CSAI - DELL TECHNOLOGIES

WHITE PAPER

ACHIEVING CYBER RESILIENCE THROUGH DATA PROTECTION ACROSS CRITICAL INFRASTRUCTURE & SECTORS

Released by CYBER SECURITY ASSOCIATION OF INDIA (CSAI)
with the support of Dell Technologies

21st January, 2026

www.ncsai.in

Achieving Cyber Resilience through Data Protection across Critical Infrastructure/Sectors

With the rapidly changing threat landscape, the cybersecurity posture must also continuously evolve for organisations. **Cybersecurity frameworks** such as the **NIST Cybersecurity Framework (CSF), ISO 27001, CIS Critical Security Controls, PCIDSS, SOC2, etc.** provide apt guidance on how organizations should prepare for, withstand, and recover from different cyber attacks. However, these frameworks intentionally provide a high level path for implementing the security controls / measures required to safeguard the organisations. Through this paper and referencing the NIST Cybersecurity Framework (NIST CSF), we discuss the **Respond** and **Recover** functions while attempting to achieve/create a more actionable process in the context of clean cyber recovery.

In **NIST CSF** terms, the **Recover** function is to develop and implement appropriate steps to maintain actionable plans for resilience and restore capabilities or services that were impaired due to a security incident. It assumes an incident has already occurred and emphasizes a planned and controlled recovery that brings the business to normal.

Evolving Cyber Resiliency and the Need for Clean Recovery

Every organization must continuously review its **Cyber Resiliency Posture** — how well it is prepared to withstand, respond to, and recover from cyber incidents. The time taken to respond and recover from a cyber incident, for an organization reflects its **Cyber Resiliency Maturity**.

Recovery is a vital element of cyber resiliency. The Backup and Recovery Architecture implemented in an organization plays a very vital role and provides confidence to the organization to **confidently recover critical applications and data** in order to bring back the business operations online after an attack and provide the requisite serviceability to its customers. Recovering from a cyber-driven disruption, however, is fundamentally different than recovering from a operational outage in traditional IT or service/business disruption.

During a cyber incident, the most critical task is identifying a **“clean” copy** of the most recent data backup. Organizations exhibit confidence in their ability to recover through continual assessment against three core aspects:

- **Reduce exposure for all systems** – Infrastructure hardening through **Secure Configurations**, prompt closure of exploits / vulnerabilities through robust **Vulnerability Management**, and **minimize the attack surface** before an incident strikes the organisation.
- **Detect and respond to incidents** – Rapid / quick identification of suspicious or malicious actors / vectors and take immediate actions to contain and remediate.

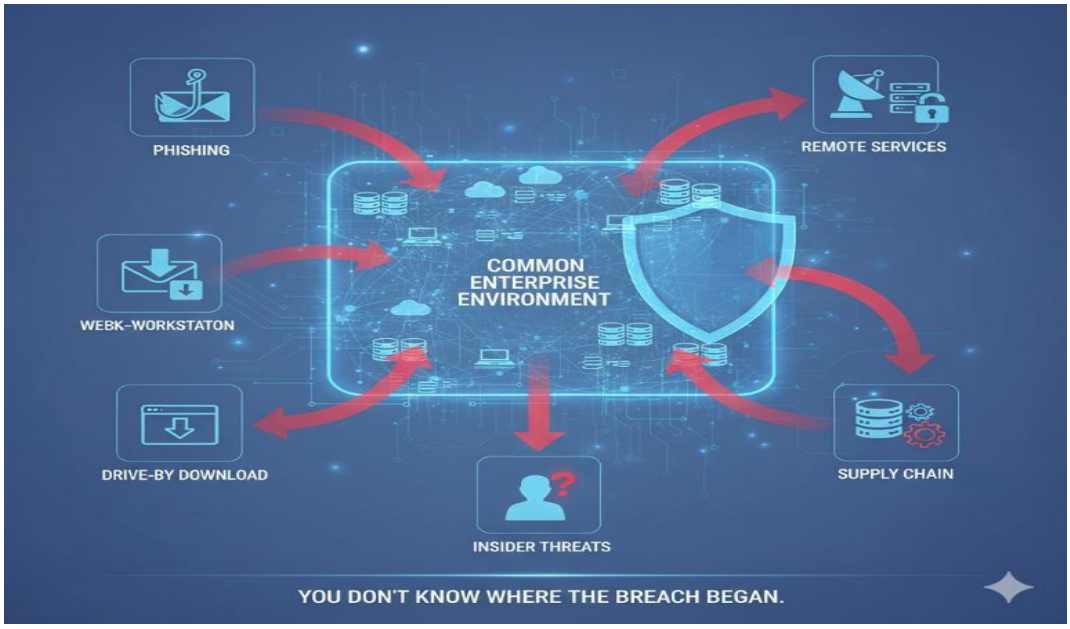
- **Restoration Testing – regularly test the restoration of backed up data** – periodic validation of clean, recoverable copies of critical workloads and the recovery process itself which works under realistic simulations.

Minimising Exposure: Initial Access and System Vulnerabilities

Despite a plethora of detection mechanisms and tools, it remains difficult to isolate or narrow down when a threat actor first gained access and how extensive is the quantum of the damage / compromise in the given environment. Many breaches, especially those involving malware or destructive ransomware, begin with exploiting system vulnerabilities.

Frameworks such as **MITRE ATT&CK** catalogue the tactics and techniques used by real-world adversaries. The initial access can occur through multiple vectors including:

- Phishing emails and malicious attachments
- Content injection or drive-by downloads
- Compromised external remote services



As one of the measures for proper remediation, organizations must adopt and implement a strong **Patch Management** for prompt and proactive closure of vulnerabilities.

However, not all compromises originate from obvious known vectors. Breaches can happen through:

- The **supply chain**, where third-party software, services, or hardware are compromised
- **Insider threats**, whether intentional or inadvertent
- Unauthorized or tampered **hardware** added to information systems

In highly regulated or mission-critical environments, these risks can get magnified when the critical systems of the organization are hosted in **collocated data centres**, where the physical and logical separations isolations may be weaker or more complex to manage.

Building Secure Data Protection Architectures

To achieve **clean recovery**, it is crucial that the systems responsible for protecting applications and data are **designed, implemented and maintained correctly**. Organizations typically choose between:

- **"Build your own" architectures** – Custom-designed and integrated architectures and solutions assembled from various components.

- **"Ready-to-use" architectures** – Pre-engineered solutions with opinionated design and controls implementation that may not match the scalability required as the organisations grow.

Regardless of the approach, the guiding principle is the same: architect the environment to be as **secure, resilient, and recoverable** and scalable to meet the organisation's requirements.

Threat actors, with their malicious motives, may seek to either:

- Steal sensitive data, or
- Corrupt or encrypt data to demand ransom, or
- Silently manipulate data for espionage, or
- Delete data to cause operational disruption

Most organizations rely on **disk-based backup solutions** and use tapes or cloud-based storage solutions to primarily store backups for long-term retention and portability. When the disk-based solutions are built for general-purpose storage or server-based designs, there are multiple performance, configuration, and security considerations that need to be looked into. These environments, therefore, require **strict governance** measures to minimize the exposure across:

- Operating systems
- Backup and data protection software
- Storage systems
- SAN switches and network components
- Firmware across the entire stack

Continuous monitoring of all the layers is essential to detect configuration drift, vulnerabilities, or misuse before attackers exploit them.

Intrinsic Security, Access Control, and Governance

Information systems used for data protection must be built using **trusted hardware and software components**. Systems with **intrinsic security requirements,** implemented at the chip or processor level, ensure that only authenticated BIOS or firmware can boot. Each time the system powers on, the built-in cryptographic authentication functions verify that the firmware is genuine. If tampering is detected, the system does not boot normally, preventing the execution of low-level attacks.

Deploying the **Zero Trust Security Architecture**, these systems should enforce:

- **Role-Based Access Control (RBAC)** – Users are granted only the minimum permissions based on pre-defined roles and the associated access levels.
- **Multi-Factor Authentication (MFA)** – Access requires multiple, independent factors for authentication, thereby reducing the risk of credential abuse.

However, there have been many instances where **privileged and authorised accounts** themselves e.g. administrative accounts, service accounts, are either exploited or created with malicious intentions. At times, such accounts also go undetected for long periods. To mitigate this, organizations need **governance models** where no single administrator can perform high-risk actions that may potentially compromise critical business / customer data.

Examples include:

- **Dual control / four-eyes principle** – Any change to critical policies, such as retention settings or deletion of backup data, must be authorised by an additional privileged user (e.g., a security officer). Such actions may be configured using Maker-Checker mechanisms
- **Time-based command blocking** – Critical bulk operational commands (such as bulk deletion) may be blocked during specific timeframes, preventing both accidental and intentional destruction of critical data even by administrators.

It is important that these controls are **implemented as built-in, default system features**, not just documented as processes. Software-enforced controls are less prone to human error and ensure consistent enforcement, even under stress or during an active incident. Here, it is also important to note that such systems / applications should be developed using the **Security by Design** principles.

Protecting Backup Data: Encryption and Time Integrity

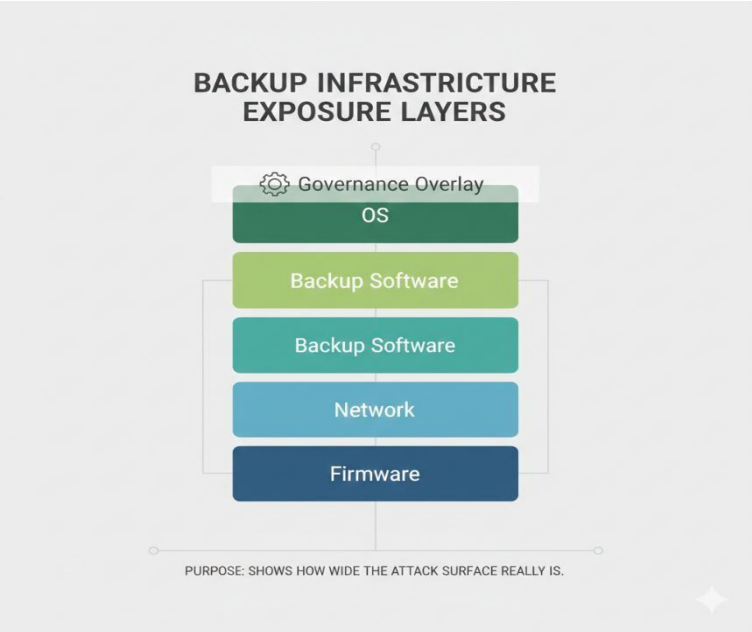
Backup systems are easy and attractive targets for threat actors, especially those seeking **data pilferage or data breaches**. Backups files often aggregate sensitive information from databases, file shares, and applications, making them a rich single source of truth. Historically, backup

environments have also been less protected than production systems, which increases their appeal factor to attackers.

To counter this, organizations need implement **end-to-end encryption** strategies for backed up data. By adopting these methodologies, it is ensured that the data protection is not treated as a mere checkbox item; but the encryption-decryption capabilities ensure that the data is protected:

- From the moment it leaves the client
- Across the network
- At rest on primary and secondary storage
- During replication to other sites or cloud locations

In other words, the data protection is meted at all the three stages of data processing i.e. Data-in-Use, Data-inTransit, and Data-at-Rest.



Using strong encryption algorithms such as **AES-128** or **AES-256** and **FIPS-validated cryptographic libraries,** it is ensured that compromised backup sets are useless to attackers who do not have access to the cryptographic keys used while taking the backups, even if they are in physical possession of the storage media, or intercepting network traffic using the Man-in-the-Middle attacks, or if the secondary site is compromised.

A strong Key Management Strategy and process will provide Organizations with **full control over PKI Infrastructure**, including the backed up data stored in public cloud environments. Losing control of PKI Infrastructure effectively means losing control of the data.

Another critical risk is **“attack on the clock”** scenarios, where attackers manipulate system time to defeat retention policies or immutability guarantees. To prevent this, backup systems should:

- Monitor time using a **protected internal clock**
- Continuously comparison of system time against trusted references
- Alert generation on time drifts beyond acceptable thresholds or when it appears to be manipulated
- Lock or protect filesystems if significant time anomalies are detected

These measures ensure that time-based retention and immutability policies cannot be bypassed simply by changing the clock.

Immutability: Necessary but Not Sufficient

Immutability can be enforced at multiple levels for backup data. **Regulatory-grade immutability** provides the most stringent level of protection, preventing both deletion and tampering of data, once it is written to the media and a retention period is defined. Under regulatory-grade controls:

- Data cannot be altered or deleted until retention period expires, even by administrators.
- **Access controls** and **segregation of duties** ensure clear separation between system administrators and records managers.
- Reliable **timestamps and audit logs** are maintained, and system time manipulation is tightly controlled.

While immutability is a powerful safeguard, **it is not sufficient on its own** in view of the modern techniques used in the cyberattacks. Now, the adversaries actively target the backup infrastructure, steal credentials, and take control of the management consoles and not just production data. If an attacker controls your identity provider, hypervisors, or backup servers, they may still attempt to tamper with policies, encryption keys, configurations or even monitoring systems.

This is where **Isolation of the data also known as Air-Gapping,** becomes critical. Immutability must be combined with architectural separation that assumes an attacker might already have a broad administrative access in the production environment.

Isolated and Air-Gapped Vault Architectures

To withstand advanced cyberattacks, organizations should implement an **isolated (air-gapped) cyber vault**. An **Isolated Vault** is a logically, and often physically segregated environment where **immutable, access-controlled copies** of the most critical data are stored. Key characteristics of an isolated vault include:

- **Network isolation** – The vault runs on its own network segment, with no direct inbound connectivity from production.

- **Independent credentials and identity** – Vault access is managed separately from production identity systems such as Active Directory.

- **Automated air gap** – The vault is connected to production environment only during automated replication windows which in turn are tightly controlled through Access Control implementations

The design separates **data paths** from **control paths**:

- The **only** traffic between production and the vault is **encrypted backup data** over a dedicated replication link.

- No management traffic, user interfaces, or remote shells (e.g., SSH) traverse this link.

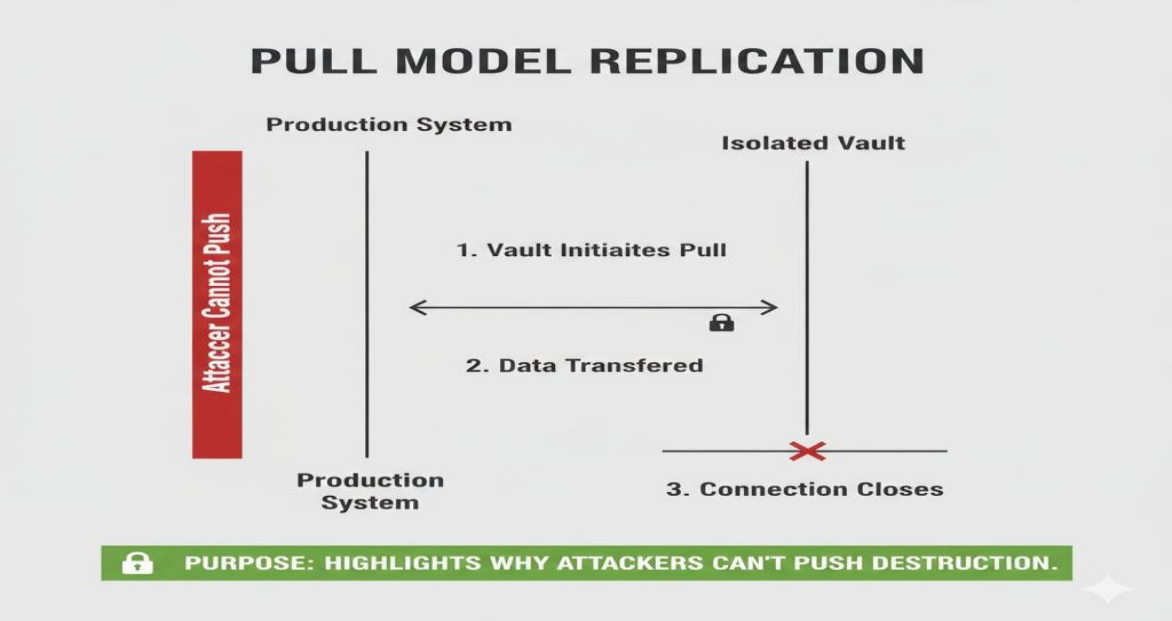
In this model, even if attackers gain full control of the production domain, the backup servers, or the hypervisors, it would still be difficult to **log into the vault, change policies or cofigurations, or destroy vault data** over the data link.

The vault operates on a **pull model**:

- As per the configured backup schedule, the vault reaches out to pull in new backup data from the data source.

- After replication, the connection is closed, ensuring there is no persistent inbound path available for exploitation by the attackers.

This architecture makes the vault a **last line of defense**: a secure location where clean, immutable copies of critical data are preserved, beyond the reach of attackers who may dominate the production environment.



Beyond Anomaly Detection: Full-Content Integrity Analytics

Many organizations rely on **anomaly detection** to identify potential malware or ransomware activity in backup data. Traditional anomaly detection typically focuses on **metadata and behavioural patterns**, such as:

- Changes in file counts or sizes
- Shifts in file extensions
- Unusual backup durations or volumes
- Abnormal system events or backup behaviours
- Abnormal network activity going out of the perimeter network.

While useful for early warning, **metadata-only anomaly detection has significant limitations** in modern, stealthy attack scenarios:

- Advanced attackers may corrupt file contents or database pages while leaving names, sizes, and timestamps largely unchanged.
- "Low-and-slow" encryption or corruption may stay under anomaly thresholds and avoid detection.
- Models that rely on behavioural analytics and thresholds, can be **poisoned** over time as attackers gradually manipulate the environment.
- Anomaly engines often run in the **same environment that is under attack**, meaning their configurations, credentials, and monitoring data can also be tampered with.

To reliably identify **clean, recoverable copies**, organizations need **deep, full-content integrity analytics** across all workloads—files, virtual machines, and databases.

Such solutions should:

- Perform **content analysis**, and not just metadata checks.
- Use of full-content **indexing and analytics** to inspect files, databases, and cryptographic key infrastructure datasets.
- Calculate **hundreds of content-level indicators** (e.g., structural changes, entropy, header integrity, and database-page anomalies).
- Detect partial, stealthy, and low-and-slow encryption that does not trigger simple anomaly rules.

By establishing a well-defined and documented architecture and it's sub-components, to see how each object is impacted over time, the **full-content integrity analytics** can flag data corruption in a deterministic manner and confirm which of the available restore points are clean and useable.

When these analytics are run **inside the isolated vault** on **immutable backup copies**, they provide an independent, tamper-resistant view of the integrity factor of data. This combination allows security and recovery teams to:

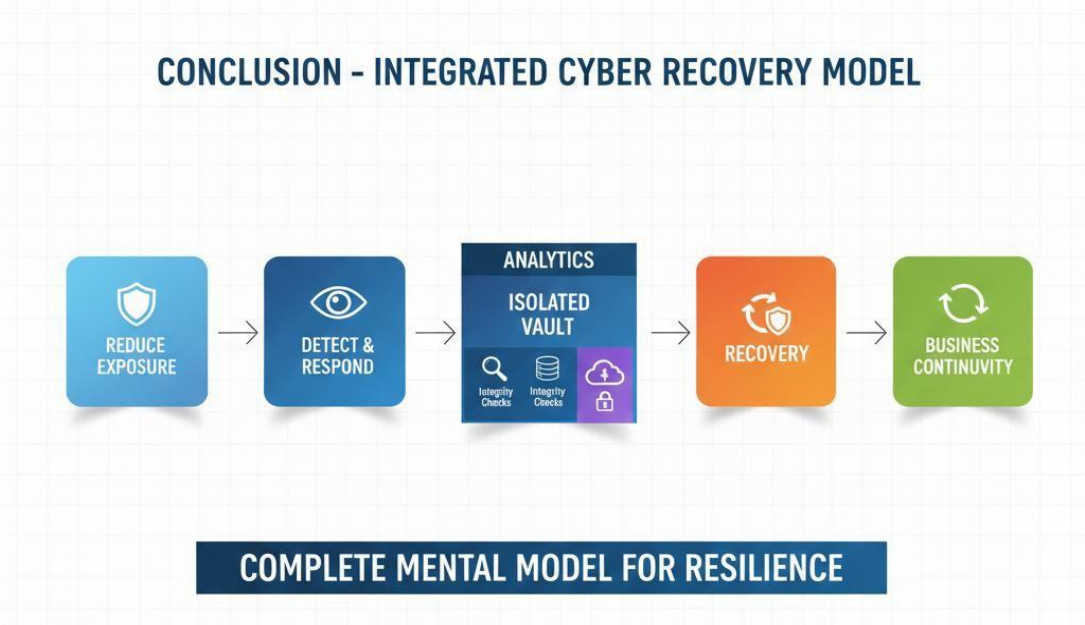
- Identify **known-good** recovery points with high confidence
- Avoid restoring corrupted or partially encrypted data to the production environments
- Reduce the risk associated with tampering of critical data that is required for recovery,

In summary, while anomaly detection remains valuable as an **early warning system**, the adoption of **deep, full-content integrity scanning** of **immutable backup copies** stored in an **operationally air-gapped vault** can reliably determine which data is uncorrupted, safe to restore, and capable of bringing the business back online after a cyber incident, in true sense.

Conclusion

Modern cyber threats have forced the organizations to rethink their recovery strategies beyond the traditional disaster recovery architectures. To confidently achieve **a clean cyber recovery**, organizations are required to:

- Improve on their Cyber Resiliency Maturity Model and their Cyber Resiliency Posture on a continual basis**,** aiming at across reducing the exposure or the attack surface, rapid detection and response, and a periodic and thorough recovery testing drills.
- Architect the data protection systems with **inherent security controls**, strong governance model, Maker-Checker controls for authorisations, and robust encryption methodology.
- Implement a **regulatory-grade immutability** that combines with protected retention and stringent access controls.
- Build an **isolated, air-gapped vault** with independent credentials, isolated network configuration, and stringently configured and isolated data and control paths.
- Leveraging the anomaly detection with augmentation to **full-content integrity analytics** helps in identifying clean, recoverable data.



By adopting these elements and methodologies, the organizations will be able to dramatically reduce the risk imposed by the cyberattacks and perpetrators of such attacks, to compromise their last line of defense and shall be able to restore their business operations known-good data and confidently maintain business continuity, even after a cyber incident.

Dell Technologies Power Protect Cyber Recovery Solution

The Dell PowerProtect Cyber Recovery solution can be positioned as the practical implementation of the clean cyber recovery principles described in this whitepaper, aligned to the NIST Cybersecurity Framework (CSF) Respond and Recover functions and focused on restoring business services from known-good data after an incident. It combines hardened data protection platforms with role-based access control (RBAC), multi-factor authentication (MFA), dual-control governance for high-risk operations, end-to-end encryption and strong key management, and regulatory-grade immutability within a logically and operationally isolated cyber vault that uses independent identity, network isolation, and an automated, policy-driven air gap with separated data and control paths. Within this vault, CyberSense provides the deep, full-content integrity analytics advocated in the whitepaper, inspecting the actual contents of files, databases, and other workloads for corruption, stealthy or "low-and-slow" encryption, and other malicious manipulation to identify a truly clean copy and last known-good backup set for recovery, going beyond simple metadata-based anomaly detection.

Beyond delivering this isolated, immutable, and intelligent data vault with Dell PowerProtect Cyber Recovery, Dell Technologies Services extend the solution with Services for Cyber Recovery plus Incident Response and Recovery Services and the Incident Recovery Retainer Service, bringing a global team of industry-certified cybersecurity experts to help contain attacks and then rebuild, restore, and redeploy even complex, vendor-agnostic infrastructure, data, and applications end-to-end. These services can be consumed proactively as a retainer or engaged at time of crisis, ensuring that recovery runbooks, clean-room testing, and orchestration are already aligned to business priorities when an event occurs. Having deployed thousands of cyber recovery vaults and guided customers through some of the most destructive ransomware and data-wiping incidents, Dell applies proven methodologies, automation, and best practices to accelerate time to business recovery—not just data restore—creating a key differentiator versus typical backup product vendors who generally stop at restoring data and do not provide the same level of end-to-end support across forensics, infrastructure rebuild, and secure return to production. Together, Dell PowerProtect Cyber Recovery, CyberSense, and Dell's cyber recovery and incident response services operationalize the architectural patterns in this paper—secure protection, isolated vaulting, content-aware integrity analysis, and expert-led response—into a cohesive last line of defense that materially strengthens cyber resiliency and confidence in clean cyber recovery.

Cyber Security Association of India (CSAI)

The **Cyber Security Association of India (CSAI)** is a trusted, not-for-profit industry association focused on strengthening cyber resilience, governance, and risk oversight across Indian enterprises and institutions. As cyber threats increasingly impact business continuity, regulatory compliance, and organisational reputation, CSAI provides a strategic platform for leadership-level engagement on cybersecurity.

CSAI enables CXOs, board members, and senior executives to view cybersecurity as a business and governance imperative rather than a purely technical issue.

Why CSAI for Leadership

- Helps boards and CXOs understand cyber risk in business terms
- Provides sector-specific insights aligned with Indian regulations
- Facilitates peer-level dialogue and experience sharing
- Supports informed decision-making on cybersecurity investments
- Acts as a bridge between regulatory expectations and enterprise execution

Strategic Objectives

- Enhance board-level visibility and accountability for cyber risk
- Support cyber resilience, crisis preparedness, and response readiness
- Enable executive dialogue across regulated and critical sectors
- Contribute industry perspectives to policy and regulatory discussions

Value to CXOs

- Closed-door CXO and CISO roundtables
- Insights on BFSI, critical infrastructure, and regulated sector risks
- Thought leadership on cyber resilience, governance, and digital trust
- Engagement with policymakers, regulators, and domain experts

Alignment with Regulatory & National Priorities

CSAI supports executive leadership by contextualising cybersecurity within:

- BFSI regulatory expectations for cyber risk, resilience, and governance
- National critical infrastructure protection priorities
- Data protection obligations, breach preparedness, and accountability
- CERT-In driven incident reporting, readiness, and coordination
- National cybersecurity strategies and digital trust initiatives.

Acknowledgements

Cyber Security Association of India (CSAI)

- **Lt. Gen. (Dr) Rajesh Pant,** Former National Cyber Security Coordinator, PMO, Chairman CSAI
- **Sh. MAKP Singh**, Vice Chairman, CSAI and former CISO, Ministry of Power
- **Prof. NK Goyal,** President Cyber Security Association of India/ CMAI
- **Sh. Vijayant Gaur**, Director General, CSAI
- **Sh. Sanjeev Khanna**, Advisor, CSAI, Maharashtra Chapter

Dell Technologies

- **Sh. Venkat Sitaram,** Sr Director & GM, Infrastructure solutions, Dell Technologies India
- **Sh. Nitin Bhatia,** Data Protection Specialist, Dell Technologies India
- **Sh. Adesh Manjrekar,** Specialist- Security and Resilience Platform Dell Technologies India