Deloitte.

Together makes progress

CYBER DEFENSE & RESILIENCE

Boardroom Resilience: Leading through disruption

Contents

A note *to the CISO*

This guide provides a strategic framework for the board to actively guide the organization's resilience efforts in an increasingly disruptive world.

By passing this along, you can help align the board on a proactive resilience strategy, facilitate more strategic investment conversations, and solidify their understanding of the critical role cybersecurity plays in the organization's ability to not just survive, but thrive through disruption.

The new reality: Disruption as the norm

Cyber is facing a new age of security threats. As cybercrime grows more advanced, it's no longer an option to assume security. Disruption has become the new normal. For the board, the mandate is clear: Lead the charge in fostering a culture where resilience is not an IT issue, but a core business imperative.

By conducting rigorous readiness assessments, enhancing governance, and relentlessly asking the critical questions, the board can create an organization that is prepared not only to weather the next storm but to emerge from it stronger, with customer trust and business continuity intact.

Key disruption drivers

AI-amplified fraud

AI enables more scalable reconnaissance, faster exploit development, and highly convincing social engineering and deepfake impersonation, which can lead to increased compromise rates and response complexity.

Additionally, attacker dwell times are decreasing from weeks or days to mere hours. The time from initial access to enterprise-wide impact is shorter than ever. This puts immense pressure on detection and response capabilities.

The crypto horizon risk

Nation-state actors and sophisticated criminal groups are actively exfiltrating massive volumes of encrypted data. While they may not have the computational power to break current encryption standards, many are stockpiling this data with the expectation that future advancements—particularly in quantum computing—will render current cryptography obsolete.

This means the most sensitive long-term data—intellectual property, strategic plans, and state secrets—is at risk of future exposure, even if it is securely encrypted by today's standards. It's critical to begin inventorying sensitive data, evaluating its long-term risk, and developing a roadmap for transitioning to post-quantum cryptography (PQC) to help mitigate this future threat.

Third-party supply chain fragility

A significant pattern in major cyber incidents is developing where the initial point of compromise is an upstream provider. These aren't isolated events; they're creating cascading failures that result in widespread outages and breaches downstream.

A major contributing factor is concentration risk. Reliance on a handful of dominant software-as-service (SaaS) and shared-service platforms means that a single point of failure in one of their environments can translate into a systemic, enterprise-wide event.

The core of the problem is a critical effectiveness gap in third-party risk management (TPRM) programs. For many organizations, existing questionnaires and annual reviews are failing to provide the timely, actionable intelligence needed.

Accelerating regulatory scrutiny

The regulatory landscape is moving from a post-incident compliance exercise to a real-time demand during the incident itself. The burden of proof is shifting. Regulations like the European Union's Cyber Resilience Act, which comes into effect in September 2026, are part of a larger trend.

It's no longer enough to simply have controls. Instead, organizations are expected to demonstrate their continuous effectiveness on demand, even under the duress of an active investigation.

Practical implication for boards

These disruptions mean resilience conversations should move from "are we secure?" to "what's our time-to-detect/contain/recover for crown-jewel services, and what third-party or cloud dependencies can break that?"

What boardroom resilience *truly means*

Boardroom resilience is the organization's ability to keep critical customer and business services running—or restore them within agreed time frames—despite cyber incidents, third-party failures, and other major disruptions, with transparent governance and controlled impact.

Core outcomes of a resilient enterprise

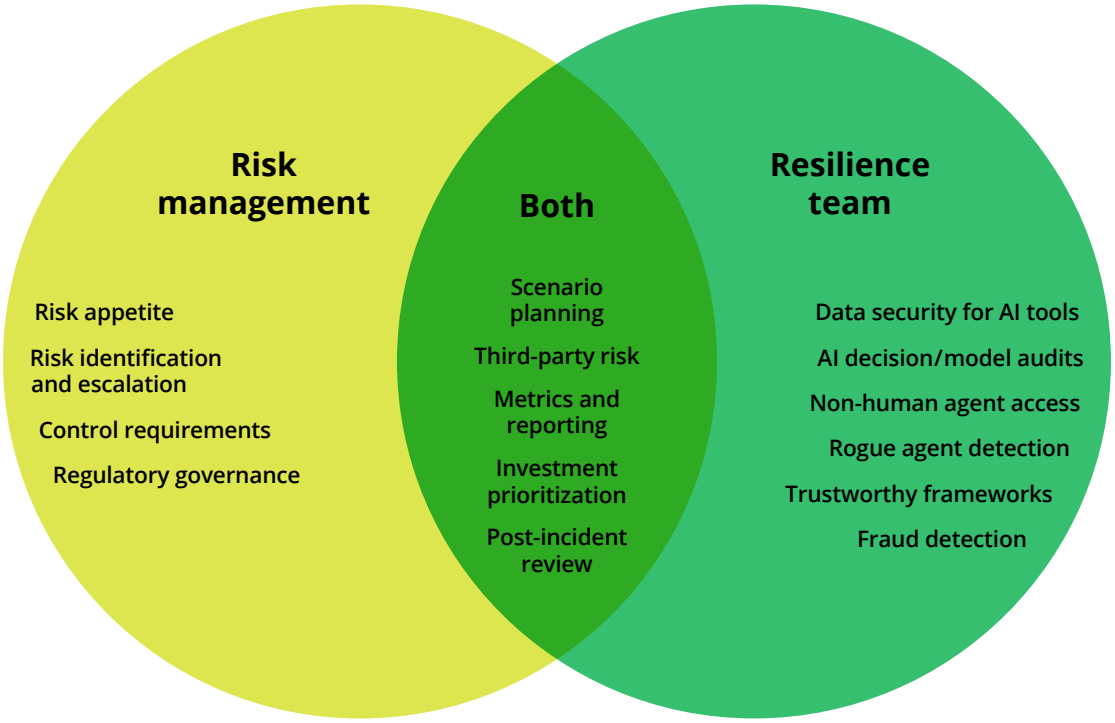
- **Protect customers and sensitive data:** Limit harm and prevent issue spread.
- **Maintain minimum viable company:** Keep highest-priority products/processes operating at minimum viable levels.
- **Recover essential technology:** Accelerate the restoration of essential systems and prioritize critical business services to minimize disruption.
- **Make fast, governed decisions:** Activate clear incident command, escalate appropriately, and document choices.
- **Learn and reduce recurrence:** Complete root-cause fixes and validate control improvements.

Risk management vs. resilience

Although risk management and resilience both affect the security of the enterprise, they play different roles.

RISK MANAGEMENT	RESILIENCE
Defines what level of disruption and loss is acceptable and facilitates governance	How the organization can continue critical outcomes and recover with that tolerance when disruption happens

Figure 1. **Risk management vs. resilience and where the two overlap**



Who owns resilience?

A leading practice for end-to-end cyber resilience calls for one executive accountable with clear decision rights, plus shared execution responsibility across IT, security, operations, legal, and communications.

In most organizations, the COO or CIO is accountable for operational resilience (keeping critical services running and recoverable), with the CISO accountable for cyber risk management (threat, control standards, security monitoring/response capability).

Figure 2. **Resilience ownership hierarchy**

The board: Ultimate oversight; approves risk appetite and receives material incident reporting

CEO: Ultimate oversight; approves risk appetite and receives material incident reporting

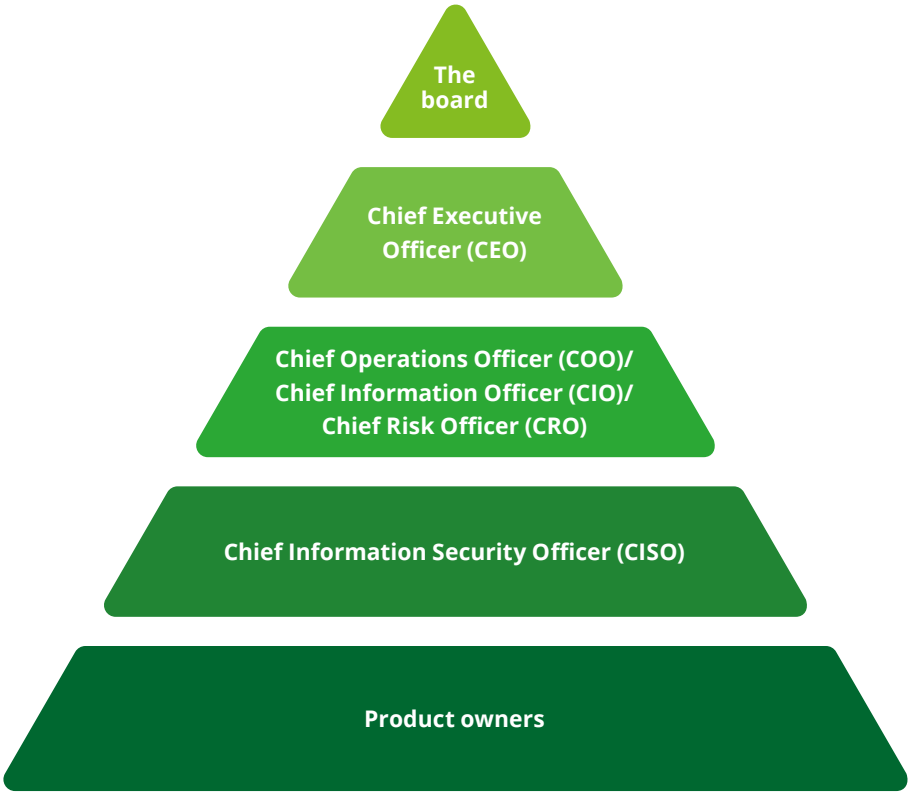
COO: Responsible for resilience across business operations, plants, call centers, etc.

CIO: Responsible for resilience across digital and technology operations

CRO: Responsible for the enterprise-wide risk management framework that governs resilience policy and investment

CISO: Accountable for the cyber program and a key decision-maker during incidents

Product owners: Accountable for critical service resilience outcomes, customer impact, prioritization, and risk acceptance for their services



Creating a cyber-resilient culture

A cyber-resilient culture is defined less by awareness and more by consistent behaviors that reduce likelihood and impact of incidents—especially under pressure.

The hallmark is a team that can anticipate, prevent, detect, respond, and recover as a normal way of working.

Cultural litmus test

Ask your team this one question: When a deadline is at risk, do we skip controls or do we adapt safely?

If the answer prioritizes speed over safety, you may need to revisit the core behaviors of resiliency culture.

Core behaviors to foster

- **Leaders model trade-offs:** Executives transparently make and document security versus speed decisions, rather than treating security as an afterthought.
- **Psychological safety for reporting:** Employees report mistakes, suspicious activity, and near misses early and without fear.
- **Clear and local accountability:** Systems have named owners; teams know their crown jewels, dependencies, and recovery objectives.
- **Resilient-by-default:** Teams build and operate using approved, tested patterns that ensure services can withstand disruption.
- **Relentless hygiene habits:** Timely patching, account removal, access reviews, and strong secrets management are ongoing operations.
- **Resilience muscle memory:** Regular incident drills, restore tests, and playbook use ensure people know roles and escalation paths.
- **Learning after events:** Post-incident reviews focus on root causes and system fixes, not blame.
- **Third-party responsibility mindset:** Teams actively evaluate vendor risk, demand evidence, and plan contingencies.
- **Data stewardship:** Employees minimize data collection, classify data correctly, and challenge unnecessary access, treating privacy and security as trust commitments.
- **Measurement drives behavior:** Metrics emphasize risk reduction outcomes (e.g., time-to-remediate, restore success).
- **Deliberate focus:** Driving a purposeful focus on essential services and the highest impact scenarios to enable meaningful progress across an ever-expanding resilient landscape.

Steps the board can take

The steps below provide a framework for creating resiliency, enabling the board to effectively manage risk, ensure timely and transparent disclosure, and foster a culture of security that permeates every level of the organization.

STEP 1

Conduct a readiness assessment

- Design disclosure controls and procedures to elevate cyber incidents to the appropriate individuals to determine incident materiality in a timely manner.
- Confirm that those making the disclosures have controls that allow for complete and accurate disclosure of all material information.
- Validate operational preparedness across select cyber capabilities (e.g., incident response, risk management, governance, reporting).

STEP 2

Evolve cyber incident response and recovery capabilities

- Define a process for assessing materiality criteria and embed in incident response process.
- Continue to meet disclosure obligations as incidents evolve.
- Clearly communicate the threat and impact implications through defined reporting channels.
- Confirm ability to recover essential services and technology from a destructive cyber attack.

STEP 3

Apply stakeholder coordination and orchestration processes

- Engage with legal counsel prior to disclosure.
- Facilitate timely and appropriate disclosures.
- Develop accountability for compliance and disclosure.
- Provide consistent disclosures with transparency.
- Policies should be specific, and employees should be educated on how to apply them.

STEP 4

Enhance the cybersecurity governance framework

- Strengthen governance by educating the board and management.
- Foster a culture of responsibility and accountability.
- Implement operating models for risk management.
- Identify board committee or subcommittee responsible for cybersecurity oversight and how often they will be updated on cybersecurity risks.

STEP 5

Enhance third party oversight and procedures

- Establish third party governance and operating models including inventory and risk classification of third parties.
- Perform pre and post contract oversight, including contractual clauses on material incident reporting.
- Establish two way communication channels to enable reporting and information sharing.

Resources for the board

Effective board oversight requires specific, actionable information and a clear understanding of key questions. It's critical that they are armed with the documents and information needed to make timely decisions.

Top 10 questions the board should ask:

1. What is the organization's cyber risk appetite or tolerance? What levers do we have to manage it?
2. What is the overall cyber strategy and plan for protecting assets? What are the crown jewels that we must protect, including data and other assets?
3. What is management's rationale for investing and allocating resources to monitor cyber risk, guard against it, and expedite response and recovery?
4. Do we have trained and experienced staff who can forecast cyber risks?
5. Do we know the board and relevant committee roles and responsibilities in various situations?
6. Assuming we do have a ransomware attack, breach or incident, are we prepared to operate through it? Can we recover essential services and technologies?
7. How are critical infrastructure and regulatory requirements met?
8. What controls are in place to monitor cloud and supplier networks, as well as software running on company devices, such as mobile devices?
9. How are vulnerabilities identified and disclosed? How do frontier AI models change these processes?
10. What metrics do we have in place to measure cybersecurity performance, trends and overall risk?

Minimum board materials to request annually:

- Readiness assessment
- Disclosure controls and procedures
- Operational preparedness validation: Evidence across incident response, business continuity, disaster recovery, risk management, governance, and reporting.
- Incident response plan
- Risk register
- Cyber insurance status
- Cyber outcomes and lessons learned from any major incident
- Resilience investment roadmap

Key takeaways for the board

In an era where disruption is the new constant, the focus of boardroom oversight must evolve from traditional cybersecurity defense to a proactive stance of enterprise wide resilience. The escalating sophistication of threats driven by AI, the looming risk of the crypto horizon, fragile supply chains, and intensifying regulatory scrutiny demand more than just robust security controls.

They require a demonstrated capability to withstand and recover from impact. The ultimate goal is to move from a position of vulnerability to one of enduring strength in the face of perpetual change.

Get in touch

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

Pete Renneker
Managing Director
Resilience Market Offering Leader
Deloitte & Touche LLP
+1 513 833 6179
renneker@deloitte.com

Deloitte.