Hewlett Packard Enterprise | FUJIFILM | adience

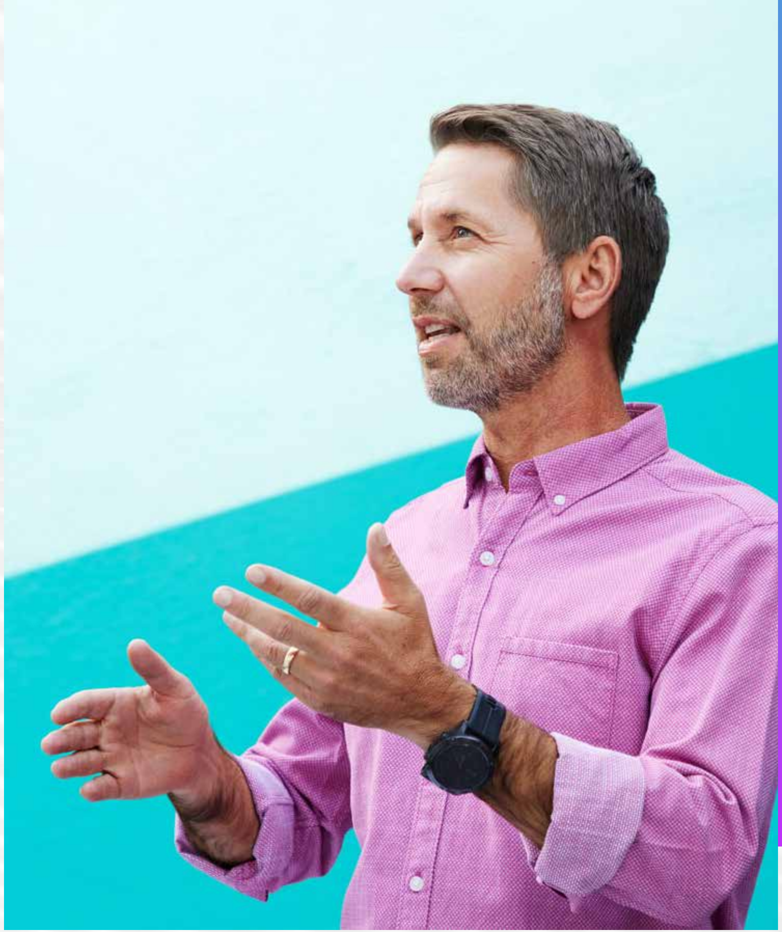
Using tape to defend against ransomware attacks and improve cyber security.

Prepared by Adience for HPE and
FUJIFILM Recording Media USA.

March 2023

Our starting point

HPE StoreEver and FUJIFILM Recording Media USA wanted to gain more information to inform their go-to-market strategy for tape storage solutions. Specifically, they wanted to explore the attitudes the market has toward ransomware attacks.



Project goals | The study sought to:

Identify what technology is being used to respond to attacks

Explore if tape played an important role and/or if they regret not having tape

Evaluate whether they consider/use tape as a response to threats

Understand what would make them more likely to consider tape storage devices

Who we spoke to

152 survey responses to a 10–15 minute survey representing a mix of businesses/roles

Industry

Healthcare/social assist: 25

Manufacturing: 23

Media and publishing: 20

Telecoms: 19

Education: 14

Real estate/leasing: 13

Other: 38

Size
(by employees)

50-499: 41

500-2,499: 56

2,500+: 55

Data stored on premise

200-499 Terabytes: 48

500-999 Terabytes: 45

1+ Petabytes: 59

Job role

C-Suite Exec: 27

VP/Senior VP: 28

Senior Director: 24

Director: 21

Senior Manager: 16

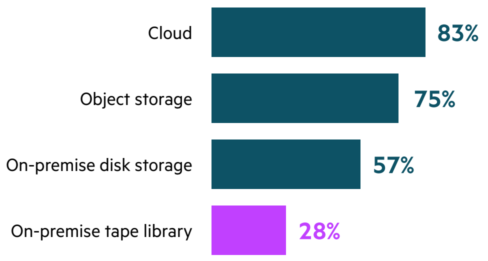
Manager: 21

Other: 15

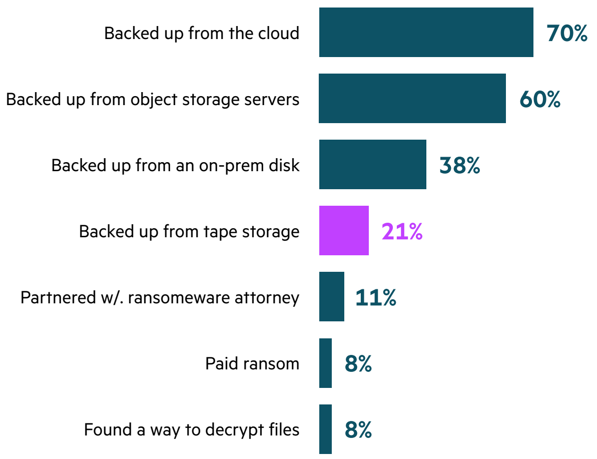
Survey respondents had to meet the following criteria: Be based in the US, work full-time, have over 49 employees, have a dedicated IT function, work within or influence the IT function, store data on-premise or a mix of on-premise and in the cloud, have more than 199 terabytes of data, have experienced a ransom attack in the last two years, and strongly influence/make the decision about how to defend against ransomware attacks. The survey was conducted by telephone/online methods and was live from January 27th – February 15th.

Tape was rarely used by this audience compared to the cloud or object/disk storage

Backup methods used before attack



Methods used to recover data



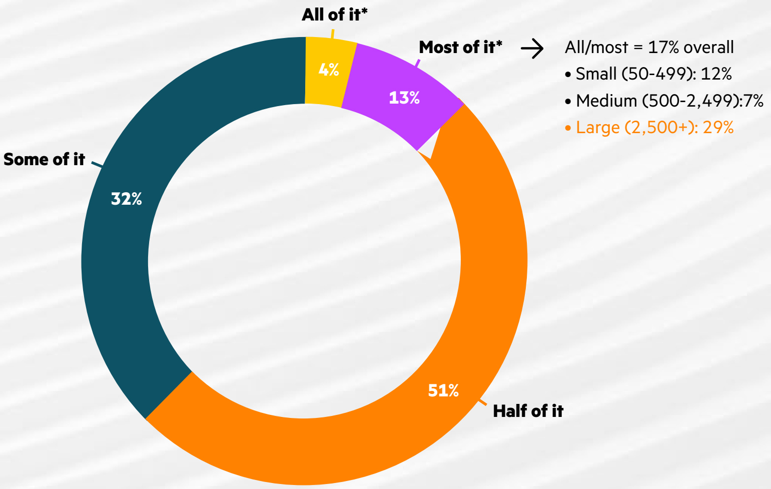
Hewlett Packard
Enterprise

FUJIFILM

Q20: Which of the following backup methods were you using before the ransomware attack? N: 152
Q26: Which of the following methods did you use to recover your data? N: 131

Ransomware attacks threaten a significant amount of company data, especially among large businesses

Proportion of mission critical data threatened



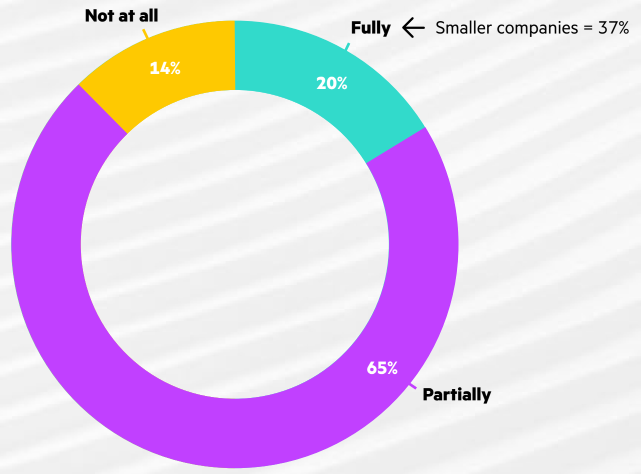
All/most = 17% overall

- Small (50-499): 12%
- Medium (500-2,499):7%
- Large (2,500+): 29%

Q14: What proportion of your on-premise data is mission critical?
By mission critical, we mean you would need urgent access/recovery to it following a ransomware attack. N: 152

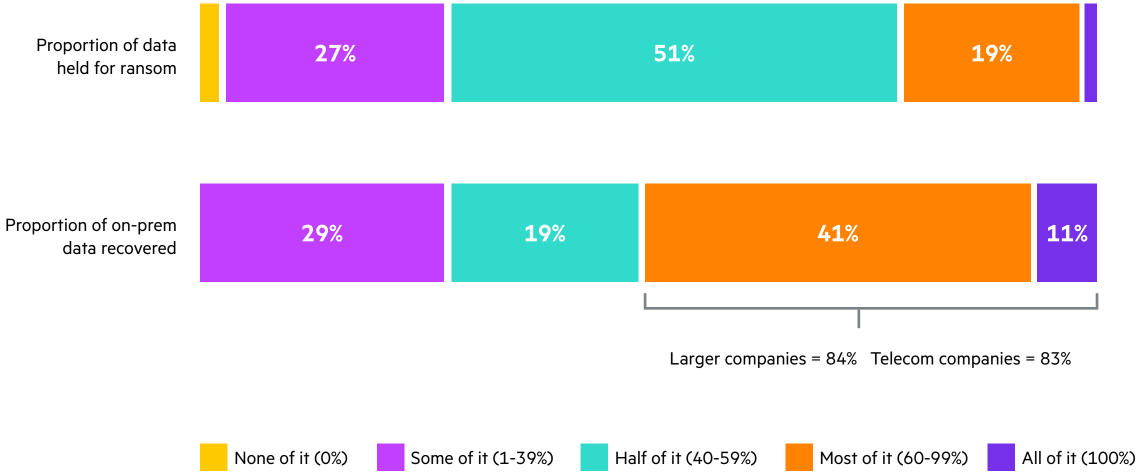
Most attacks are partially or fully successful, especially among smaller businesses

Attack ‘success’



Q21: To what extent was the attack successful? N: 152

And as a result, around half of data can be held to ransom, although most of it gets recovered

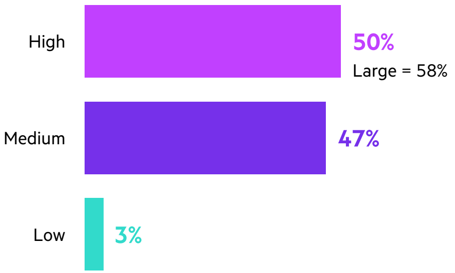


Larger companies = 84%   Telecom companies = 83%

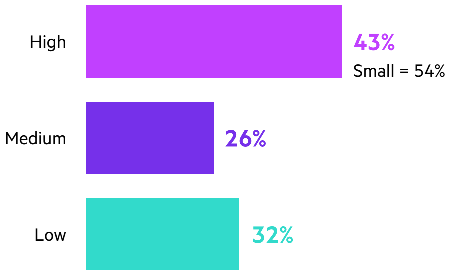
Q23: What proportion of your data was held for ransom? N: 131
Q25: What proportion of your on-premise data was recovered? N: 131

Despite all this potential risk, many are confident of their defenses and aren't prioritizing improving them

Level of confidence in cybersecurity defenses



Priority to improve ransomware defenses



Hewlett Packard Enterprise | FUJIFILM

Q17: What level of confidence does your organization have in its current cybersecurity defenses? N: 152
Q18: How much of a priority is it for your organization to improve its ransomware defenses? N: 152

High priority

"It will close down function for a few hours, **lowering profits and vital working systems, and will take days to go back up and work normally,** losing money just to secure data."

"Security is of high importance. **We would lose a lot of market credibility** if we had a highly publicized successful attack."

"The day-to-day operations of the business **would be crippled without access to accurate financial records** such as receivables, payables, and payroll records."

"We have a lot of sensitive information on our database, and **we can't afford to lose it."**

Low/medium priority

"Our **security systems are solid,** and we are **constantly updating our software and tools."**

"Our organization **has automated threat detection** in place to increase our chances of protection."

"We **have an offline database of all records,** so it is a low priority."

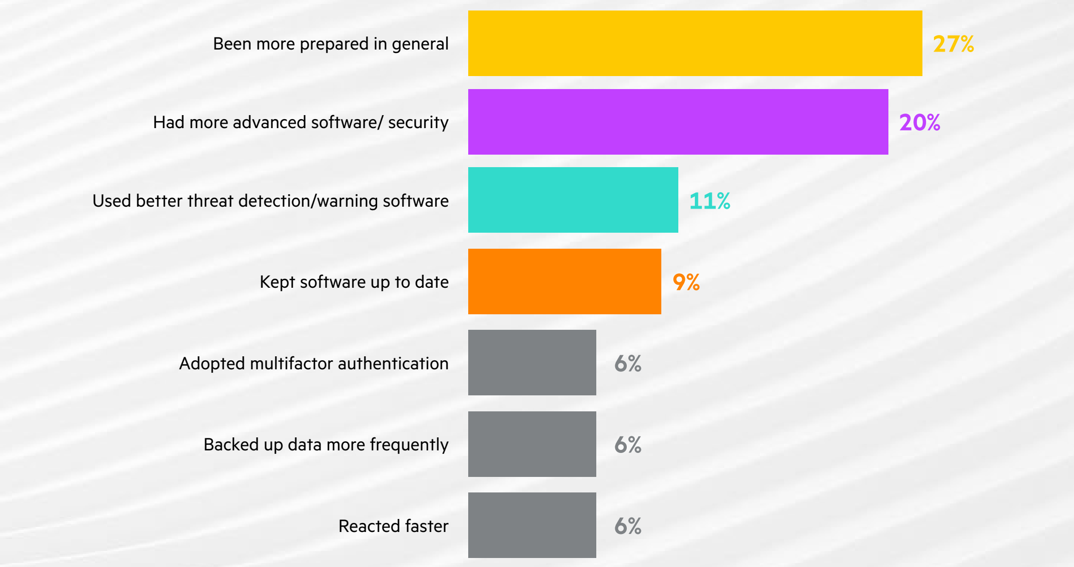
"We **have good existing measures in place,** but there is still some room to improve."

"We are pretty confident in what we have now, but also realize things change quickly and **we want to be prepared."**

Q19: You mentioned that it is a (high/medium/low) priority. Why is that? N: 152
Q18: How much of a priority is it for your organization to improve its ransomware defenses? N: 152

When they reflect on what went wrong in their past attack, they often focus on the role of software/ processes, not hardware/tape

What they could have done differently to get a better outcome



Q30: What could have you done differently to get a better outcome? N: 44

Hewlett Packard Enterprise | FUJIFILM

“We **should have implemented something way earlier.”**

“Used **more advanced software.”**

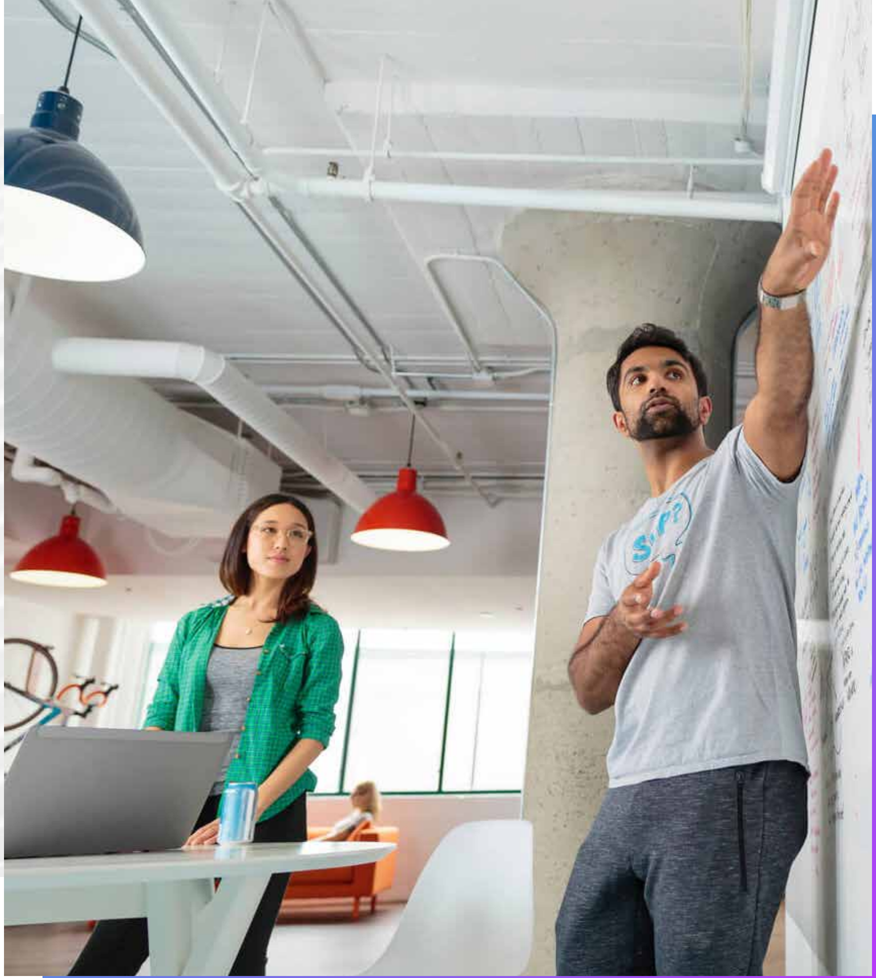
“Security tools need to be enhanced to provide
a **better warning at the time of the attack.”**

“Could have **kept our software up to date** and
can also use **better threat detection.”**

“For better results, we can **embrace multifactor authentication**
for our users and **maintain our software updates.”**

“Secure systems before, **backup data
to cloud** more frequently.”

“We needed **more security and faster responding.”**

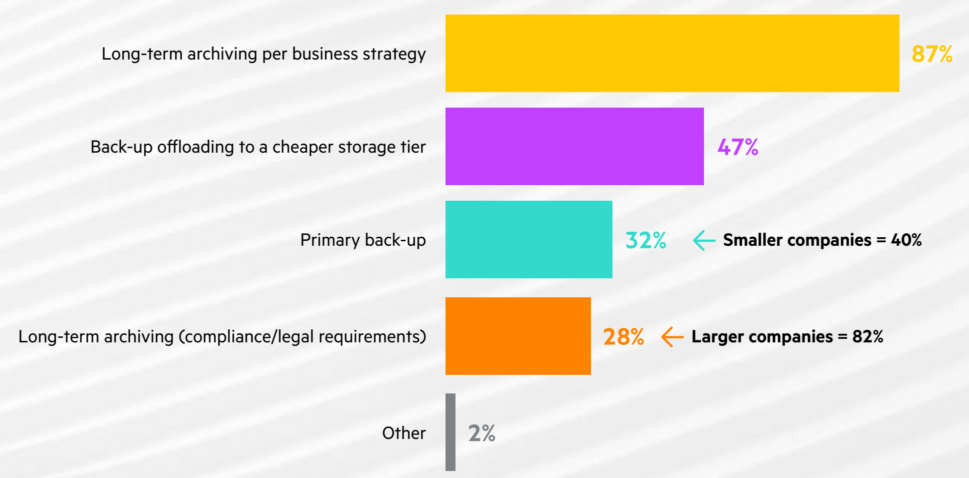


Q30: What could have you done differently to get a better outcome? N: 44

Hewlett Packard Enterprise | FUJIFILM

Current tape users tend to leverage tape for its archival role but also for backup applications

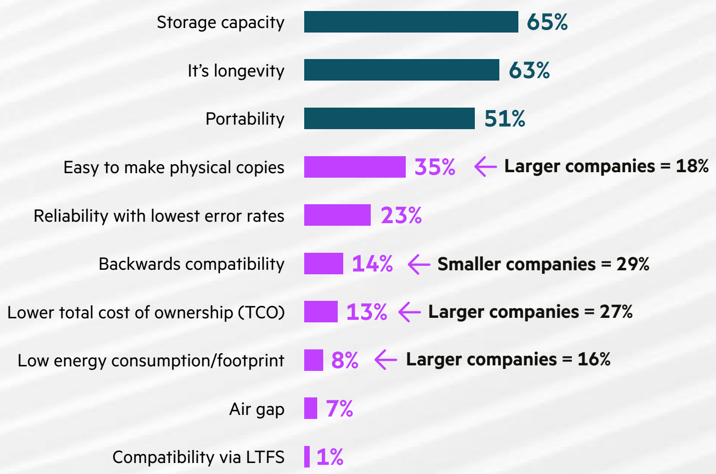
Reasons for using tape storage



Q34. What are the main reasons that your organization uses tape storage? N: 60

And while decision-makers are aware of many of tape's strengths, the benefit of air gap is yet to be fully realized

Perceived benefits of tape storage



Q35: What do you see as the main benefits of tape storage? N: 152

“Unlike other storage options, tape storage is **longer lasting and more reliable.”**

“Tape storage has the **lowest error rates**, which makes **it more reliable and protects our data from attacks** far more than other storage devices.”

“For the **prevention of further ransomware attacks** and for **keeping all our important data safe and secure.”**

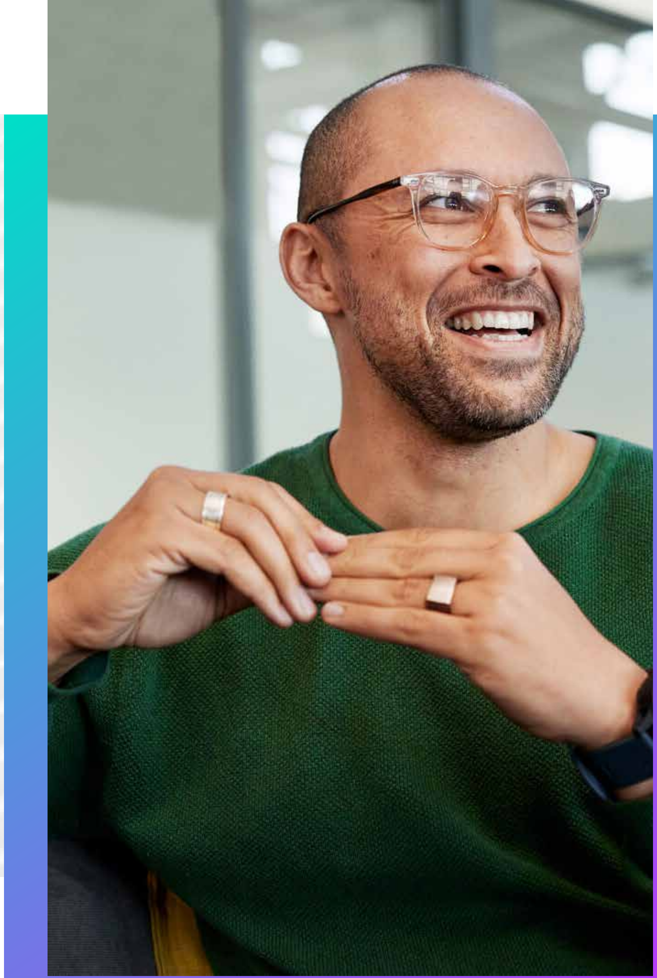
“To provide **additional security,** and it is **easy to make physical duplicates** for our day-to-day activities.”

“To **keep data more safe and secure,** and also they **provide high storage capacity.”**

“Tape storage is the **most secure** and easy way to **protect the data from future attacks.”**

“Their **low cost and improved portability** would be the primary reasons for choosing them.”

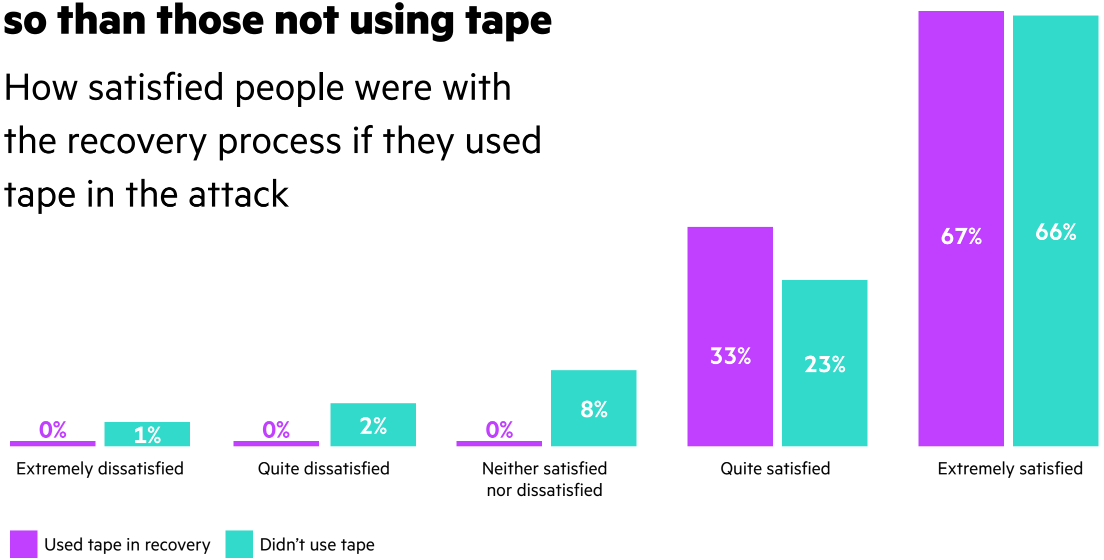
“In comparison with cloud backups, tape storage is **more cost-effective.”**



Q30: What could have you done differently to get a better outcome? N: 44

And those using tape in the recovery process were extremely satisfied with it, even more so than those not using tape

How satisfied people were with the recovery process if they used tape in the attack



Hewlett Packard Enterprise | FUJIFILM

Q29: How satisfied were you with the outcome of the recovery process? N: 131

Key Statistics

68%

of businesses say that the majority of their on-premise data is mission critical.

86%

of businesses who've experienced a ransomware attack in the last two years say that it was partially or fully successful and required recovery.

29%

of businesses who've experienced a successful ransomware attack say that they recovered less than half their data.

49%

who've experienced a successful ransomware attack say it took longer to return to normal than they can survive without mission critical data.

55%

of businesses who've experienced a ransomware attack in the last two years didn't add any new technologies to their ransomware defenses.

100%

of businesses we spoke to who'd used tape to recover their data without a ransom said that tape played a significant part in them not needing to pay the ransom.

100%

of businesses who used tape to recover their data were satisfied with the outcome of the recovery process (compared to 89% of businesses who didn't use tape). 67% were extremely satisfied.

Hewlett Packard
Enterprise

FUJIFILM

Hewlett Packard
Enterprise

FUJIFILM

adience

www.adience.com