Deloitte.

*Together makes progress*

# The board's playbook for cyber resilience

# *A note to the CISO*

As a chief information security officer (CISO), one of your most important tasks is bridging the gap between technical complexity and strategy. Communicating the importance of cyber resilience to your board is key to securing the alignment and investment needed to protect the organization. This guide has been specifically crafted to help you in that effort. Written for a board-level audience, it translates core concepts of resilience into the language of business impact, strategic oversight, and governance. We encourage you to share this with your board members to facilitate a more informed and productive dialogue about your collective responsibility in building a resilient enterprise.

## Turning disruption into ***opportunity***

Cyber disruptions are happening with increasing frequency and, as a leader, your role is to steer your organization through uncertainty and ensure long-term viability. Cyber resilience has evolved from a technical concern to a fundamental pillar of business strategy. It is the bedrock upon which organizations build trust, protect enterprise value, and drive sustainable growth. This guide is designed to provide you with a clear, strategic overview of **cyber resilience—what it means, why it matters now more than ever, and the pivotal role you play in governing it effectively.**

## Risk versus resilience: ***A strategic distinction***

It is crucial to understand the difference between traditional risk management and a modern resilience-focused strategy. Risk management is about identifying and mitigating known vulnerabilities. Resilience, however, is about building the capacity to withstand and recover quickly from unexpected incidents. Traditional risk-based approaches are often bound by what can be anticipated. An end-to-end resilience strategy prepares organizations for the unimagined.

## Why ***resilience*** matters now

The landscape of risk has fundamentally shifted. There is a convergence of factors making resilience an urgent priority:

- **Regulatory pressure:** New regulations—such as the **Digital Operational Resilience Act (DORA)** in Europe and enhanced **Securities and Exchange Commission (SEC)** reporting requirements in the US—are elevating operational resilience from a leading practice to a regulatory mandate. These are no longer just guidelines. They’re requirements that carry the potential for significant penalties for noncompliance.
- **Real-world lessons:** Recent high-profile cyber events serve as reminders of the potential for massive financial, operational, and reputational damage. These incidents demonstrate that no organization is immune.

**Customer expectations:** Your customers and partners trust you with their data. That trust is fragile. A failure in resilience can lead to a significant loss of confidence and, consequently, a loss of business.

## The board’s role in ***cyber resilience***

As a board member, you hold ultimate accountability for the oversight of your organization’s operational resilience. Your role is not to manage the technical details but to govern the strategy and ensure the organization is prepared. Recommended actions include:

- Regularly reviewing and challenging the organization’s resilience plans, policies, and associated metrics.
- Scrutinizing and approving spending in support of resilience, ensuring resources are allocated to the most critical areas.
- Building awareness of the most likely and high-impact cyber scenarios to understand the potential business consequences and the plans in place for recovery.

# *Five questions* board members should ask

To guide oversight, you can focus your discussions with management around these five fundamental questions:

1. ***What will be impacted?***
   - Identify critical business services.
   - Map operational dependencies such as staff and third-party systems.
2. ***Where do you need to focus?***
   - Determine priorities based on financial impact, organizational viability, and potential harm to the customers or market.
3. ***How long can you go without the service?***
   - Understand and define plausible  outage scenarios.
   - Create impact tolerance statements for each critical business service.
4. ***How do you address the problem?***
   - Establish connection between incident response, recovery, continuity planning, and crisis management.
5. ***How do you plan for the future?***
   - Build test scenarios and contingency plans.
   - Identify areas of enhancement and invest to address gaps.

# *Core implementation* areas

| | | |
|---|---|---|
| Determine critical business services | **What will be impacted?** | • Shift the focus from business processes to business services<br>• Identify critical business services<br>• Map supporting operational dependencies:<br>– staff<br>– third parties<br>– systems |
| Assess relative impact importance | **Where do you need to focus?** | • Evaluat operational disruption based on three impact categories:<br>– Financial stability<br>– Organizational viability<br>– Harm to customer/other market participant<br>• Establish criteria/process to assess criticality & single points of failure<br>• Determine priorities for immediate focus |
| Define plausible disruption scenarios and tolerances | **How long can you go without the service?** | • Understand and define plausible scenarios for outages and long-term disruptions<br>• Set impact tolerance statements for each critical business service and take action in order to remain within established thresholds<br>• Obtain senior and/or board-level approval to impact tolerances |
| Harmonize response and communication | **How do you address the problem?** | • Establish connection between incident response, recovery, continuity planning, and crisis management<br>• Indicate alternate services and redressal arrangements<br>• Establish training & education plans and mediums for the stakeholders |
| Testing, measuring and improving resilience | **How do you plan for the future?** | • Define and establish objective success criteria<br>• Build test scenarios and contingency plans<br>• Identify gaps, single point of failure and areas of enhancement<br>• Invest to address gaps |

**Anticipate and assess** > **Plan and prepare** > **Protect and control** > **Respond and recover**

## *Targeted metrics* at a glance

To effectively monitor the organization’s posture, the board should receive regular reporting on a select set of metrics:

- **Risk exposure and posture:** An aggregate risk score and a summary of top risks identified and treated.
- **Incidents and threats**: The number of confirmed security incidents and the time it takes to detect and respond.
- **Compliance and regulatory alignment:** The status of compliance with regulations such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), etc.
- **Resilience and preparedness:** The frequency and outcomes of incident response drills and simulations.
- **Investment and resource allocation:** A clear view of cybersecurity spending versus the budget and any critical staffing gaps.
- **Third-party and supply chain risk:** Coverage of third-party security assessments and the number of incidents originating from outside the organization

## Next steps *for the board*

Resilience is a continuous journey, not a destination. Your ongoing engagement is critical. In the near term, the board should receive quarterly updates on resilience efforts and stay informed of assessment and simulation outcomes. For the longer term, prioritizing investments in cutting-edge technologies, such as cyber vaults, can help you further strengthen your overall resilience plan. By fostering a culture of preparedness from the top, you can help ensure the organization is ready to adapt and thrive in an ever-changing environment.

# Get in touch

**Sharon Chand**
Principal
Cyber Defense & Resilience Leader
Deloitte & Touche LLP
+1 773 294 6430
shchand@deloitte.com

**Mike Kosonog**
Partner
Cyber Resilience Market Offering Leader
Deloitte & Touche LLP
+1 313 396 3622
mkosonog@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.