

# THE EVOLVING ROLE OF THE CISO

**Transformation from  
Technician to Strategic Leader  
with Growing Accountability  
but Limited Authority**



**Amit Basu**

Vice President, CIO & CISO  
International Seaways

New York

[linkedin.com/in/amitbasu](https://www.linkedin.com/in/amitbasu)



ORIGINAL CISO IN 1995

CURRENT CISO

?

# ROLE BORN IN THE SHADOWS, NOW CENTRAL TO THE ENTERPRISE

## Evolution of the CISO Role

The Chief Information Security Officer's role has evolved from a technical position to a strategic boardroom presence in 30 Years

## Digital Risk Landscape

As digital risks increase, the CISO is critical in ensuring the enterprise's data and reputation are protected.

## Centrality of Trust

The CISO's role emphasizes the importance of trust in the digital economy, safeguarding not only data but customer confidence.

## Enhanced Accountability

CISOs today face significantly increased accountability, with growing expectations from boards and regulators, often without enough authority



# ORIGINAL CISO IN 1995 – THE SHADOWY TECHNICIAN



1995–2005:  
  
THE  
TECHNICAL  
GUARDIAN

# BIRTH OF THE CISO ROLE

## Emergence of the CISO Role

The CISO role was created to address growing cybersecurity threats to the Banks in the 90s.

## The Citibank Cyberattack

In 1994, a significant cyberattack on Citibank highlighted vulnerabilities in financial institutions and sparked the need for dedicated security leadership.

## First Appointed CISO

Steve Katz became the first CISO at Citibank, representing a major shift in how organizations approached cybersecurity management.





# FOCUS ON PERIMETER DEFENSE AND INCIDENT RESPONSE



## **Perimeter Fortification**

Cybersecurity during this era was primarily focused on establishing strong perimeter defenses to protect network boundaries.

## **CISO Roles and Responsibilities**

CISOs, mainly from IT backgrounds, were responsible for implementing firewalls, antivirus tools, and reactive incident response strategies.

## **Reactive Incident Response**

The focus was largely on reactive measures to incidents rather than proactive strategies to prevent breaches.

## **Business Relevance of Cybersecurity**

Although critical, the business relevance of cybersecurity was not well understood, leading to CISOs operating in the shadows.



# 2005–2015: THE COMPLIANCE ENABLER



# EXPANSION OF DIGITAL FOOTPRINT AND REGULATORY SCRUTINY

## **Digital Footprint Expansion**

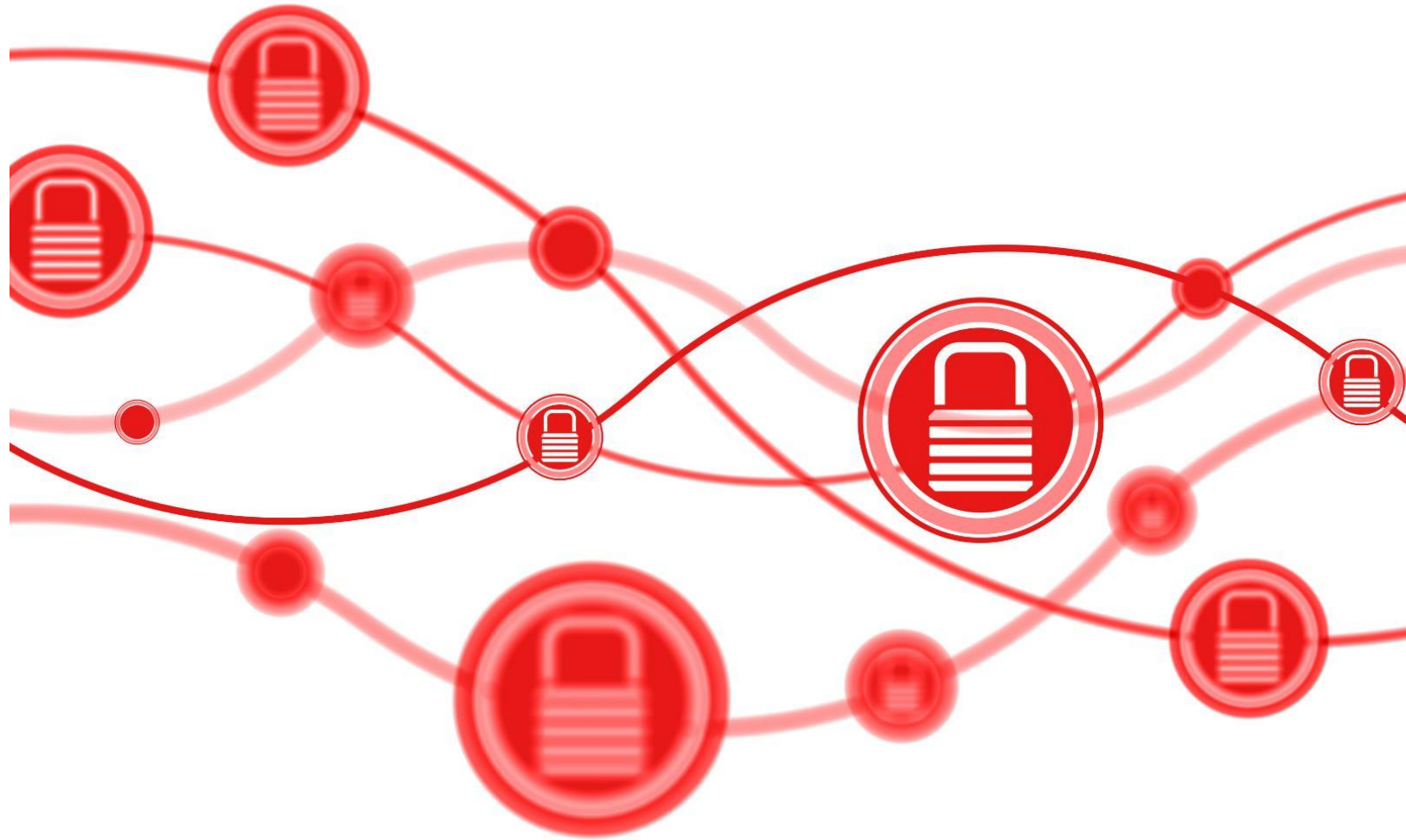
The digital footprint of organizations grew significantly, leading to increased visibility and data exposure in the digital landscape.

## **Regulatory Scrutiny Increase**

With the rise of digital operations, regulatory scrutiny intensified, highlighting the need for compliance in cybersecurity.

## **Cybersecurity Compliance Laws**

Laws such as Sarbanes-Oxley, PCI DSS, and HIPAA established essential compliance standards for organizations to follow.







# ROLE EVOLUTION TO RISK MANAGER

## **Governance Framework Navigation**

CISOs are now expected to navigate complex governance frameworks to align security with business objectives.

## **Business Continuity Planning**

Overseeing business continuity planning is crucial for CISOs to ensure organizational resilience in the face of risks.

## **Collaboration with Legal and Audit**

CISOs collaborate with legal and audit teams to ensure compliance and mitigate risks effectively.

## **Perception as Inhibitors**

Despite evolving into risk managers, CISOs are often perceived as obstacles to speed and innovation.





2015–2020:

THE  
BUSINESS  
RISK  
ADVISOR



# IMPACT OF HIGH-PROFILE DATA BREACHES

## **High-Impact Data Breaches**

High-profile data breaches like Target and Equifax highlighted vulnerabilities in corporate cybersecurity, raising awareness at the board level.

## **Cybersecurity as a Priority**

The frequency of data breaches emphasized the importance of cybersecurity, making it a critical issue for company leadership.

## **Emerging Risks from Technology**

The rise of cloud computing and mobile services increased exposure to new risks, demanding continuous adaptation from organizations.



# INTEGRATION OF SECURITY WITH BUSINESS STRATEGY



## **CISO's Role Evolution**

CISOs are now bridging the gap between security measures and overall business strategy, showcasing the importance of cybersecurity in driving business goals.

## **Vendor Oversight**

CISOs play a vital role in vendor oversight, ensuring that third-party partnerships align with the organization's security objectives.

## **Translating Risk to Impact**

CISOs are now translating technical risks into business impacts, making security a key part of strategic discussions at the board level.

## **Security as a Business Enabler**

Security is emerging as a critical business enabler, facilitating digital transformation and automation rather than serving as an obstacle.

# 2020–2025: THE STRATEGIC PARTNER





# ACCELERATION OF DIGITAL TRANSFORMATION AND SOPHISTICATED THREATS

## Impact of COVID-19

The COVID-19 pandemic significantly accelerated digital transformation, leading to widespread remote work and increased reliance on technology and also enhanced opportunities for cyber criminals.

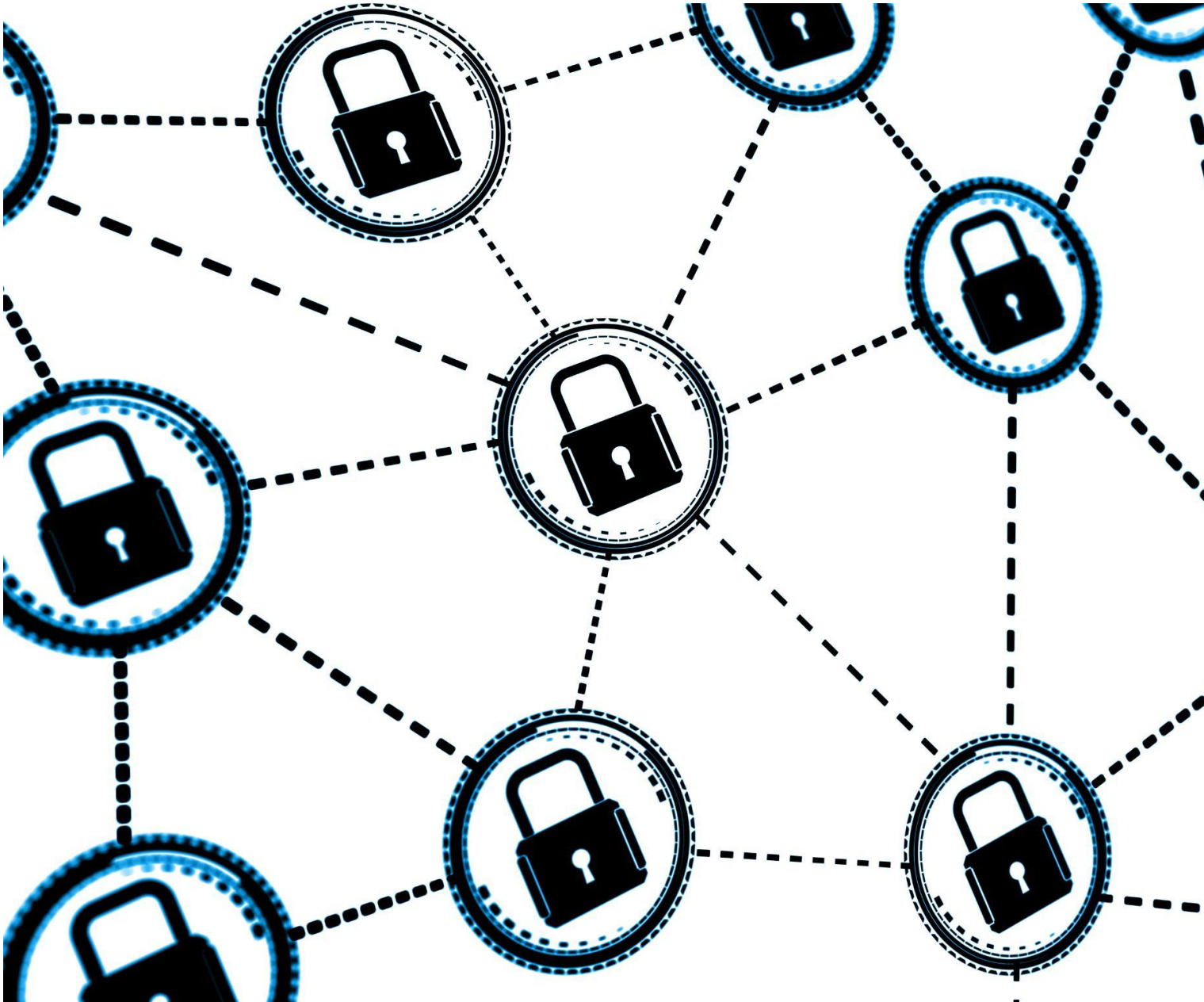
## AI Adoption

Organizations adopted AI technologies to enhance efficiency, streamline processes, and improve decision-making during the transformation period.

## Sophisticated Threats

As digital transformation progressed, cyber threats became more sophisticated, leading to a surge in ransomware attacks and enhanced security concerns.





# OVERSIGHT OF ENTERPRISE-WIDE RISK PORTFOLIOS

## **Enterprise-Wide Risk Management**

CISOs are now responsible for managing a comprehensive portfolio of risks that encompass various aspects like data privacy and supply chain vulnerabilities.

## **Cybersecurity Frameworks**

Standard frameworks like Zero Trust, NIST CSF, and MITRE ATT&CK are now essential for effective cybersecurity strategies in organizations.

## **Role of Today's CISO**

Today's CISO plays a crucial role in advising on cyber resilience, risk appetite, and ensuring business continuity strategies are in place.



FROM  
DEFENDER TO  
EMPOWER:

THE CISO AS  
CHANGE  
AGENT



# ENABLING INNOVATION AND SECURE-BY-DESIGN SYSTEMS

## **CISO as Change Agent**

Modern CISOs are no longer just defenders; they are change agents driving innovation within their organizations.

## **Secure-by-Design Systems**

Building secure-by-design systems is essential for fostering trust and enabling innovation across digital platforms.

## **Cultivating Cyber Awareness**

Fostering a culture of cyber awareness empowers employees to recognize and respond to security threats effectively.

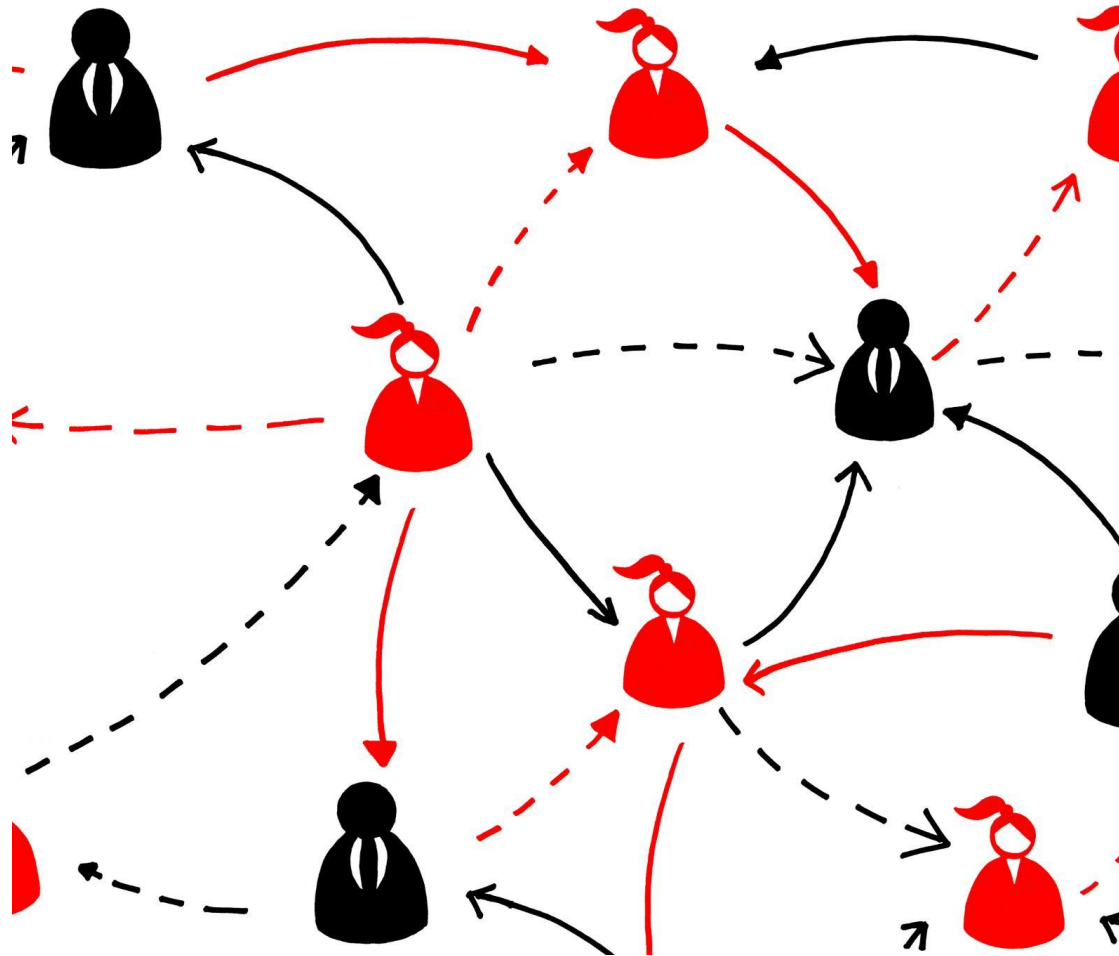
## **Translating Technical Complexities**

CISOs play a key role in translating complex technical information into business-friendly terms for stakeholders.





# STRATEGIC VISION, DIPLOMACY, AND RESILIENCE



## **Strategic Foresight**

CISOs must develop the ability to anticipate future challenges and opportunities, ensuring their organizations remain competitive.

## **Cross-Functional Diplomacy**

Effective collaboration with other departments is essential for a CISO to navigate complex organizational dynamics and foster cooperation.

## **Emotional Intelligence**

CISOs must cultivate emotional intelligence to manage relationships and understand the needs of their teams and stakeholders.

## **Guiding Resilience and Growth**

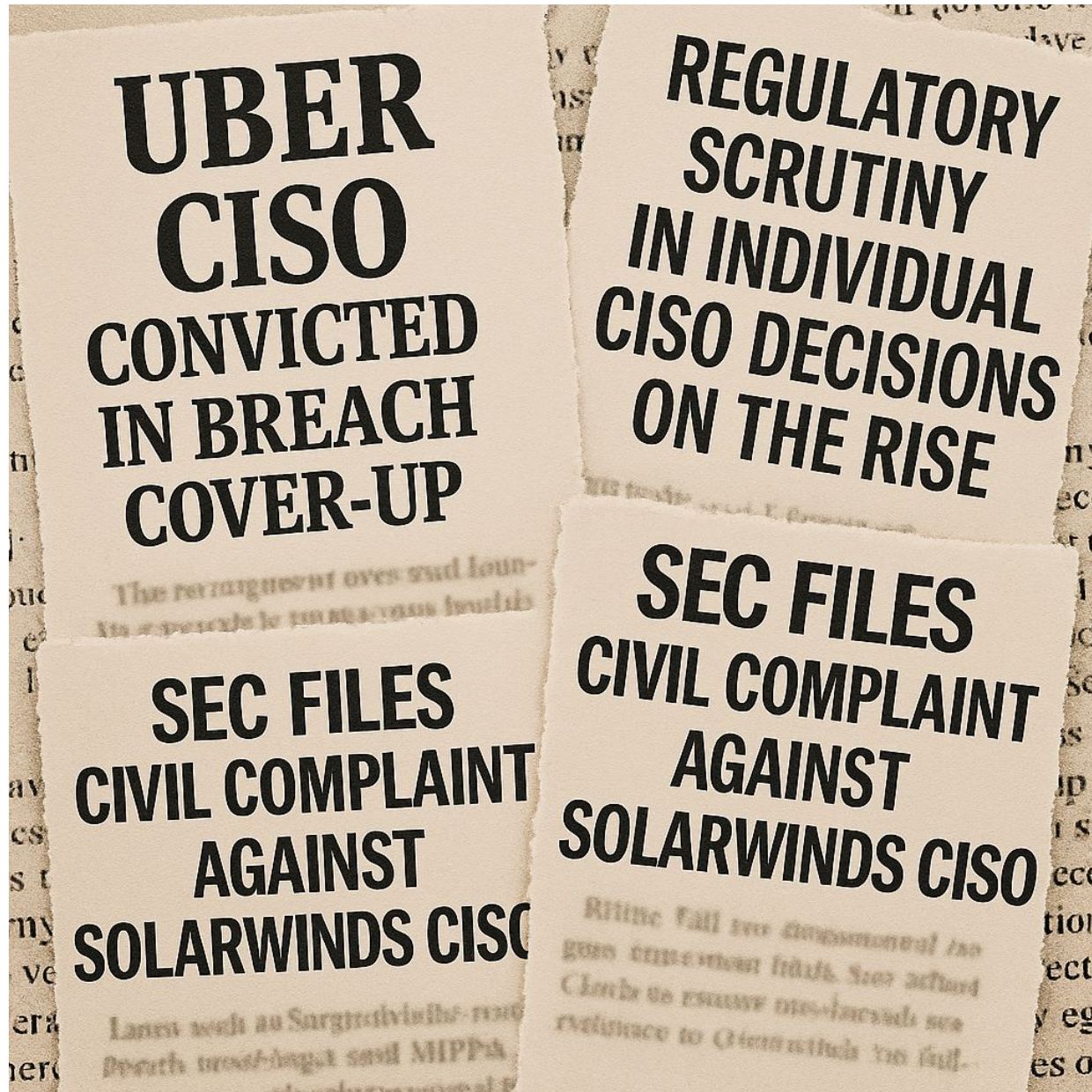
CISOs are now viewed as key players in guiding organizations toward sustainable growth and resilience against emerging threats.



ACCOUNTABILITY  
ERA:

THE CISO  
ACCOUNTABILITY  
PARADOX





## THE PERSONAL COST OF DEFENDING THE ENTERPRISE

### Legal and Criminal Liability

Risk of being held personally accountable even when acting under corporate directive.

### Regulatory Scrutiny

Increasing focus by regulators on individual decision-making (not just organizational failures).

### Reputational Damage

Media narratives often highlight systemic failures with individual fault permanently damaging a CISO's credibility.

### Job Insecurity and Role Ambiguity

Lack of clear cybersecurity accountability without full decision-making authority, yet full responsibility.

### Mental and Emotional Strain

Continuous high-stakes pressure, especially during or after incidents.

### Contractual Gaps and Indemnity Limitations

Not all CISOs are protected by D&O insurance or indemnity clauses.

# THREE QUESTIONS EVERY BOARD SHOULD ASK TODAY



Does our CISO have clearly defined authority and escalation rights?

Is our D&O insurance explicitly extended to cybersecurity leadership?

Have we endorsed a professional framework to reduce liability exposure and elevate credibility?

A CISO without protection is a vulnerability



# WHAT CISOS NEED NOW

- Accreditation of the role
- Peer support network
- Indemnification coverage
- Training and continuing education

**Are we ready to protect those who protect the enterprise?**

A professional community advancing the credibility, capability, and protection of today's cybersecurity leaders.



**PROFESSIONAL  
ASSOCIATION  
OF CISOS**

[theciso.org](https://theciso.org)