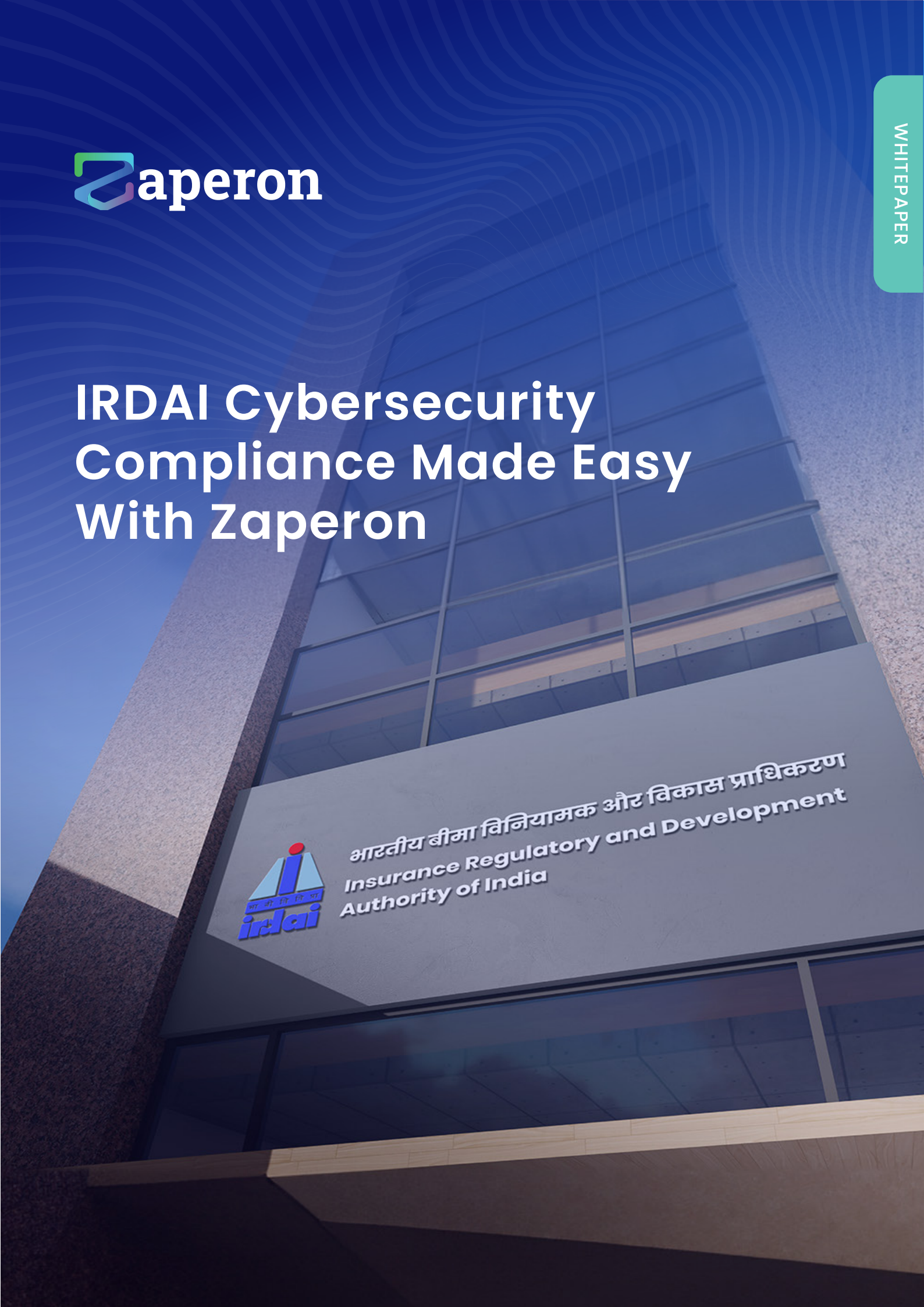
Zaperon

WHITEPAPER

IRDAI Cybersecurity Compliance Made Easy With Zaperon



Introduction

In the insurance industry, increase in cyber-attacks is a concern mainly driven by the sector's extensive handling of large volumes of sensitive personal and financial data. A report published by Black Kite reveals that 82% of major insurance carriers globally were targeted by ransomware attacks in 2021.

Since the insurance business largely revolves around trust, a major breach can have a huge impact on the insurer's brand and market value. This heightened risk necessitates robust cybersecurity frameworks, which are integral to maintaining trust and compliance within the industry.

In India, the **Insurance Regulatory and Development Authority of India (IRDAI)** plays a vital role in overseeing the industry's adherence to cybersecurity standards, ensuring consumer protection, fair competition, and financial stability. Cybersecurity is a critical component of IRDAI compliance as the insurance industry becomes increasingly data-driven.



IRDAI Rolls Out Revised IT Governance and Cybersecurity Guidelines for Insurance Sector

Acknowledging the criticality of protecting sensitive data and fostering trust, the IRDAI introduced Information and Cyber Security Guidelines on April 24, 2023.

These guidelines aim to bolster the insurance sector's cybersecurity framework against emerging cyber threats.

1. **Policy Development:** Organizations must adopt comprehensive policies covering Information and Cyber Security, Data Classification, Asset Management, and others to ensure a robust cybersecurity framework.
2. **Risk Assessments:** Annual risk assessments by external providers are required before major technological changes, covering all aspects of the organizations including systems, processes, and third-party vendors.
3. **CERT-In Compliance:** Entities must adhere to CERT-In's directives, including mandatory reporting of specific cyber incidents within 6 hours and appointing a liaison for compliance.
4. **Data Protection Measures:** Implementation of measures like encryption, access control, and limitation on collecting sensitive personal information is necessary to align with India's data protection framework.

Who Needs to Comply?



Consequences of Non-Compliance

FINANCIAL PENALTIES
Fines for non-compliance.

LOSS OF LICENSE
Revoking the entity's license, stopping operations.

LEGAL ACTION
Legal proceedings and penalties.

REPUTATIONAL DAMAGE
Trust and credibility can suffer.

OPERATIONAL DISRUPTIONS
Changes may disrupt operations and incur costs.

REGULATORY SCRUTINY
Increased monitoring and auditing.



IRDAI Compliance with Zaperon Identity Protection Platform 2.0

Section 2.3

ACCESS CONTROL

All user accesses to Organization's information assets shall be specifically and individually authorized based on business need.

Procedures shall be administered to ensure that appropriate level of access control is applied to protect the information in each system from unauthorized access, modification, disclosure, or destruction to ensure that the information remains accurate and confidential and is available when required.

COMPLY WITH ZAPERON

Zaperon implements least privilege access controls based on user roles, device identity, IP, geo-location, antivirus status, operating system version, and access time. These controls ensure that users only have access to necessary resources and data as per business needs and they could only access them from authorized, secure devices. Continuous monitoring and logging of privileged user activities provide a clear audit trail.

Section 2.1.6

MONITORING, LOGGING, AND ASSESSMENT

All critical information systems deployed by Organization for information processing, storage, or security shall be monitored through the following means:

I. Real-time monitoring through manual means or technology systems capable of generating alerts.

II. Logging of all activities or transactions performed on information systems and periodic analysis of logs.

III. Periodic or one-time security posture assessment exercises including but not limited to device configuration review, security testing of information systems, and review of IT processes set up for real-time or periodic monitoring.

COMPLY WITH ZAPERON

Zaperon continuously monitors user behavior and device posture, and provides a comprehensive log for all applications accessed by users, along with visibility into the real-time security posture of devices. The system also tracks the activities of admin users. Zaperon enhances security with strong passwordless authentication using PKI and phishing-resistant multi-factor authentication (MFA), which validate 15+ factors related to device certificates, user behaviour, device posture and context.

Section 2.2.2

WORK FROM REMOTE LOCATION

1. Prevent occurrence and recurrence of cyber incidents by implementing proactive security measures.
2. Create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards, and guidelines.
3. Create mechanisms for security threat early warning, vulnerability management, and response to security threats.
4. Create mechanisms to prevent leakage of confidential information.

Remote access to employees/ vendors/ contractors shall be provided on need to know and need to do basis only.

COMPLY WITH ZAPERON

Zaperon employs a zero-trust architecture that secures remote access to apps, network devices, and servers without relying on vulnerable VPNs. It uses phishing-resistant multi-factor authentication (MFA) for robust protection of critical systems. Zaperon continuously logs and monitors the posture of all devices, including those used remotely, ensuring only secure and compliant devices can access enterprise resources.

Zaperon also prevents data leak from endpoints and cloud applications. By providing remote access based on need-to-know and need-to-do principles, Zaperon prevents cyber incidents, supports conformity to cybersecurity standards, offers early threat warnings, manages vulnerabilities, and prevents confidential information leakage.



Zaperon Identity Protection 2.0

PKI-BASED PASSWORDLESS AUTHENTICATION

Utilizes PKI for secure, password-free access, minimizing data breach risks.

PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION

Implements MFA with over 15 factors to enhance security against phishing attacks.

CONTINUOUS ZERO TRUST ACCESS CONTROL

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

PROACTIVE IDENTITY THREAT DETECTION AND RESPONSE

Identifies anomalies proactively to mitigate identity threats and reduce security incidents.

COMPREHENSIVE IDENTITY PROTECTION

Integrates proactive threat detection and response to safeguard users, devices, applications, and cloud infrastructure comprehensively.

Zaperon transforms identity protection with its advanced platform, safeguarding organizations against identity-based threats. Using PKI-based passwordless access and phishing-resistant multi-factor authentication, it enforces continuous zero-trust policies based on user behavior and device status. With proactive identity threat detection and response, Zaperon ensures strong 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.