. API SECURITY AND MOBILE APPLICATION SECURITY GUIDELINES

Provides standards for securing APIs and mobile apps to prevent unauthorized access and data breaches.



5. CYBER CAPABILITY INDEX (CCI)

Introduces a metric to assess an organization's cyber resilience and readiness against cyber attacks.



6. SOFTWARE BILL OF MATERIALS (SBOM)

Requires the documentation of software components to manage supply chain risks and mitigate vulnerabilities.

Who Needs to Comply?

- Listed Companies
- Stock Exchanges
- Intermediaries
- Mutual Funds
- Portfolio Managers
- Credit Rating Agencies
- Custodians
- Depositories and Participants
- Investment Advisors
- Venture Capital Funds & Alternative Investment Funds
- Proxy Advisors
- Foreign Institutional Investors (FIIs) and Foreign Portfolio Investors (FPIs)



Consequences of Non-Compliance

MONETARY PENALTIES
Significant fines and additional penalties for delays.

LEGAL ACTION
Criminal prosecution and costly litigation.

OPERATIONAL DISRUPTIONS
Suspension of trading and debarment from the securities market and detailed audits.

REPUTATIONAL DAMAGE
Public disclosure of violations affecting investor confidence.

IMPACT ON MANAGEMENT
Disqualification of directors and personal liability.

INVESTOR COMPENSATION
Orders for restitution and refunds to investors

SEBI imposed a fine of **₹2 lakhs** on CDSL Ventures Ltd. after it failed to implement proper security measures to protect its IT infrastructure that led to a malware attack on November 18, 2022.

CDSL VENTURES LIMITED
...exploring new horizons

ventura

A fine of **₹5 lakhs** was imposed on stockbroker Ventura Securities Ltd. for non-compliance to various cyber security requirements including using applications without proper certifications, which increased their risk.

Ensure SEBI Compliance with Zaperon Identity Protection Platform 2.0

CLAUSE 5

Strong log retention policy should be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. REs/Members are advised to audit that all logs are being collected. Monitoring of all logs of events and incidents to identify unusual patterns and behaviors should be done. Refer SEBI circular CIR/MIRSD/24/2011 dated December 15, 2011.

COMPLY WITH ZAPERON

Zaperon logs application access information for all the users and real-time compliance of each user device. Activities of the admin users can also be tracked in the system logs. These logs are securely stored and can be audited to identify any unusual patterns or behaviors, ensuring compliance with SEBI regulations.

CLAUSE 6i

Strong password policy should be implemented. The policy should include a clause of periodic review of accounts of ex-employees. Passwords should not be reused across multiple accounts or lists of passwords should not be stored on the system.

COMPLY WITH ZAPERON

Zaperon eliminates the need for passwords, thereby mitigating risks associated with password reuse and storage. Our console allows for immediate revocation of access for ex-employees from devices and applications. In case any identity threat is detected, Zaperon promptly blocks the access and issues alerts.

CLAUSE 6ii

Enable multi-factor authentication (MFA) for all users that connect using online/ internet facilities and also particularly for virtual private networks, webmail, and accounts that access critical systems.

COMPLY WITH ZAPERON

To secure any type of applications (SaaS, on-premise, desktop), Zaperon enables phishing-resistant MFA that validates 15+ factors related to device certificate, user behavior, device posture and context. This is crucial to ensure only authorized users get access to the applications.

CLAUSE 7ii

For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) should be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter.

COMPLY WITH ZAPERON

Zaperon leverages zero trust framework to offer least privilege access, continuous device trust and proactive identity threat detection.

Each user is assigned to applications that they can access and only from authorized and secure devices.

Zaperon also uniquely identifies each user device using PKI-based certificate and continuously monitors the device posture ensuring secure access for users from any location.



Zaperon Identity Protection 2.0



PKI-BASED PASSWORDLESS AUTHENTICATION

Leverages PKI to provide secure, passwordless access, minimizing the risk of data breaches from credential compromise.



PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION

Deploys MFA that resists phishing attacks, boosting security with over 15 factors.



CONTINUOUS ZERO TRUST ACCESS CONTROL

Continuously applies zero trust policies based on user behavior and device status, ensuring ongoing compliance and security.



PROACTIVE IDENTITY THREAT DETECTION AND RESPONSE

Identifies anomalies in user behavior and device posture, reducing the likelihood of identity-based attacks.



COMPREHENSIVE IDENTITY PROTECTION

Ensures robust security of users, devices, applications, and cloud infrastructure by combining strongest authentication of PKI, phishing-resistant MFA and proactive threat detection and response.

Zaperon revolutionizes identity protection with its cutting-edge platform, shielding organizations from identity-based threats. By leveraging PKI-based passwordless access and phishing-resistant multi-factor authentication, it maintains continuous zero-trust policies informed by user behavior and device posture. Through proactive identity threat detection and response, Zaperon provides robust security for users, devices, applications, and cloud infrastructure.


+1 202 600 5234


+91 8800 170387

sales@zaperon.com

www.zaperon.com

© 2024 Zaperon, Inc.
All Rights Reserved.