



Business Challenge

In today's digitized world, as organizations become more dependent on technology, they also become more exposed to exploitation, fraud, and theft. Increasingly, these threats put organizations at risk worldwide- bringing business operations to a halt for days and even weeks- costing millions.

In fact, according to Forbes, 2021 saw 50% more cyberattack attempts per week compared to 2020¹.

Beyond the concern of exposure of sensitive information or proprietary data, the growing reality is that many cyberattacks are specifically designed for data destruction or encrypting data and holding it for ransom. Many recent ransomware attacks were particularly damaging to manufacturing systems, hospital information systems, banking systems and local governments. These attacks can bypass traditional security controls at the perimeter, allowing the attacker to go undetected for months or sometimes even years, impacting the most amount of systems possible, and leaving the business even less prepared to recover. In addition to bad actors outside of your organization, the unfortunate truth is that insiders are involved in a growing number of cyber-attacks and leadership needs to be prepared to protect their business against all types of threats.

This rise in cyberattacks poses a rising risk to business operations, impacting the confidence of your customers and business stakeholders in your recovery capabilities.

A study conducted by Forbes found that

78%

of organizations lack confidence in their company's cybersecurity posture².

Increase confidence with your ability to recover from a cyberattack with Professional Services for Cyber Recovery

Summary of benefits

- Adaptable recovery methods based on the impact of the attack
- Flexible solutions to be able to respond to evolving business needs
- Reduce risk through preparedness of processes
- Mature processes that build cyber resilience

Service Description

Dell's Professional Services for Cyber Recovery enables organizations to increase their cyber resilience through a holistic cyber recovery program which brings together technology, process, and people to form a last line of defense for the business.

With Dell's Services we help achieve an air-gapped data protection vault, keeping an isolated copy of your most critical data (e.g. essential applications, data and intellectual property) off the production network and separated from production backup systems. With no direct network connection and multiple roll-back points available, having an uncompromised 'gold copy' ready for recovery will allow you to feel confident in your ability to recover from a cyberattack.

Offer Overview

Advisory and Design: Create consensus and speed design

Deploy and Implement: Basic Deployment through to highly custom

Runbook and Validation: Runbook development, testing and validation

Operate and Manage: Operate and Manage the solution

Cyber Recovery Service Capabilities

Proven methodologies, collaborative approaches and industry best practices to help you accelerate security initiatives and become more resilient

We work to build consensus between key stakeholders, speed solution design through optimizing architecture, create a strategic roadmap to drive program maturity and tie agile and incremental activities to the bigger picture.

Operationalize a cyber recovery solution tailored to your exact business needs

Our implementation services span from basic deployment through to highly custom services to tailor the solution to your exact business needs. We can expand solutions based on specific business and IT requirements to enable you to achieve business recovery at speed and scale, integrate cyber recovery into organization wide cyber incident response plans and integrate with ITSM/ ITIL processes.

Develop runbook and operational procedures for recovery

Respond to a cyberattack with precision and agility through runbook development, regular testing and validation of recovery procedures to build program maturity.

Drive consistency in operations and reduce risk

We offer Residency Services, where we can provide specialized experts with deep, technical skills and experience in to aid in testing recovery to production, additional CyberSense alert tuning or more. These residents will act like an extension of your IT staff, providing technical expertise and experience to enhance your internal capabilities and resources.

Furthermore, after your Cyber Recovery Solution is up and running, our Managed Services can provide day-to-day vault operations, monitored 24x7x365 by global operations team, enabling you to drive consistent procedures and testing and support recovery operations.

Keep your teams' skills up to date with the latest cybersecurity training

With a variety of modules, from PowerProtect focused modules in Cyber Recovery Training, DD concepts and features, virtual edition implementation and DM implementation and administration to a variety of security certifications from user authentication, access controls and security standards, NIST Cybersecurity Framework and Introduction to IT Frameworks, keep your teams' skills up to date with the best-of-breed, latest cybersecurity certifications and training.

Over
1000
customers

Thought
leaders with
expertise
in cyber
recovery for
over 6 years

Over 20
years of
business
resiliency
innovation

For more information visit <https://www.dell.com/en-us/dt/services/consulting-services/cyber-recovery.htm>

¹ <https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=4f9a64186b61>
<https://www.cybersecurityintelligence.com/blog/corporate-cyber-attacks-up-50-last-year-6069.html>

² <https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-----what-you-need-to-know-for-2021/?sh=4599b11058d3>