FORRESTER®

Future-Proof Your Healthcare Organization With A Robust Data Protection Strategy

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY PURE STORAGE | DECEMBER 2020

Introduction

Hospital organizations of all sizes must contend with unplanned primary IT infrastructure failures; when mission-critical systems are down for hours or, in some cases, days, practitioners and patients alike are left unsupported. However, smaller hospitals — those with fewer than 500 beds — often feel the impact even more acutely since, in many instances, they are the only care providers in the community.

A robust data protection strategy is crucial to mitigate the effect of these unplanned outages. Many hospital decision-makers recognize that their current approaches of weekly or monthly cloud-based or physical backups are inadequate to meet today's needs. They are looking to invest in a real-time backup solution that will allow them to care for their patients, uninterrupted by technical failures.

Key Findings

Nearly all hospital organizations have experienced multiple unplanned primary infrastructure failure incidences within the past 24 months — leaving critical systems unavailable for hours on end.

To combat unplanned outages dramatically impacting patient care and provider workplace experience, 57% of decision-makers plan to invest in a real-time backup data solution within the next 24 months.

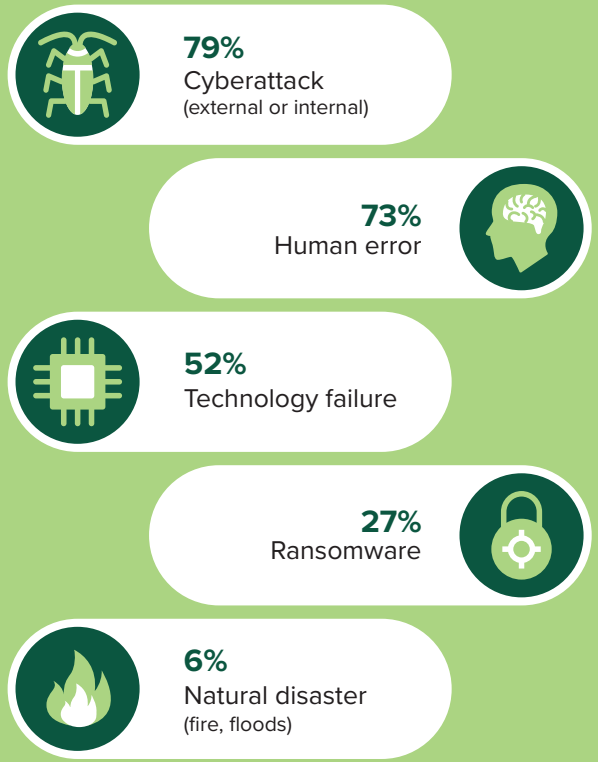
Increased trust — from both patients and practitioners — is the top benefit anticipated from a real-time backup solution.

Unplanned Outages Come In A Variety Of Forms

Nearly every small hospital system decision-maker reports a primary infrastructure failure — i.e., unplanned downtime — within the past 24 months. Small hospitals specifically have experienced, on average, two different types of failures, with the most common being a cyberattack or human error.

In October 2020, the US Cybersecurity and Infrastructure Security Agency (CISA) issued a joint advisory with the FBI and HHS.[1] This advisory notified healthcare organizations of a detected increase in the level of activity in bad actors targeting US-based hospital systems with phishing campaigns designed to infect hospital networks with malware that creates backdoor access for cybercriminals and deploys ransomware on local servers. This threat remains active today.

"In the past 24 months, which of the following has caused primary infrastructure failure (i.e., unplanned downtime) at your organization?"



Base: 153 IT, security, finance, risk, and operations decision-makers for data storage and security
Source: A commissioned study conducted by Forrester Consulting on behalf of Pure Storage, November 2020

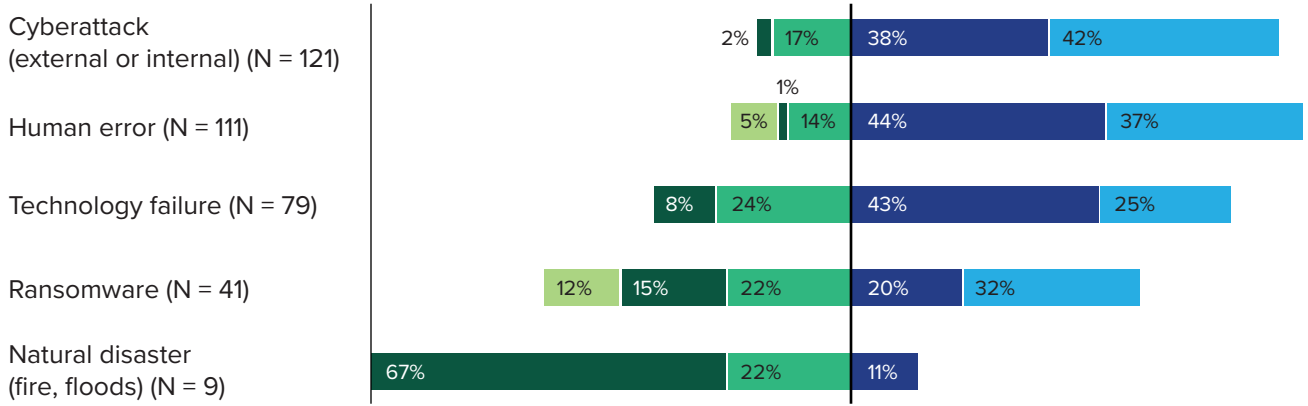
Hospitals Experience Outages Multiple Times A Year

Most hospital decision-makers report having experienced a primary infrastructure failure more than three times within the past two years. Eighty-one percent say their organizations have suffered an outage because of a human error at least three times within the last two years; 80% have experienced such a failure because of a cyberattack at least three times within the last two years. For 42% of small hospital leaders, a cyberattack has left their systems inoperable at least twice a year — a dramatic uptick from previous reports.

42% of small hospital decision-makers have experienced an outage at least twice in the past year.

"In the past 24 months, how frequently have you experienced these failures?"

- Never
- Once
- Twice
- Three times
- More than three times



FORRESTER OPPORTUNITY SNAPSHOT:

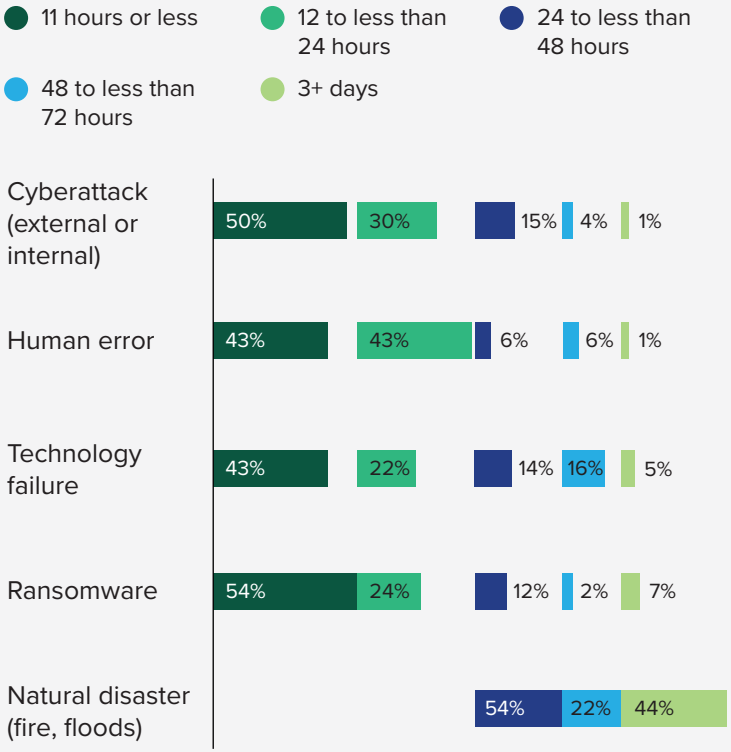
Base: Variable IT, security, finance, risk, and operations decision-makers for data storage and security
Source: A commissioned study conducted by Forrester Consulting on behalf of Pure Storage, November 2020

Outages Leave Hospital Systems Down For Hours Or Days

Each of these incidents leaves hospital systems down for hours, and sometimes days, on end. For each cyberattack in the past year, 80% of decision-makers say their systems were down for up to 24 hours — which, when compounded with the multiple attacks that many hospitals face over the course of a year, means days of system malfunctions.

Nearly 50% of hospital leaders report that after their most recent human error-caused infrastructure failure, their systems were down from 12 to 48 hours — translating to hours of patient information lost, practitioner time spent reentering information, and IT staff time spent resolving the issues.

"Thinking of each of your recent primary infrastructure failure incidents, how long were your systems unavailable to end users?"



Base: Variable IT, security, finance, risk, and operations decision-makers for data storage and security
Source: A commissioned study conducted by Forrester Consulting on behalf of Pure Storage, November 2020

The Impacts Of Primary Infrastructure Failures Are Both Short- And Long-Term

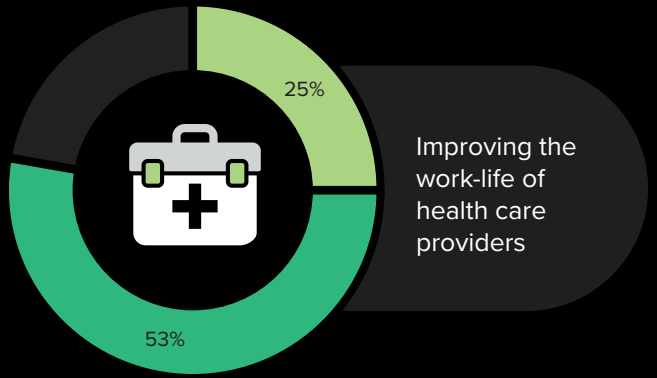
Unplanned downtime has short- and long-term effects on hospital systems, their practitioners, and their patients.

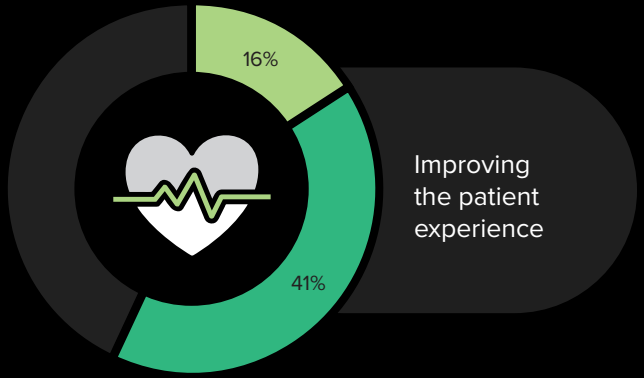
Primary infrastructure failures have a significant impact on the Quadruple Aim goals — the framework for the delivery of high-value care — of small hospital systems. Seventy-eight percent of decision-makers say that a primary infrastructure outage impacts their goal of improving the work-life of healthcare providers; 57% note that such outages also impact their aim to improve the patient experience.

In the short term, nearly 70% of decision-makers note that their cyberinsurance premiums have increased because of their most recent primary infrastructure failure. Over 40% also report loss of practitioner and patient trust.

"What impact did your primary infrastructure failure(s) have on the following Quadruple Aim goals?"

- Significant impact
- Moderate impact





FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY PURE STORAGE
DECEMBER 2020

Base: 153 IT, security, finance, risk, and operations decision-makers for data storage and security
Source: A commissioned study conducted by Forrester Consulting on behalf of Pure Storage, November 2020

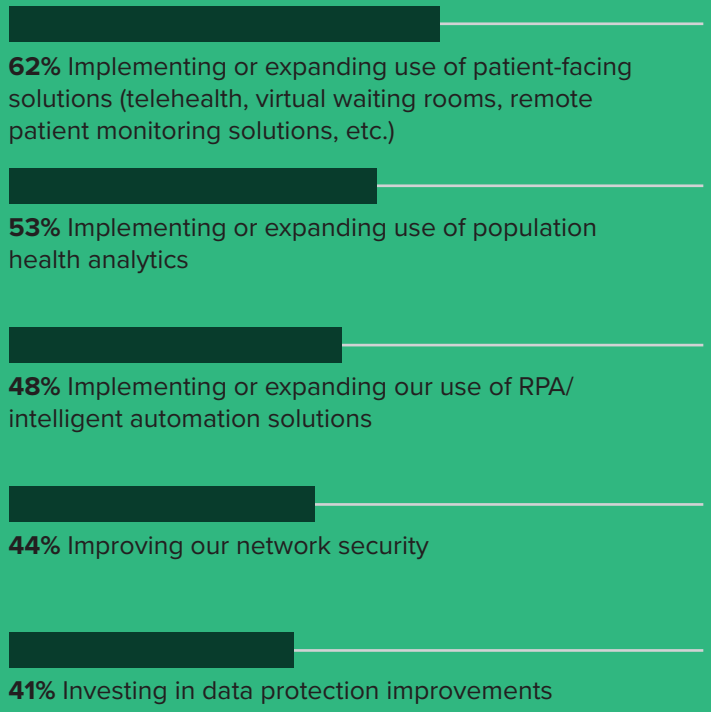
Decision-Makers Realize They Must Update Their Currrent Approaches To Data Protection

Decision-makers at small hospital systems recognize that their current approaches are inadequate. Many complain of long lag times between backups, slow manual backup processes, and lengthy restorations from backups.

Over 40% of decision-makers are prioritizing investing in data protection improvement as one of their top 5 IT priorities for the next 12 months. They realize that their current approaches to data protection — backing up to the cloud in weekly or monthly increments or, as is the case for 46% of decision-makers surveyed, still managing cumbersome manual backup processes — is ineffective and ultimately harming their organizations.

“Please rank your top 5 IT investment priorities over the next 12 months.”

● Ranked in top 5



Base: 153 IT, security, finance, risk, and operations decision-makers for data storage and security
Source: A commissioned study conducted by Forrester Consulting on behalf of Pure Storage, November 2020

A Real-Time Backup Solution May Be The Answer

Small hospital systems are ready to modernize. Leaders recognize the severe limitations of their current approaches to data protection and the reality of an unplanned outage happening with some frequency.

Over a quarter of decision-makers note that they are planning to implement a real-time backup in the cloud within the next 12 months; 57% plan to invest in such a solution within the next two years. Within five years, 86% of decision-makers say their hospital systems will have implemented a real-time backup in the cloud.

As for barriers to implementing such a solution, most decision-makers say that they face few challenges. The ROI is clear to most, and two-thirds have budget in place to support improvements.

"Does your organization plan to invest in a technology solution to provide real-time backups in the cloud?"

26%

Planning to implement in the next 12 months

31%

Planning to implement in the next one to two years

27%

Planning to implement in the next three to five years

16%

Interested, but no plans to implement

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY PURE STORAGE
DECEMBER 2020

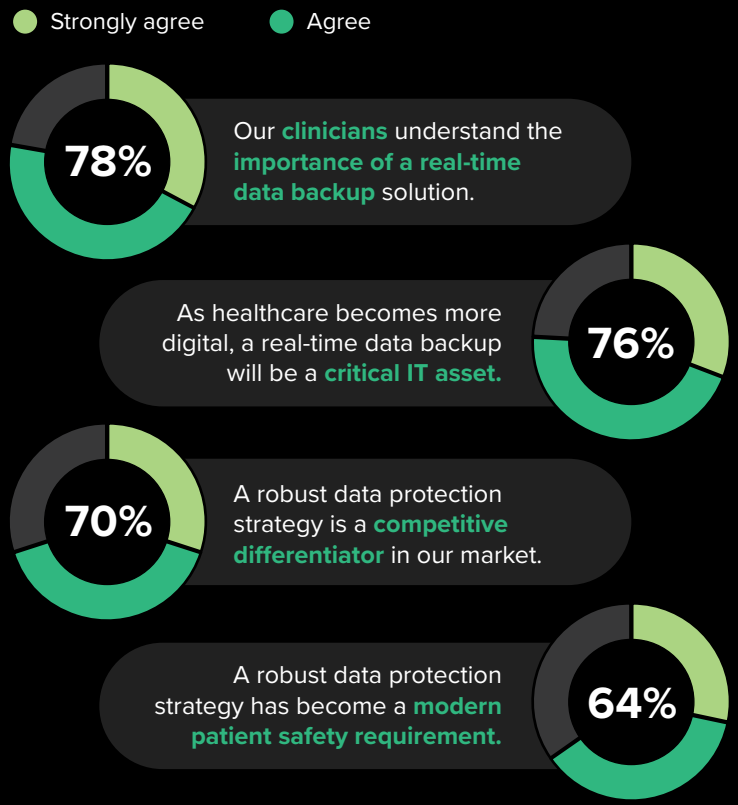
Base: 153 IT, security, finance, risk, and operations decision-makers for data storage and security
Source: A commissioned study conducted by Forrester Consulting on behalf of Pure Storage, November 2020

A Robust Data Protection Strategy Is Critical For Hospital Systems

Decision-makers recognize that real-time backups will be increasingly mission-critical to their healthcare organizations. In fact, 80% anticipate increased trust from their patients and community with a real-time back up, and 76% anticipate increased trust from their practitioners.

Importantly, leaders see real-time backups as the lynchpin of a future-proof healthcare organization. Seventy-six percent note that as healthcare becomes more digital, a real-time data backup will be a critical IT asset; 70% agree that a robust data protection strategy is a competitive differentiator in their market. Crucially, clinicians and patients reap the rewards with a real-time backup: 78% of leaders believe their clinicians understand the importance of a real-time backup solution, and 64% of decision-makers agree that a robust data protection strategy has been a modern patient safety requirement, not just a nice-to-have.

"Please indicate your level of agreement with the following statements."



Base: 153 IT, security, finance, risk, and operations decision-makers for data storage and security
Source: A commissioned study conducted by Forrester Consulting on behalf of Pure Storage, November 2020

Conclusion

For healthcare systems of all sizes, a primary infrastructure failure is not a question of if, but of when. All organizations will experience a primary infrastructure failure; they must be ready with a robust data protection strategy to minimize the effects of such an outage.

- Eighty percent of decision-makers at small healthcare organizations report an outage lasting hours, if not days, at least three times within the past two years.
- Short-term impacts include increases in insurance premiums and loss of trust, but outages also critically affect the long-term Quadruple Aim goals of hospital systems.
- Decision-makers at these small hospital systems must evolve their data protection strategies to remain competitive. Fifty-seven percent plan to implement a real-time backup solution within the next two years.

Project Director:

Ana Brzezinska, Market Impact Consultant

Contributing Research:

Forrester's eBusiness & Channel Strategy Professionals research group

Methodology

This Opportunity Snapshot was commissioned by Pure Storage. To create this profile, Forrester Consulting conducted an online survey of 153 IT, security, finance, risk, and operations decision-makers for data storage and security at small hospital (under 500 beds). The custom survey began and was completed in November 2020.

ENDNOTES

[1] Source: "Ransomware Activity Targeting the Healthcare and Public Health Sector," Cybersecurity & Infrastructure Security Agency, October 28, 2020 (https://us-cert.cisa.gov/ncas/alerts/aa20-302a).

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Demographics

HOSPTIAL TYPE

- 45%: Teaching hospital
- 24%: Acute-care nonteaching hospital
- 18%: Community hospital
- 13%: Long-term acute-care hospital

HOSPTIAL SIZE

- 9%: 25 to 49 beds
- 31%: 50 to 99 beds
- 33%: 100 to 250 beds
- 26%: 251 to 999 beds

RESPONDENT LEVEL

- 18%: C-level or VP
- 55%: Director or manager
- 28%: Project manager or full-time contributor

CURRENT DATA PROTECTION STRATEGY

- 35%: Daily backups to the cloud or a physical form factor
- 46%: Weekly backups to the cloud or a physical form factor
- 20%: Monthly backups to the cloud or a physical form factor

Note: Percentages may not total 100 because of rounding.


FORRESTER®