Deloitte.

In association with **Dell Technologies**

WHEN DATA IS AT RISK, WHO'S RESPONSIBLE?

SIX ESSENTIAL CONVERSATIONS TO HELP IMPROVE YOUR CYBER RESILIENCE

As cyber threats increase, so does the scale of disruption an attack can have on an organization. Following a major security incident, Chief Information Security Officers, Chief Technology Officers, and their executive leadership (Boards of Directors and CEOs) may find themselves dealing with more than a public relations issue—they could be held responsible for certain cyber failures that happened on their watch.

But they don't have to go it alone. By bringing teams together and leveraging modern automation, AI, and technology solutions, leaders can shift the focus from triage to triumph with open, honest dialogue about their current cybersecurity posture. This guide explores the critical need for cyber resilience and how Deloitte and Dell Technologies (Dell) can help organizations address challenges and scale their capabilities by focusing on actionable outcomes.

ASSESSING THE THREAT LANDSCAPE

Ransomware attacks rose by

126%

in the first quarter of 2025 with North America accounting for

62%

of global incidents.[1]

Average ransom payment amount of

$1M

in 2025.[2]

Over

25%

of organizations take up to a month to recover.[2]

WHAT'S AT STAKE? REAL-WORLD EXAMPLES WITH REAL-TIME IMPLICATIONS

Cyberattacks can lead to severe financial, reputational, and operational impacts for organizations across sectors and locales.

FINANCIAL LOSSES

Organizations can incur significant costs due to ransom payments, operational downtime, incident response, forensic investigations, and restoring systems data.

REPUTATIONAL DAMAGE

When a data breach occurs and private data is made public, users or the general public may lose trust in the impacted organization, leading to significant reputational harm.

REGULATORY AND LEGAL CONSEQUENCES

Failure to protect data can lead to legal penalties, while victims of data breaches may file lawsuits against affected organizations.

OPERATIONAL DISRUPTION

Encryption of data can disrupt operations, causing productivity losses and service interruptions. Similarly, cyberattacks can cause service interruptions that affect customers and partners.

WHICH THREATS LOOM LARGEST?

Ransomware has evolved from data exfiltration to data encryption and destruction. A common form of ransomware is the **double extortion attack**, where cybercriminals encrypt stolen data, exfiltrate it, then threaten to release the data publicly or sell it on the dark web if the ransom is not paid.

Emerging technologies such as **artificial intelligence (AI)** can help attackers evade traditional security measures, automate attacks, and rapidly adapt techniques. On the flip side, companies should embrace AI for cyber and use it to help tip the scales in their favor. AI capabilities can support the defense and resilience landscape with things like AI-enabled threat hunting and AI-enabled detection. It's about using AI to combat AI.

ANSWERING THE CALL BY BUILDING CYBER RESILIENCE

Given the complexity and interconnected nature of today's systems, even existing capabilities such as disaster recovery or cybersecurity controls may not provide a full solution to protect against every threat. In response, organizations should devise a unified approach to cyber resiliency—one that brings together the right elements and collaborators to prepare for, respond to, and recover from a cyberattack.

Cyber resilience can help mitigate unscripted endings using multiple layers of defense, detection, response, and recovery. This complex initiative spans across functions and departments within an organization. It combines the ability to reduce cyber threats—such as ransomware attacks—with the capabilities to recover impacted systems and limit disruption to the business.

Effectively mitigating risks and responding to incidents requires coordinated efforts from IT, security, compliance, legal, executive leadership, and beyond. No single individual or department possesses the comprehensive experience or resources needed to address all aspects of cyber resilience. Organizations should have a collaborative, enterprise-wide approach rooted in fundamental governance and fiscal responsibility.

To build cyber resilience, organizational leaders should prioritize having six essential conversations designed around key topics.

CONVERSATION ONE

ENGAGE AT THE TOP

01
Set a vision and plan for operational resilience to combat complex organization-wide disruption scenarios like cyberattacks.

02
Align senior leaders on the objectives of the program and demonstrate risk reduction throughout the implementation process. This is vital for sustained support.

03
Senior leaders should champion the initiative, integrating cyber resilience into the organization's broader strategic goals.

C-SUITE ROLL CALL: ASKING THE RIGHT PEOPLE THE RIGHT QUESTIONS.

When a security incident occurs, it impacts the entire organization. Communication teams manage the narrative, operations handles customer service, and IT resolves technical issues. By discussing relevant questions, business leaders can contribute their individual perspectives and insights for a broad and unified approach to safeguarding against cyber threats.

ROLE	QUESTIONS	
Board of Directors	• How would a cyberattack impact our business and operations? • How confident are we in our ability to respond and recover? • Are we investing adequately in cyber resilience?	• What is our current cyber risk exposure and how are we managing it? • Do we have a dedicated cybersecurity committee or advisor on the board?
Chief Executive Officer (CEO)	• What is our level of operational resilience to ransomware attacks? • Who on the executive team is directly accountable for driving cyber resilience? • How robust is our business continuity plan?	• How does our resilience strategy align with our business strategy? • Have we established a culture of resilience? • How frequently do we review and update our cyber resilience plans?
Chief Operating Officer (COO)	• Have we identified and prioritized our most critical business services? • What must be true to operate those business services without underlying technology? • Have we defined our "minimum viable company (MVC)" parameters?	• How would we maintain operations if we experienced a sudden loss of underlying technologies? • How well do we manage cyber risks posed by vendors and third parties?
Chief Information Officer (CIO)	• How resilient are the organization's essential technologies to ransomware attacks? • What is our plan to recover applications, infrastructure, and technology underpinning critical business services?	• How do we promote cloud service security and resilience? • How do we handle the security and resilience of remote and hybrid work environments?

ROLE	QUESTIONS	
Chief Risk Officer (CRO)	• How resilient are our core operations to destructive cyberattacks? • How confident are we in restoring data and systems after an attack? • How do we assess and quantify the business impacts of cyberattacks?	• How are we integrating cyber resilience into our broader risk management framework?
Chief Information Security Officer (CISO)	• Do we have visibility into the level of protection for our critical business assets? • How quickly can we identify, contain, and remediate threats targeting these critical assets? • How aligned are our threat detection and response capabilities with our resilience strategies?	• How do we coordinate across legal, IT, communications, and executive teams during cyberattacks? • Is our organization prepared for a potential prolonged system outage caused by cyberattack? • How effective are we in educating business stakeholders on cyber threats?
Chief Legal and Compliance Officer (CLO)	• How do we maintain compliance with evolving cyber resilience regulations? • Who is responsible for cyber crisis decision making within the organization? • How are legal privilege and confidentiality maintained during cyber incidents?	• Are our customer, partner, and third-party contracts updated to include incident notification, liability sharing, and cyber responsibilities? • How do we report data breaches to authorities and affected individuals?

CONVERSATION TWO

UNDERSTAND YOUR CURRENT STATE

01
Analyze organizational readiness across business, technology, and cyber operations and explore potential impact of a ransomware attack.

02
Assess business survival needs and identify recovery capabilities as foundational steps in developing a cyber resilience strategy.

03
Conduct thorough preparedness assessments that can reveal current state vulnerabilities and areas needing improvement.

BUILDING A RESILIENT DEFENSE THROUGH TACTICS AND FRAMEWORKS

Ransomware threats are able to thrive because they can slip through the cracks. When security controls fail, traditional backups may be at risk since threat actors frequently target backups before the live environment. And if they survive, using them for recovery can reintroduce malware or corruption unless steps are taken to validate data integrity.

Deloitte's Ransomware Preparedness Framework accelerates exposure insights by helping organizations understand how an attack unfolds and how prepared they are to handle it. Key to the framework is an initial set of principles:

OBSTRUCT DELIVERY
Establish a first line of defense against attacks launched on the organization.

IMPEDE EXECUTION
Detect and stop malicious activities and code that has been deployed within the organization.

RESTRICT MOVEMENT
Limit the ability of threat actors to move laterally within networks.

ACT QUICKLY
Accelerate investigative and response activities across the enterprise.

RECOVER EFFECTIVELY
Deploy advanced technologies and AI-driven recovery automation designed to efficiently restore operations after an attack.

The Ransomware Preparedness Assessment accelerates remediation efforts by leveraging Deloitte's experience in ransomware response and recovery, as well as guidance from industry-leading frameworks. The approach includes four phases:

01 DISCOVER
Gather information on current state, threats, vulnerabilities, goals, and initiatives.

02 ASSESS CYBER READINESS AND RESPONSE
Review security posture and ransomware training and awareness.

03 ASSESS BUSINESS AND TECHNICAL RECOVERY
Assess impact of cyberattacks on essential services and recovery capability.

04 REPORT AND INFORM
Conduct a workshop to raise awareness, share findings, discuss risk mitigation, and develop a roadmap.

CONVERSATION THREE

IDENTIFY THE HEART OF THE BUSINESS

01
Identify services necessary for the organization's survival; focus on protecting these rather than every bit and byte.

02
Map essential services to define a "minimum viable company" operating environment—only the functions and services that *must* remain operational to run the business.

03
Establish the business recovery requirements necessary for maintaining operational continuity.

DETERMINING YOUR "HEARTBEAT"

Determining which business functions are essential to operational continuity is a key step in cyber defense, and the answer varies across industries. For example, financial services organizations will need to continue processing transactions and provide access to online banking, while health care facilities need uninterrupted patient care services and access to electronic medical records systems. Manufacturers must keep production line operations and supply chain management running.

What exactly is the "heartbeat" of your organization? It's the critical business services that need to continue with minimal interruption and should therefore be at the top of your list for risk mitigation. Otherwise, the ongoing viability of the organization would be in jeopardy.

Think of it as the collection of processes, applications, resources, and dependencies required to deliver an end-to-end capability to a customer, supplier, or dependent business function. If affected, these services would significantly impact your reputation or brand, as they are a key aspect of how the company identifies itself.

It takes a collaborative approach between security, infrastructure, business, finance, and operations leaders working together to determine what are the most important assets. Applications and data needed to deliver the operations deemed most essential to the business likely belong in the cyber vault, as they're key to prioritizing recovery.

CYBER VAULTS AND LINES OF "LAST DEFENSE"

A cyber vault is a last resort measure to protect critical applications and data from permanent destruction during an attack. An industry leader such as Dell can equip organizations with capabilities to restore essential business operations after a cyberattack by providing an off-network, protected recovery environment. This environment safeguards data supporting essential business services and requires ongoing maintenance from both business and IT to remain effective.

Cyber vaults also contain core infrastructure services essential for all business operations, including network configurations, backup catalogs, baseline configurations and Domain Name System (DNS). Data related to these services is safeguarded through four mechanisms:

ISOLATION

Control plane isolation (aka "logical air gap") prevents access and blocks any lateral movement into the environment.

SECURITY

Physical and logical protections and insiders who have physical access.

IMMUTABILITY

Protection against corruption,unauthorized changes, or deletion of data.

ANALYSIS

Regular data integrity checks to ensure that data is valid for recovery operations and free from malware and command-and-control artifacts.

UNDERSTANDING THE PURPOSE OF A CYBER VAULT

While cyber vaults are powerful for enabling recovery of applications and data after a severe attack, they do not replace disaster recovery or backup technologies, which continue to enable timely recoveries from non-adversarial disruptions. Cyber vaults also do not guarantee recovery within specific timelines and must also be complemented by a broad, business-led strategy.

CONVERSATION FOUR

DEVELOP A BROAD STRATEGY

01
Build capabilities to detect, respond to, and recover from destructive attacks, supported by appropriate technology.

02
Establish an operating model and governance structure to support maintenance of the solution (essential for long-term resilience).

03
The strategy should encompass all aspects of the organization, so every department understands its role in maintaining cyber resilience.

HOW CAN ORGANIZATIONS RESPOND?

Organizing effectively means bringing the business and technical environments together on the journey of preparing to receive the threat, respond when it occurs, and ultimately recover from it. AI can serve as a force multiplier, enabling organizations to detect, respond to, and recover from cyber incidents with greater speed and precision.

At a tactical level, organizations can consider implementing the following measures to start building cyber resilience:

DATA BACKUP AND RECOVERY

Regularly back up data and ensure that backups are stored securely and are not accessible from the same network. Consider activating immutability on your backup target storage to make it more difficult for threat actors to impact the backup if they obtain access. AI-driven monitoring tools can validate the integrity of backups, detect anomalies that may indicate tampering or ransomware activity, and automate backup verification processes for faster recovery readiness.

ENDPOINT DETECTION AND RESPONSE (EDR)

Deploy EDR solutions to detect and respond to suspicious activities on endpoints. Modern EDR tools leverage AI to identify and respond to sophisticated threats in real time. Extend this observability into the backup environment by sending logs to your security information and event management (SIEM) platform or using a managed service to provide this capability.

INCIDENT RESPONSE PLAN

Develop and regularly update an incident response plan to enable a swift and effective response to ransomware attacks. AI-driven automation can also help accelerate response actions and reduce manual effort.

NETWORK SECURITY

Strengthen security by implementing network segmentation to limit lateral movement, contain potential threats such as ransomware, and protect sensitive data. Complement segmentation with verification tools such as multi-factor authentication to secure access to critical systems and data, further reducing the risk of unauthorized access and enhancing overall network resilience. AI-powered network monitoring can help detect and respond to anomalous activity in near real time.

CONTINUOUS TESTING

Test rigorously and persistently to proactively validate strategies, identify gaps, and drive operational readiness. AI-based simulations can further enhance testing by modeling complex attack scenarios.

DATA-DRIVEN PROGRAM

Leverage real-time data, metrics, and analytics to pinpoint vulnerabilities, anticipate disruptions, measure readiness, and drive continuous improvement in resilience. AI and machine learning can also analyze incident data, extract lessons learned, and recommend adjustments to resilience strategies, helping organizations adapt to evolving threats.

While these methods offer a solid technical blueprint for defense, the most crucial ingredient is collaboration.

To effectively combat these sophisticated cyber threats, organizations need to go beyond technical defenses and foster a *culture* of cyber resilience. This involves aligning organizational and executive leadership to develop broad action plans that prioritize security and preparedness.

CONVERSATION FIVE

ESTABLISH CLEAR OWNERSHIP AND GOVERNANCE

01
Identify ownership gaps and assign responsibility for building and maintaining cyber resilience across business, technology, and risk.

02
Develop detailed guides (recovery runbooks) that explain how to restore systems from scratch (bare-metal recovery). This helps each stakeholder understand their roles and responsibilities.

03
Align and modernize governance and operating models.

ADDRESSING OWNERSHIP GAPS IS ESSENTIAL FOR CYBER RESILIENCE

ALIGN LEADERSHIP AND OBJECTIVES

- Align senior leadership on program objectives.
- Maintain support throughout an implementation.

ENGAGE THE BUSINESS

- Engage the business early on.
- Act on insights to enhance the strategy's effectiveness.

ADDRESS OUTDATED MODELS

- Recognize that outdated governance and operating models often lack adaptability to emerging threats.
- Identify silos that hinder cross-functional collaboration and timely decision-making.

INCORPORATE LEADING PRACTICES

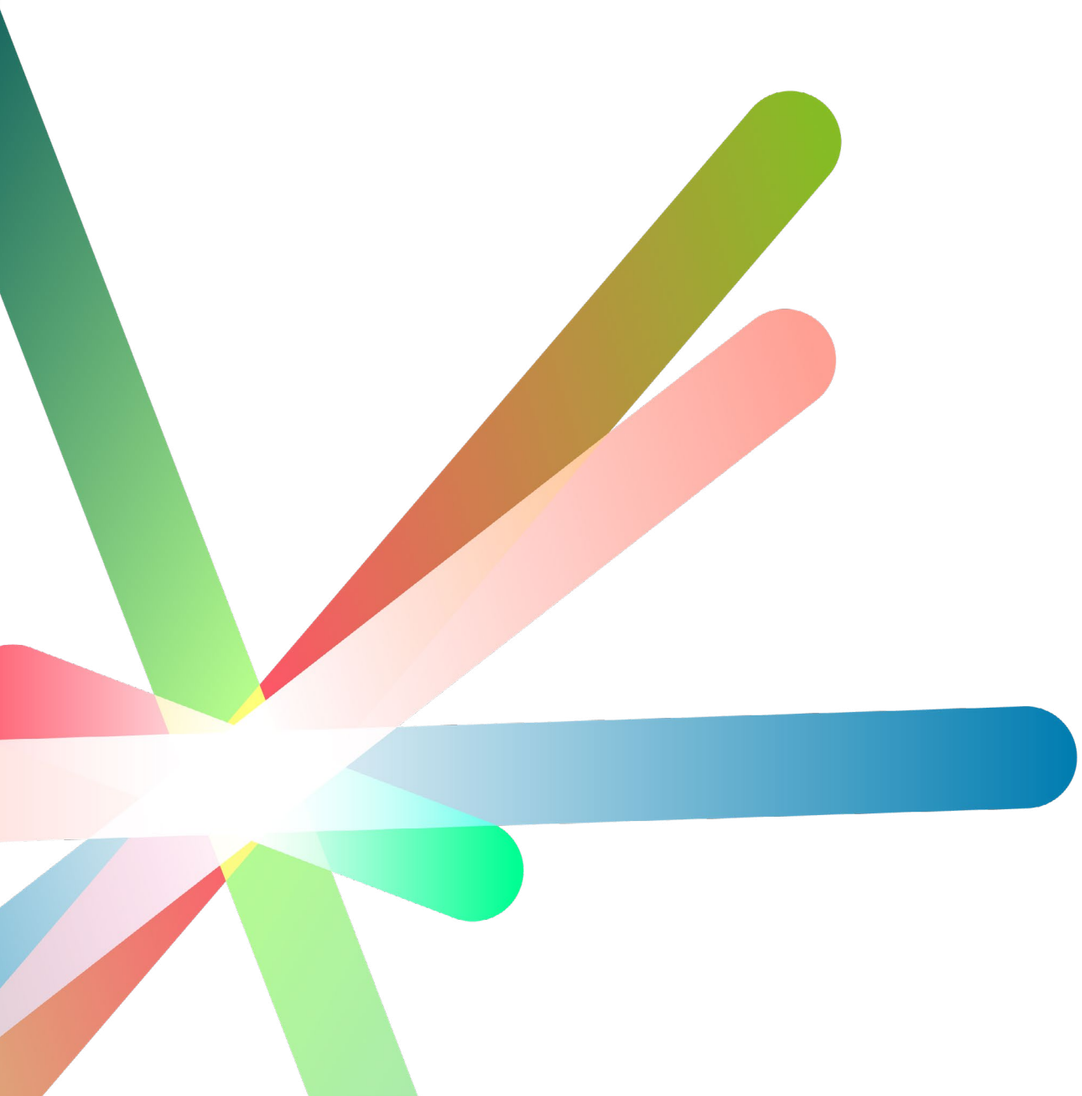
- Design models to reflect leading practices and technologies.
- Adopt a dynamic and integrated approach avoid fragmented efforts.

Navigate budget constraints and clarify recovery responsibilities.

Balancing immediate costs and resources for proactive measures with long-term cyber resilience investments can be challenging. Yet ambiguity in recovery responsibilities can cause delays and inefficient incident response. Clear roles and predefined recovery plans support a swift, coordinated response. Without this clarity, mobilizing resources and personnel promptly becomes difficult, worsening a potential attack's impact.

CONVERSATION SIX

CREATE AND MAINTAIN A PLAYBOOK



01
Establish a response playbook with clear roles and responsibilities and conduct regular tabletop exercises and training.

02
Document processes to investigate, extract, cleanse, review, and reintroduce data (this is important for effective recovery and continuity).

03
Regularly update and test the playbook so it remains relevant and effective in the face of evolving threats.

Disaster response playbooks are critical for cyber resilience. They outline response protocols tailored to your specific environment and threat landscape. Make sure yours includes:

- Clear roles and responsibilities, including defining responsibilities to ensure coordinated responses.
- Regular exercises and training, including simulations to test and refine protocols.
- Process documentation for data investigation, extraction, etc.
- Regular updating and testing to keep the playbook effective (see more below.)
- Governance and oversight structures for accountability.
- Integration and alignment with your overall resilience strategies.

Building cyber resilience through rigorous testing and preparedness.

Relentless, ongoing testing validates the effectiveness of your recovery strategies, controls, and plans—building confidence in your ability to respond to and recover from cyberattacks and other disruptions. Yet, many organizations neglect to regularly validate and update their disaster recovery plans, leaving them vulnerable to evolving threats.

To enable true recovery readiness, organizations should conduct both targeted tests of individual procedures and enterprise-wide exercises. Testing should encompass validation of technical recovery processes, business continuity strategies, and incident response and crisis command strategies. Ongoing employee training and awareness initiatives strengthen organizational preparedness, enable effective incident response, and foster the muscle memory essential for sustained resilience.

COMMITTING TO A UNIFIED APPROACH

A unified approach to cyber resilience is essential for managing security incidents effectively. When an incident occurs, it impacts the entire organization, necessitating strong communication and shared responsibility.

EFFECTIVE COMMUNICATIONS FORM THE BACKBONE OF RESILIENCY

Crisis management
Communication teams manage the narrative, providing clear and consistent information to stakeholders.

Operational continuity
Operations teams address customer service impacts, aiming for minimal disruption through clear communication.

Technical resolution
IT teams resolve technical issues and share information with communications and operations teams so they can set customer expectations appropriately. They also align solutions with business priorities communicated in playbooks and from leadership.

BUILDING CYBER RESILIENCY REQUIRES COLLABORATION ACROSS THE ORGANIZATION

Cross-functional collaboration
Regular meetings and communication channels promote a shared understanding of cyber risks.

Role clarity
Clearly defined roles and responsibilities ensure a coordinated response during incidents.

Training and awareness
Regular training sessions educate employees about their roles in cyber resilience.

Continuous testing
A perpetual approach to validating the myriad of technical, business, and cyber strategies as well as the synchronization of those strategies across the enterprise.

BUSINESS LEADERS CAN TAKE GREATER OWNERSHIP BY ESTABLISHING ONGOING DIALOGUE AROUND

Risk assessment
Regularly assess and discuss the organization's cyber risk landscape.

Incident response planning
Develop and update incident response plans with involvement from all departments.

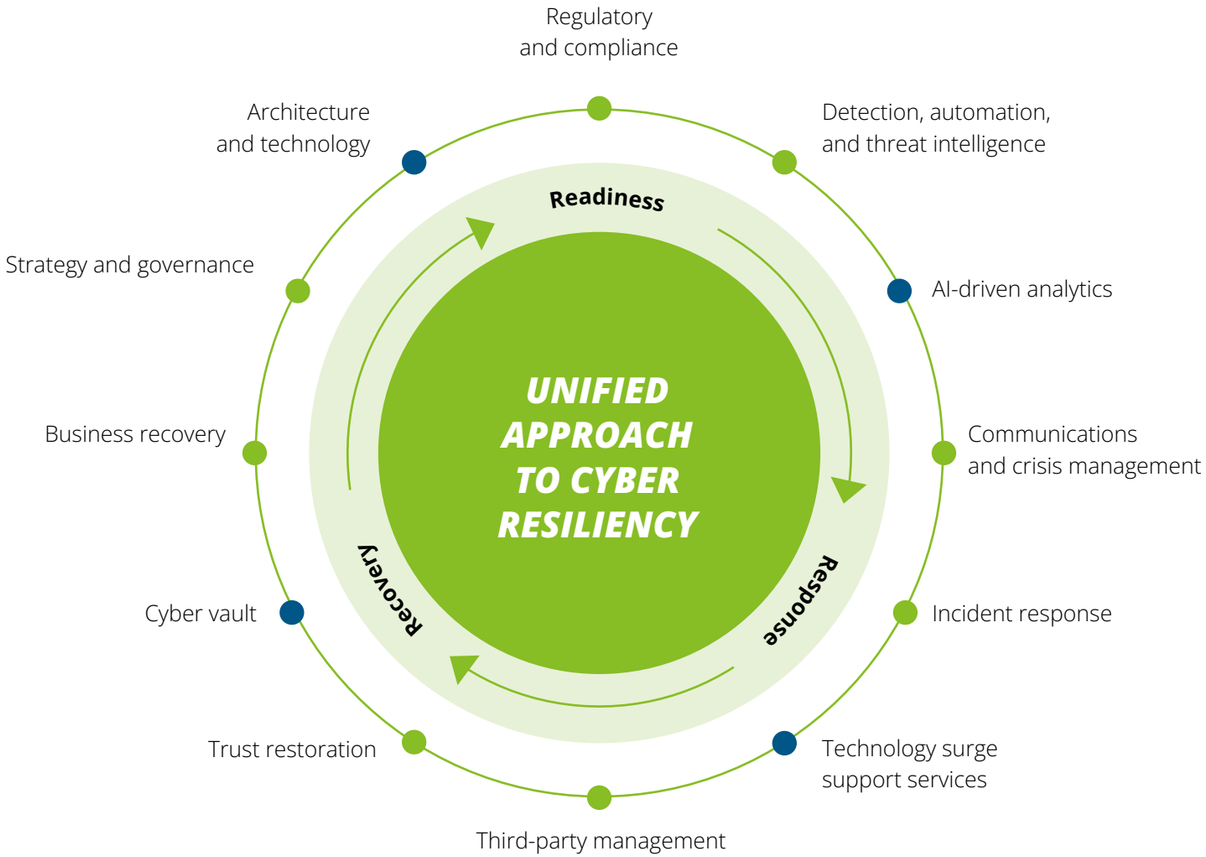
Continuous improvement
Conduct post-incident reviews to identify lessons learned and refine strategies.

STRENGTHENING CYBER RESILIENCE WITH EXPERIENCED COLLABORATORS

Where traditional disaster recovery and cybersecurity measures may fall short in addressing every potential threat, organizations need a cohesive approach to cyber resilience that integrates the right elements and collaborators to prepare for, respond to, and recover from incidents.

Deloitte and Dell collaborate to help businesses navigate the complex and evolving cyber threat landscape by leveraging advanced technology to fortify defenses and secure critical assets. Together, our goal is to help organizations understand cyberattack impacts, prioritize protection, and improve recovery times to reduce collateral damage.

Deloitte's cyber resilience services and Dell's capabilities assist organizations in reducing risks, protecting assets, maintaining service resilience, and supporting compliance to achieve business objectives with enhanced cybersecurity.



Deloitte. DELL Technologies

Together, Deloitte and Dell provide cyber resilience that helps you transform reactive necessity into proactive advantage and instills confidence in stakeholders across the organization.

DELOITTE'S RANGE OF SERVICES ARE REINFORCED BY:

SPECIALIZED CAPABILITIES
Deloitte's cybersecurity team includes cyber resilience professionals, forensics specialists, and incident recovery specialists.

TIMELY, RELEVANT STRATEGIES
Our approach evolves as new intelligence surfaces, new ransomware variants emerge, and new methods are discovered. We also bring clarity on risk exposure and business impacts to inform resilience decisions and beyond.

DEEP OPERATIONAL KNOWLEDGE
Deloitte offers a range of managed services—Extended Detection and Response, Cyber Threat Intelligence, Vault, and others—that embed 24/7 vigilance into client operations, freeing teams to focus on running the business.

FIELD EXPERIENCE
Deloitte has deep experience helping clients respond to and recover from attacks. We bring lessons learned from the field along with unified and tested methods, tools, and technologies that can help drive risk reduction.

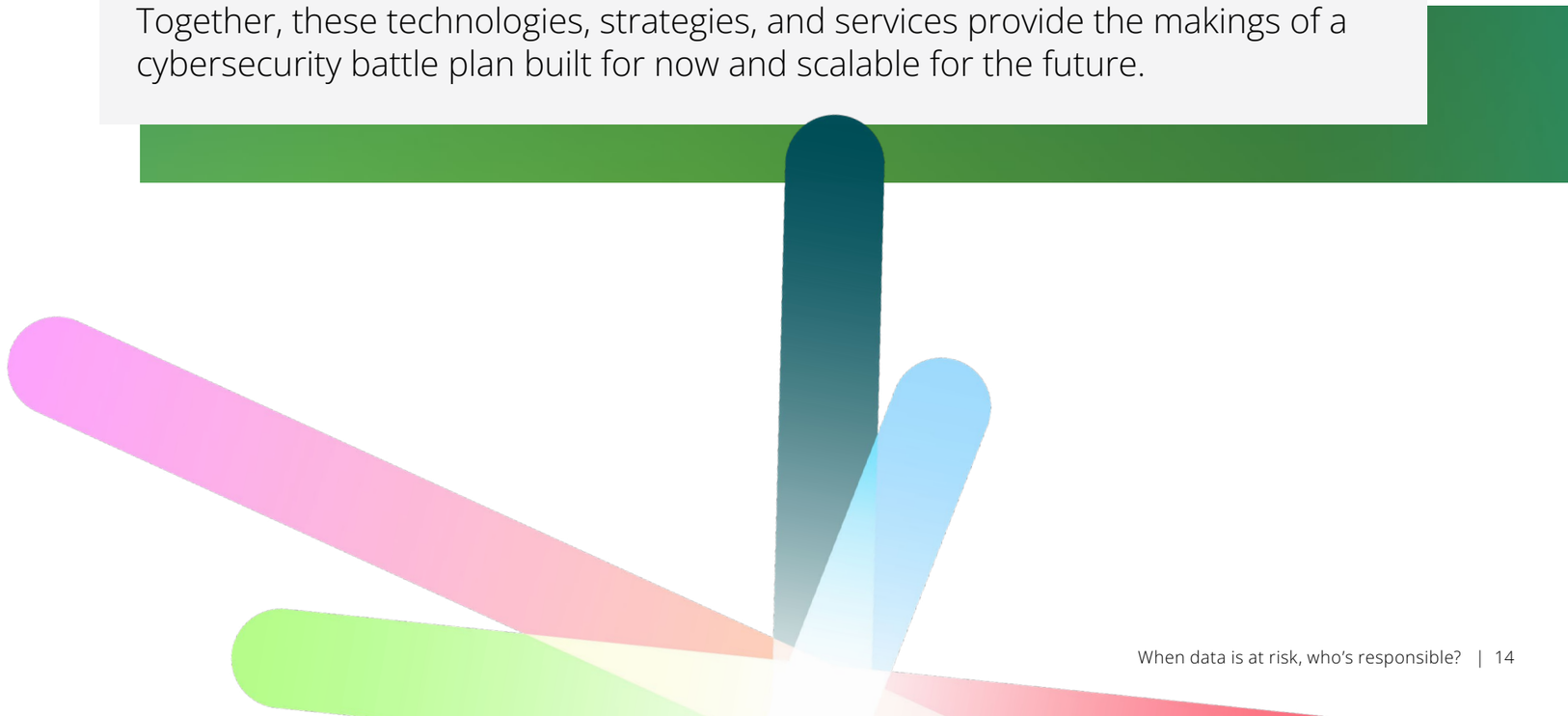
INDUSTRY SPECIALIZATION
Specific teams focus in every major sector and industry, bringing broad context for understanding challenges, as seen in our IndustryAdvantage™ methodology.

ACCELERATED APPROACH
Deloitte's ransomware assessments can inform client methodology, shortening the time it takes to gather information, make plans, and develop actionable recommendations.

Dell provides comprehensive, market-leading cyber resilience capabilities and solutions through its PowerProtect line of solutions and advanced AI capabilities. Dell solutions help organizations:

- Deploy securely, aligned to zero trust principles while monitoring and preventing drift.
- Detect and respond quickly and intelligently to threat actors and anomalies, leveraging indicators of attack and compromise to limit damage.
- Recover efficiently and securely, with options based upon recovery goals, whether the recovery scope is large or small.
- Take advantage of agile technologies and ready-to-deploy global resources to accelerate business restoration.
- Harness the power of AI to proactively strengthen cyber resilience across a myriad of use cases including threat intelligence, vulnerability identification, and cyberattack simulations.

Together, these technologies, strategies, and services provide the makings of a cybersecurity battle plan built for now and scalable for the future.



WHAT HAPPENS NEXT?

Is it time to rethink how your organization strategizes around cybersecurity and devise solutions for a dynamic future?

Improving resilience in your cybersecurity approach can enhance recovery capabilities, limit operational disruptions, and strengthen the roles and responsibilities of the people tasked with overseeing them.

But this is a cultural shift, not an overnight change. To foster a culture of cyber resilience, mitigate risks, and maintain operational continuity, organizations should engage senior leadership, align governance models, scale for the future, and implement defenses. But there's no reason to go it alone.

Deloitte and Dell are ready to help your organization devise and deploy integrated strategies and solutions, equipping you with a playbook and tools to be able to respond effectively and recover swiftly. Let's get started together.

Learn more about the Deloitte and Dell alliance at www.deloitte.com/us/dell.

GET IN TOUCH

PETE RENNEKER
Dell Alliance US Cyber Portfolio Leader
Deloitte & Touche LLP
prenneker@deloitte.com

SHARON CHAND
US Cyber Defense and Resilience Leader
Deloitte & Touche LLP
shchand@deloitte.com

SHIVAN AGRAWAL
Dell Alliance US Cyber Resilience Offering Leader
Deloitte & Touche LLP
shiagrawal@deloitte.com

GIRISH SRINIVASAN
Dell Alliance Leader
Deloitte Consulting LLP
gsrinivasan@deloitte.com

JACQUIE PERELLO
Dell Alliance Manager
Deloitte Consulting LLP
jperello@deloitte.com

JIM SHOOK
Global Director, Cybersecurity and Compliance Practice
Dell Technologies
jim.shook@dell.com

MICHAEL MEYER
Global Sales Leader, Technology, Security and Resiliency
Dell Technologies
michael.w.meyer@dell.com

RAY LIPSKY
Senior Vice President of Global Sales, Security and Resilience Platforms
Dell Technologies
ray.lipsky@dell.com

AMANDA GILLIGAN
Global Account Executive, Data & Cyber Resiliency
Dell Technologies
amanda.gilligan@dell.com

ADRIANA ENGELS
Global Alliance Leader
Dell Technologies
adriana.engels@dell.com

ANDREW KERR
EMEA Global Alliance Account Executive
Dell Technologies
andrew.kerr@dell.com

MICHAEL COOPER
APJ Global Alliance Account Executive
Dell Technologies
michael.cooper@dell.com

LUCIANE DALMOLIN
LATAM Global Alliance Leader
Dell Technologies
luciane.dalmolin@dell.com

REFERENCES

1. https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/
2. https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

ABOUT DELL TECHNOLOGIES

Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the AI era.

ABOUT DELOITTE