Enterprise Strategy Group by TechTarget

Preparedness Gap

Why Cyber-recovery Demands a Different Approach From Disaster Recovery

Disruption of IT services directly affects operational success, highlighting the importance of technology and cyber resilience. Traditional disaster recovery often falls short against modern cyber threats, necessitating advanced cyber-recovery planning to handle unknown disruptions in scope, impact, and scale.

This Enterprise Strategy Group Infographic was commissioned by Commvault and is distributed under license from Informa TechTarget, Inc.

How Cyber-recovery Differs From Disaster Recovery

While cyber-recovery shares many of the characteristics of more traditional disaster recovery, IT and security leaders report that cyber events are typically more complex than a traditional outage or disaster, requiring different processes and workflows, different technologies and features, and different personnel and skill sets for response and recovery.

68%

of organizations said that cyber-recovery involves a different workflow than traditional disaster recovery.

68%

of organizations said that cyber-recovery involves different technologies and features than disaster recovery.

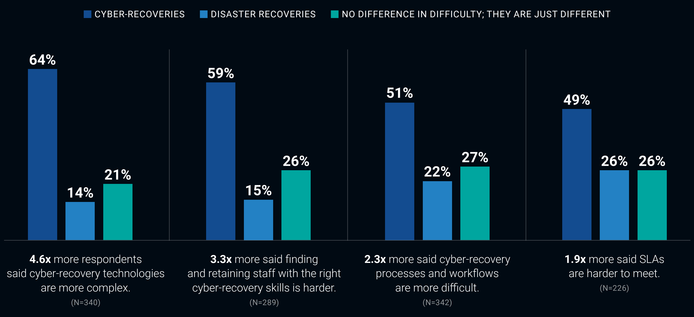
58%

of organizations said that cyber-recovery involves different personnel and associated skill sets than disaster recovery.

54%

of organizations said that cyber-recovery is more complex than disaster recovery.

Across the board, cyber-recovery is seen as more difficult and complex than traditional disaster recovery, with harder-to-meet service-level agreements leading the way.



4.6x more respondents said cyber-recovery technologies are more complex. (N=340)

3.3x more said finding and retaining staff with the right cyber-recovery skills is harder. (N=289)

2.3x more said cyber-recovery processes and workflows are more difficult. (N=342)

1.9x more said SLAs are harder to meet. (N=226)

Why Cyber-recovery Is Much More Challenging Than Traditional Disaster Recovery

More than four out of five respondents agreed that there are complexities specific to cyber-recovery, when handled incorrectly, that can create significant risk. The complexities include:

91%

said significant time and effort is required to do a forensic analysis to determine the full scope of what was infected.

85%

said recovering without first establishing a cleanroom environment creates significant risk of reinfection.

83%

said rushing to recover from a cyber incident often destroys key evidence of how the attack was executed, leaving the organization vulnerable.

Cyber- and Disaster Recovery: Separate or Components of a Combined Program?

Despite differences and additional complexity, organizations include cyber-recovery planning as a part of their broader disaster-recovery program or report a high degree of alignment between cyber-recovery and disaster recovery.

52%

of organizations include cyber-recovery as part of their broader disaster-recovery plan.

42%

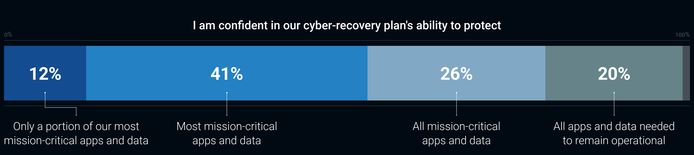
of organizations maintain separate cyber-recovery and disaster-recovery plans but have a high degree of consistency in processes and protocols used in both.

6%

of organizations maintain separate cyber-recovery and disaster-recovery plans, with a high degree of variability in processes and protocols used between them.

More Work Is Needed to Strengthen Cyber-recovery

Only 26% of organizations felt confident in their ability to protect all mission-critical applications and data. This alarming statistic demonstrates how much work is needed to achieve effective levels of cyber resilience.



Only a portion of our most mission-critical apps and data

Most mission-critical apps and data

All mission-critical apps and data

All apps and data needed to remain operational

Cyber-recovery: Critical to Cyber Resilience

Cyber resilience has become a mainstream objective for IT and security leaders alike. As strategies mature, aligning to core business resilience objectives requires collaboration and alignment between line-of-business leaders and technology leaders. While disaster-recovery strategies are well understood and reasonably well implemented for most, cyber-recovery strategies continue to be a work in progress, with different and often more-expansive requirements across people, process, and technology.

All facets of the operating infrastructure must be considered, prioritized, and protected to enable continual business and financial risk mitigation. Data resilience and cyber resilience are both core to achieving these objectives. Data protection vendors such as Commvault can help provide the strategy and solutions needed to meet these requirements.

For more information on how Commvault can help strengthen your disaster- and cyber-recovery strategy and execution, click the link below.

LEARN MORE

Source: Enterprise Strategy Group eBook commissioned by Commvault, *Preparedness Gap: Why Cyber-recovery Demands a Different Approach From Disaster Recovery*, December 2024.