Deloitte.

In association with **Dell**

WHEN INFRASTRUCTURE IS AT RISK, ***WHO'S RESPONSIBLE?***

Why cyber resiliency should be at the top of your enterprise agenda

With cyber threats on the rise, an attack has the potential to cause significant disruption to an organization. Following a major security incident, Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs), and their superiors (CEOs) may find themselves dealing with more than a PR 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, leaders can shift the focus from triage to triumph with open, honest dialogue about their current cybersecurity posture. So, what really happens when teams work as one to build cyber resiliency?

The 6 conversations you (and your teams) should be having *now*

According to recent reports, ransomware attacks increased by 62% globally in 2023[1], while the cost to recover from a ransomware attack increased by about 50%[2]. Also, over a third of victim organizations took more than a month to recover[2]. The threat of cyberattacks and bad actors deploying progressively sophisticated tactics keeps organizations and the systems they manage on edge.

Cyber resilience combines the ability to reduce cyber threats—such as ransomware—with the capabilities to recover impacted systems and limit disruption to the business. To build cyber resilience, leaders should prioritize conversations around many topics, including:

1 **Engage at the top:** Set a vision and plan for operational resilience to combat increasingly complex and global disruption scenarios like cyberattacks.

2 **Understand your current state:** Analyze organizational readiness across business, technology, and cyber lenses and explore how a ransomware attack would impact operations.

3 **Heart of the business:** Identify essential services necessary for the organization's survival and focus on protecting those services rather than protecting every bit and byte.

4 **Strategy:** Develop unified and synchronized capabilities across business, technology, and risk to detect, respond to threats, and recover from destructive attacks, supported by appropriate technology.

5 **Ownership:** Identify ownership gaps and assign responsibility for building and maintaining cyber resilience across business, technology, and risk.

6 **Playbook and governance:** Establish a response playbook with clear roles and responsibilities and conduct regular tabletop exercises and training.

[1] https://www.sonicwall.com/news/2023-sonicwall-cyber-threat-report-casts-new-light-on-shifting-front-lines-threat-actor-behavior

[2] https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/

Everyone has a seat at the table

When a security incident happens, it can affect the entire organization. Communication teams must manage the narrative, operations must address customer service impacts, and IT teams must resolve the technical issues. By establishing a dialogue around these topics, business leaders can also take greater ownership of the distinct (and unified) roles they play in helping build cyber resiliency. In these scenarios, the questions may differ, but the response is shared—and stronger for it:

BOARD OF DIRECTORS
How would a cyberattack impact our business and operations? How confident are we in the organization's ability to respond and recover from a cyberattack? Are we investing adequately in cyber resiliency?

CEOs
Does our resilience strategy align with our business strategy? Have we established a culture of security and resilience? How robust is our business continuity plan in the face of a disruptive cyberattack?

COOs
Have we properly identified and defined our essential operational services? How would we maintain operations if we experienced a sudden loss of the underlying technologies? How confident are we in our ability to do so?

CIOs
How resilient are the organization's critical technologies to destructive attacks? What is our plan to recover critical infrastructure, and the technology needed to deliver our most critical services?

CROs
How do we assess and quantify the risk of destructive cyberattacks? How are we integrating cyber and resilience into our overall risk management framework? Do we have the appropriate business and technology mitigation strategies in place?

CISOs
How effective are we in educating key stakeholders on emerging cyber threats and their potential for disruption? How can we synchronize our response activities with business continuity, disaster recovery, and crisis management?

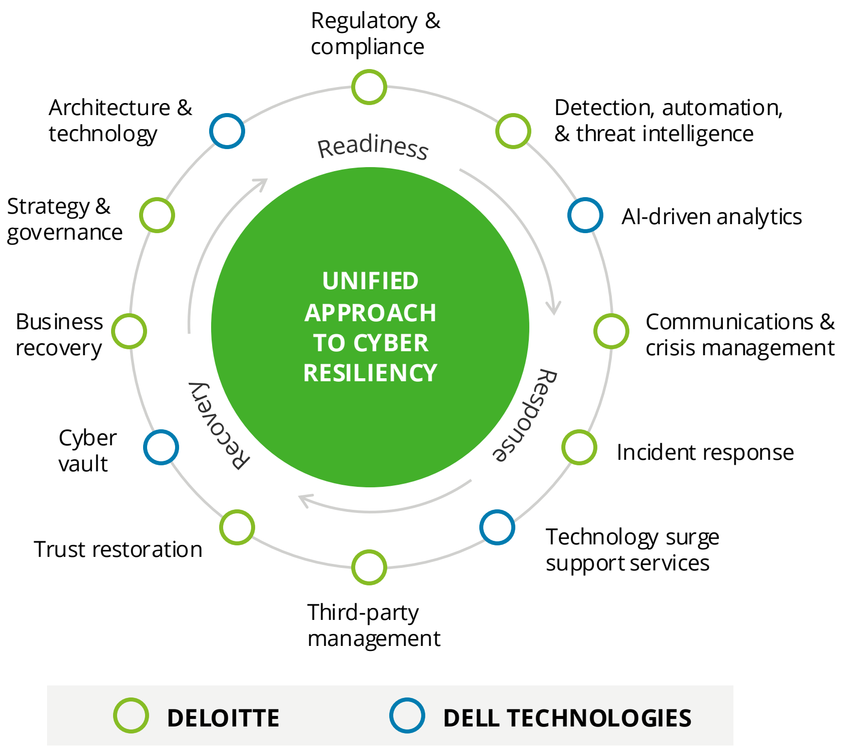
CLOs
What are our legal and regulatory obligations regarding cyber disruptions and data protection? What is our approach to managing data privacy and protecting sensitive information from these threats?

Building a unified support network for 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.

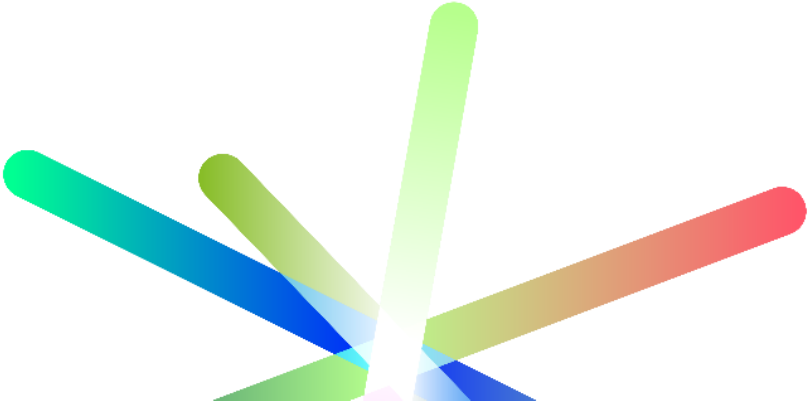
Together, Deloitte and Dell Technologies (Dell) can help businesses leverage advanced technology to fortify defenses and develop a strategy and approach to secure critical assets. It's our goal and passion to help organizations gain insights into the effects of cyberattacks, prioritize protection of critical services, know what to recover, and document recovery sequencing to improve recovery times and reduce the risk of collateral damage.

Deloitte's cyber resilience services and Dell's broad cyber resilience capabilities can assist organizations to reduce risks, protect critical assets, maintain service resilience, and support compliance to achieve business objectives with enhanced cybersecurity across the data protection environment.



Together, Deloitte and Dell deliver a level of cyber resiliency that can help clients turn reactive necessity into proactive advantage. That includes Deloitte's cybersecurity talent pool, comprised of cyber resilience professionals, forensics specialists, and incident recovery specialists, along with our deep industry knowledge and breadth of industry-specific approaches—like IndustryAdvantage^{TM}—that help clients navigate today's complex business and regulatory landscape.

Combine that with Dell's market-leading cyber recovery solutions—which have been delivering protection since 2015 through the use of mainstay solutions like PowerProtect and CyberSense—and you have the makings of a cybersecurity battle plan built for now and scalable for the future.



Taking the next step with Deloitte and Dell

It's 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 to help limit operational disruptions and strengthen the roles and responsibilities of the people tasked with overseeing them.

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

CONTACTS

Pete Renneker
Dell Alliance Cyber Lead
Deloitte & Touche LLP
prenneker@deloitte.com

Jim Shook
Global Director, Cybersecurity and Compliance Practice
Dell Technologies
jim.shook@dell.com

Shivan Agrawal
Senior Manager
Deloitte & Touche LLP
shiagrawal@deloitte.com

Adriana Engels
Global Alliance Leader
Dell Technologies
adriana.engels@dell.com

Jacquie Perello
Dell Alliance Manager
Deloitte Consulting LLP
jperello@deloitte.com

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

Learn more about the Deloitte and Dell alliance at www2.deloitte.com/us/dell.

This publication contains general information only and Deloitte and Dell are 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 and Dell shall not be responsible for any loss sustained by any person who relies on this publication.

All product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte & Touche LLP is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document.

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.