451 Research
Vanguard Report

July 2024

Achieving cyber resilience requires teamwork

Discover how security and IT teams work together to keep data safe, prevent cyberattacks and quickly recover from disruptions

Commissioned by

PURESTORAGE®

S&P Global
Market Intelligence

Introduction

In our recent storage study, nearly a fifth of organizations said an outage led to employee terminations, which should motivate both security and infrastructure operations teams to collaborate to ensure recovery operations run reliably and quickly. Data leakage resulting from a security incident could also lead to costly lawsuits from shareholders and customers. With security-related incidents such as ransomware becoming the top cause of data outages, security and IT operations professionals must work together to improve the resiliency of their IT environment.

Figure 1: Disaster recovery trends

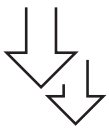
Outages are likely and costly

71%

Have experienced a significant outage

$2.15 million

Is the mean cost of recent outages



Negative business impacts

48%	Experienced lost worker productivity in their outage
32%	Lost data from their outage
20%	Experienced a damaged reputation because of their outage
19%	Of outages led to employee terminations
17%	Experienced penalties related to compliance
14%	Lost company loyalty due to an outage

Q. When was the last time your organization experienced an outage that resulted in lost data or affected worker productivity?
Q. Please estimate the total cost to your organization of its most recent outage or downtime (from outage to full recovery, including direct costs, opportunity costs, etc.).
Base: IT decision-makers whose organizations use on premises storage systems (n=269).
Q. Which of the following effects did your organization experience as a result of your previous outages? Please select all that apply.
Base: IT decision-makers whose organizations experienced an outage/downtime that resulted in lost data or productivity (n=182).
Source: 451 Research's Voice of the Enterprise: Storage, Disaster Recovery 2023.

The Take

The scope and scale of ransomware attacks has intensified in recent years, with newer attacks able to incapacitate an entire infrastructure for days or even weeks, a far more serious situation than a localized attack that compromises a few workloads and datasets. The Office of Foreign Assets Control released an advisory regarding the potential risks of US companies making ransomware payments to sanctioned persons, business and entities, which could lead to large financial penalties and prison time up to 30 years. The goal is to drive more organizations to enhance their resiliency capabilities to avoid making ransom payments.

The National Institute of Standards and Technology (NIST) makes it clear in its Cybersecurity Framework (CSF) that security and IT teams must work together to do more before, during and after a ransomware attack to ensure their infrastructures are resilient against cybersecurity incidents. The NIST CSF not only reduces the impact of attacks, but it may also be able to prevent outages and permanent data loss.

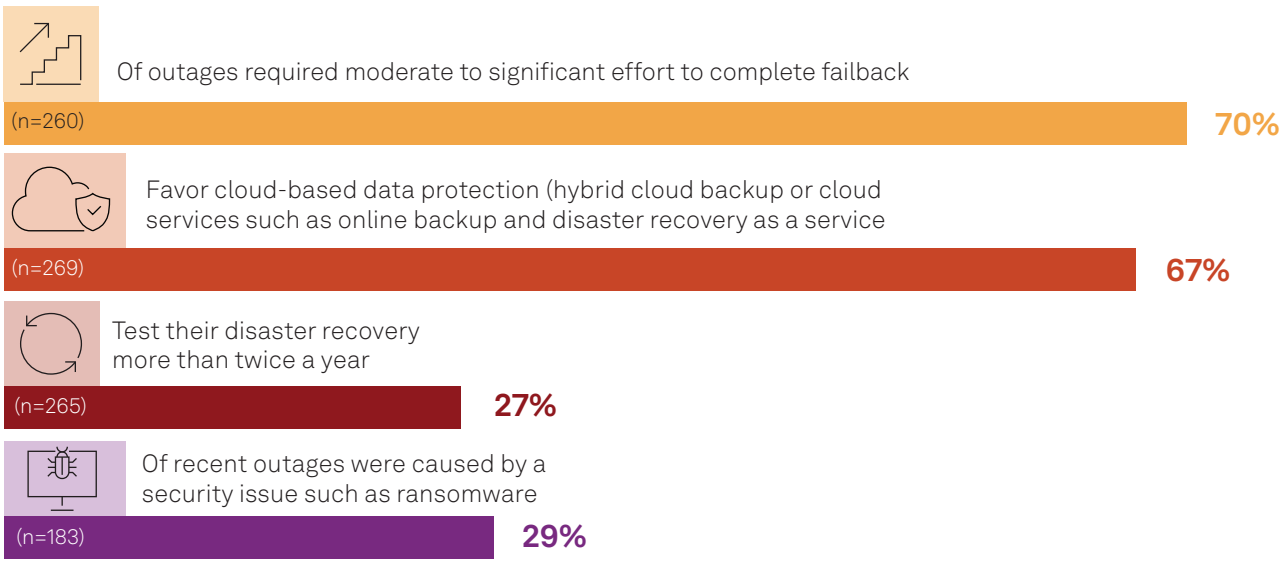
The large impact of outages

Organizations incur significant costs from downtime and outages. Recent outages cost an average of $2.15 million, up from $1.56 million a year ago, and this will likely only increase year over year. More than 70% of respondents experienced a significant outage, with almost a third occurring within the last two years (see Figure 1).

Beyond the obvious losses of data and productivity, outages hurt the business in several additional ways. For example, 48% of respondents reported they lost employee productivity due to an outage. Lost revenue from missed business opportunities affected 30% of respondents in their last outage. A damaged business reputation (20%) and lost customer loyalty (14%) were additional consequences, and these are extremely serious given the rising importance of customer experience ratings such as net promoter scores. About 17% of respondents said their outage led to compliance penalty fines, and some organizations are considering tying executive bonuses and compensation to a company's security performance.

Organizations favor cloud-based data protection for cyber resilience over exclusively on-premises. Although 34% of respondents still favor keeping their data protection tools and backup storage systems on-premises, 42% have implemented hybrid cloud offerings that maintain local backup copies for fast recovery, and they put older backups in off-site public cloud storage. From a security team perspective, end-to-end encryption, indelible data and other capabilities are required to protect data, whether it resides on-premises or in a public cloud.

Figure 2: Evolution of data protection requirements



Q. How much effort is required to resume normal operations after a failure (i.e., a failback)?
Q. Which of the following best describes your organization's current use of data protection (e.g., backup, disaster recovery)?
Q. How frequently does your organization test your disaster recovery plan?
Base: IT decision-makers whose organizations use on-premises storage systems.
Q. What was the cause of your organization's most recent outage that resulted in lost data or affected worker productivity?
Base: IT decision-makers whose organizations experienced an outage/downtime that resulted in lost data or productivity.
Source: 451 Research's Voice of the Enterprise: Storage, Disaster Recovery 2023.

Shared responsibility

Both security and IT teams have a shared responsibility to ensure their organization is safe from cybersecurity threats, and a shared liability in the risks. Although security professionals should not take over data protection processes from their infrastructure operations counterparts, they should receive assurance that backups and other resilience processes are run so as to meet industry standards such as NIST CSF. Most outages require great recovery effort. About 70% of respondents said it took a moderate to significant level of effort to complete recovery. To improve the speed and reliability of recovery operations, security and infrastructure teams must collaborate to secure the environment and ensure an attack does not lead to extensive downtime.

Steps toward reducing cybersecurity risk

The NIST CSF 2.0 recommends five functions that organizations should take to manage and reduce their cybersecurity risks:

1. **Identify:** Organizations should identify crucial business processes and assets that are required to keep a business running. This stage requires documentation of information flows and the identification of potential threats and vulnerabilities that can put assets at risk.
2. **Protect:** This calls for several requirements, including access management, the protection and monitoring of devices, and the use of automated backups to ensure data is recoverable. End-to-end data encryption is another requirement to protect data both at rest and in flight.
3. **Detect:** This requires the monitoring of networks, systems and facilities to locate possible cybersecurity attacks and compromises.
4. **Respond:** This covers actions to take when a detected cybersecurity incident has taken place.
5. **Recover:** These are functions that cover how assets and operations are restored after being impacted by a cybersecurity incident.

Storage and backup capabilities are required to fulfill several of the functions in the NIST CSF. Within the **protect** function, regular backups with indelible storage are required to ensure recovery after a cybersecurity event. The protect function also requires security professionals to have access to control capabilities to ensure that administrator accounts are monitored and secured with technologies such as multi-factor authentication. By doing this, security teams can prevent bad actors with stolen administrator credentials from erasing backup repositories that would derail recovery efforts. Protect also requires the use of end-to-end encryption to keep data safe both at rest and in flight.

In recent years, data protection and storage vendors have added in-line ransomware detection capabilities to their platforms to quickly identify cybersecurity threats and suspicious behavior (such as large-scale data deletions or encryptions). Though these capabilities are features within storage systems and software, they should also be leveraged to satisfy the **detect** function requirements in the NIST CSF.

The **recover** function within NIST CSF details how recovery operations will run to minimize recovery times and disruptions to the production environment. Although many organizations still leverage off-site tape as their remote recovery copy, cloud storage has become more common as an alternative. In conjunction with public cloud compute services, cloud storage can facilitate rapid recovery in the public cloud environment to improve recovery time objectives. Using indelible snapshots on primary storage systems allows administrators to quickly roll back volumes to restore data. Companies are also leveraging high-performance all-flash storage within their environments to store their most recent backups, which can be used to accelerate recovery operations on mission-critical workloads.

For the **recover** function, companies should create a clean restoration environment where backup and security professionals can collaborate. A clean lab space that has been separated from core infrastructure helps ensure that a virus can't spread to the rest of the production environment; this benefits security teams looking to contain the contaminated systems. The clean lab environment also allows forensics teams to conduct their validation tests to determine the cause of the breach and facilitate a clean recovery.

After an outage, organizations must make changes based on what they have learned from the incident to eliminate security vulnerabilities (among other issues) that enabled a successful attack to occur and reduce the potential of a repeat attack being successful. Looking at this from the NIST CFS perspective, this reassessment of both the environment and its vulnerabilities should be done in conjunction with the **identify** function in the framework.

About the author

Henry Baltazar

Research Director, Storage

Henry Baltazar is research director of the 451 Research Storage channel within S&P Global Market Intelligence, with a focus on data storage. In his current role, Henry analyzes the market trends around environmental, social and governance (ESG) storage challenges, infrastructure modernization and resiliency. He publishes reports on trends in data storage, disaster recovery and hybrid cloud. He is often cited as a subject expert by publications such as MIT Technology Review, Forbes and TechTarget.

Henry arrived at S&P Global Market Intelligence through its 2019 acquisition of 451 Research, where he began working as an analyst in August 2006. After spending three years running the storage research practice at Forrester, he returned to 451 Research in 2015 to fill the research director role and lead the storage practice.

Henry graduated from the University of California, Berkeley with a bachelor's degree in environmental sciences.

About S&P Global Market Intelligence

At S&P Global Market Intelligence, we understand the importance of accurate, deep and insightful information. Our team of experts delivers unrivaled insights and leading data and technology solutions, partnering with customers to expand their perspective, operate with confidence, and make decisions with conviction.

S&P Global Market Intelligence is a division of S&P Global (NYSE: SPGI). S&P Global is the world's foremost provider of credit ratings, benchmarks, analytics and workflow solutions in the global capital, commodity and automotive markets. With every one of our offerings, we help many of the world's leading organizations navigate the economic landscape so they can plan for tomorrow, today. For more information, visit www.spglobal.com/marketintelligence.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html