Understanding the Security and Data Backup Market for Managed Service Providers (MSPs)

Survey of MSPs in UK and US serving SMB customers and understanding the security and data backup market opportunity

Sponsored By

Acronis

April 2020

Roy Illsley
Distinguished Analyst
roy.illsley@omdia.com

Brought to you by Informa Tech

OMDIA

Table of Contents

Executive Summary

Methodology

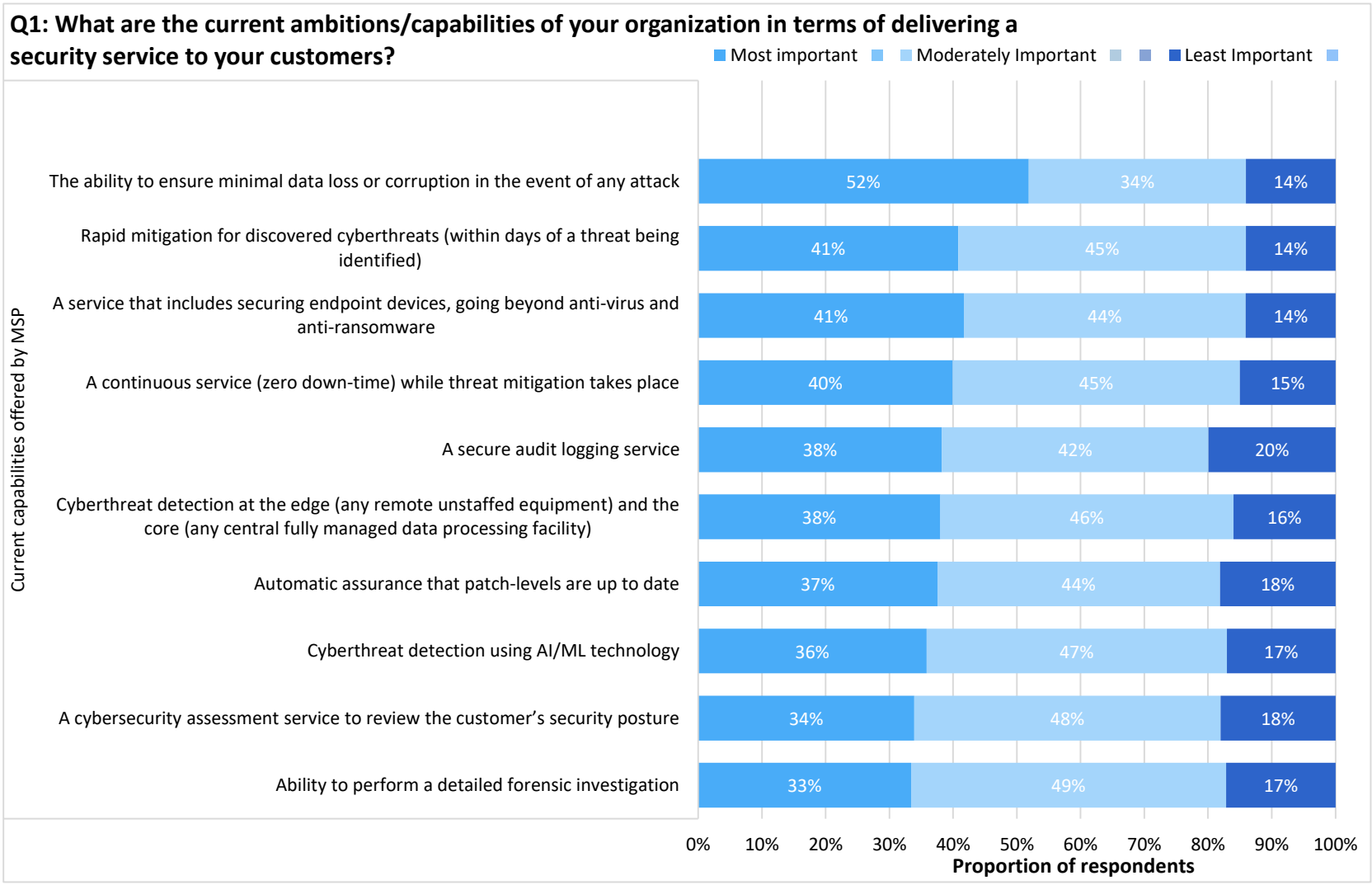
- Omdia (formerly known as Ovum) conducted an Acronis-sponsored survey of 263 MSPs in UK and US that serve SMB customers (61% US, 39% UK)
- Focused on MSPs that do not use open source technologies.
- Focused on MSPs that either deliver or are planning to deliver security and backup capabilities.

Highlights of Results

- Security is the most requested new service that customers want from MSPs.
- The needs of MSPs vary by the size and scope of their operations, with pricing being particularly sensitive. Those working globally rate this more than twice as much of a problem as those with operations in country only.
- Minimizing data loss is the clear top concern. Securing endpoint devices is the fastest growing security concern, and for backup ransomware protection. These indicate customers are looking more broadly at where threats are coming from.
- Lack of skills is the most common business challenge faced by all MSPs.
- Top US obstacle is managing the technology efficiently. Top UK and #2 US obstacle is pricing the service correctly. Joint #3 is having sufficient time and resources.
- When selecting a data protection provider MSPs put 'having everything under our control' as top capability, 56% rated it as important.
- Remaining current in terms of threats was top process challenge faced by MSPs when delivering security management as a service, 55% rated it important.
- Early identification and encryption as default were the top two technical challenges faced by MSPs in delivering security management as a service.
- US customers top business requirement was to deliver the same or better quality of service. UK customers put delivering security but not interfering with business operations.
- Ability to identify security threats fast is stopping MSPs from meeting the customer's requirements.

Download the full 45-page report HERE

Most Important Existing Capabilities for Delivering Managed Services



Top 3 Current Capabilities (Top 2 answers combined)

1. *Data loss prevention*
2. *Securing end points beyond anti-virus and anti-ransomware*
3. *Rapid mitigation*

US vs UK Differences

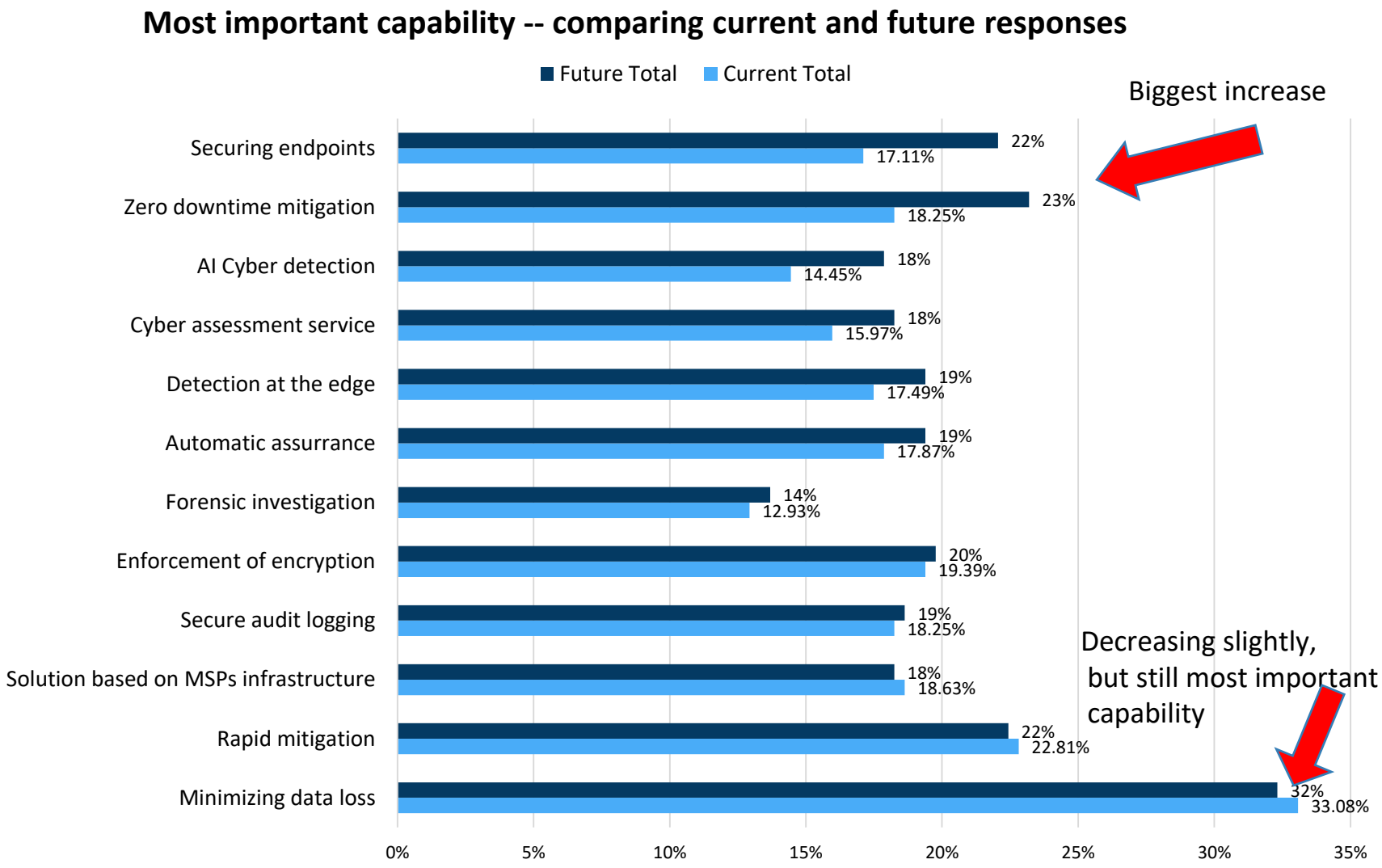
- ***Minimizing data loss*** is nearly 20% more important in US than in UK.
- ***Rapid mitigation*** is more important to US MSPs than UK MSPs, with more than 10% difference

Vertical Highlight

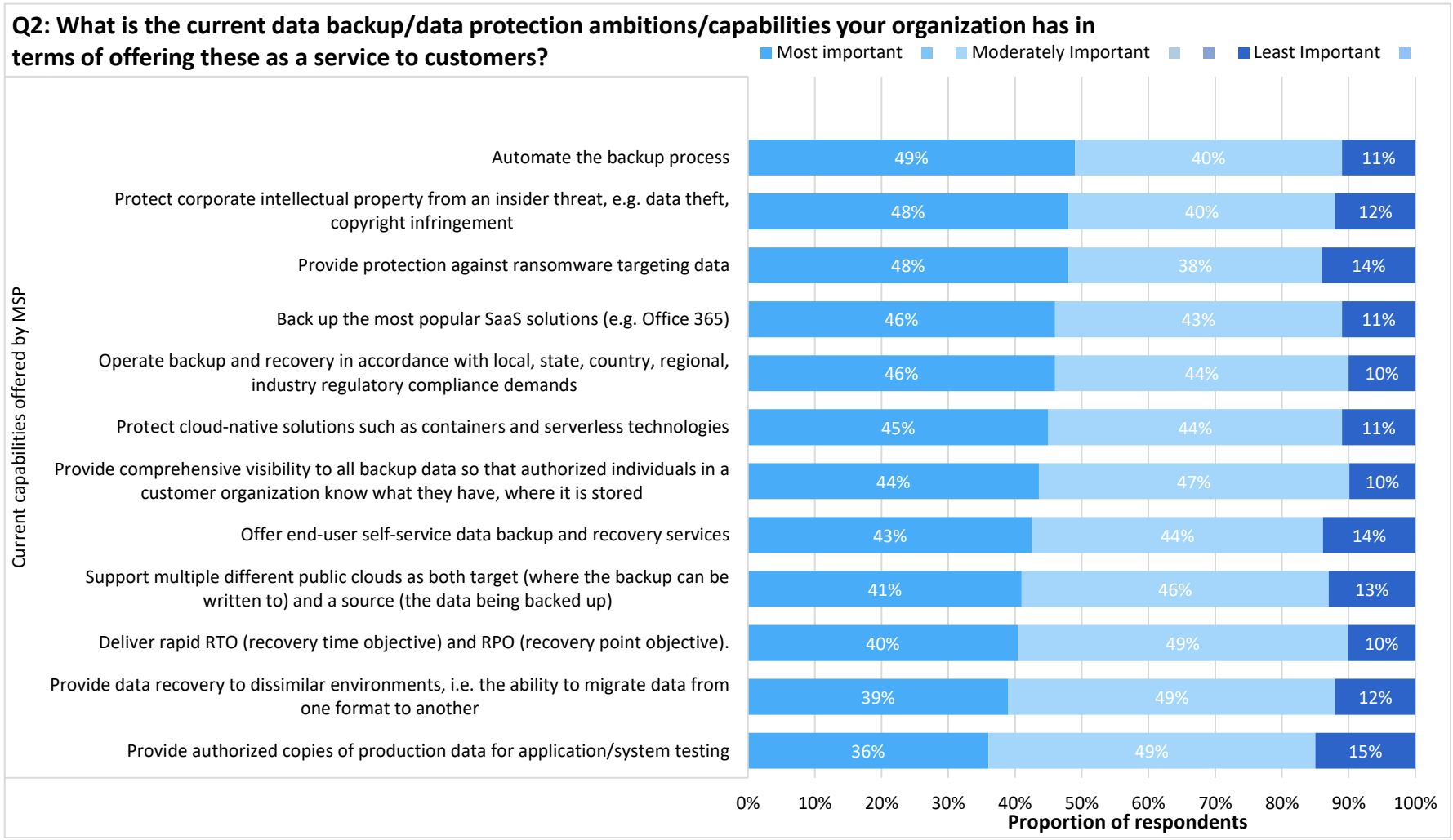
- 63% of MSPs indicated their Manufacturing clients cared the most about data loss which was even greater than Banking

Differences between current and future security capabilities

- ***Securing endpoints*** shows the biggest increase in interest from current to future security capabilities
- ***Zero downtime mitigation*** shows second biggest increase in interest, with ***AI cyber detection*** with third biggest increase
- ***Minimizing data loss*** remains top capability but shows slight decline in interest – probably not much to read into this as it is such a clear top topic of interest.
- ***Rapid mitigation*** was the second capability to show a decline of interest from current to future, but again unlikely enough to be of significance



Most Important Existing Capabilities for Delivering Backup and Data Protection Services



Top 3 Current Capabilities (Top 2 answers combined)

1. *Automate the backup process*
2. *Protection against ransomware*
3. *Protect corporate IP*

US vs UK Differences

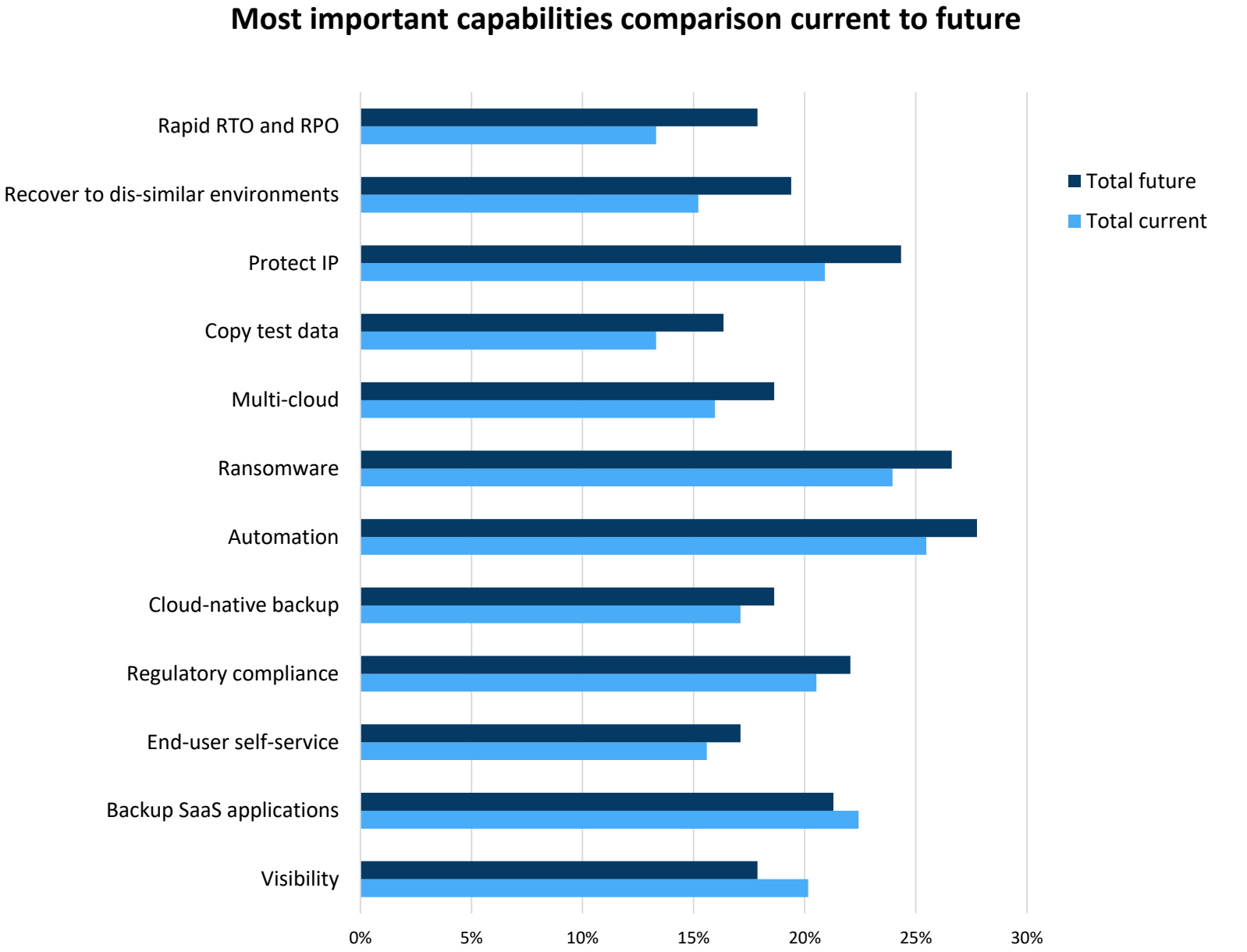
- ***Protection from ransomware*** was seen as less important in the UK than the US (41% vs 52%)

Vertical Highlight

- MSPs indicated their Hospitality clients cared the most about Automation (64%)

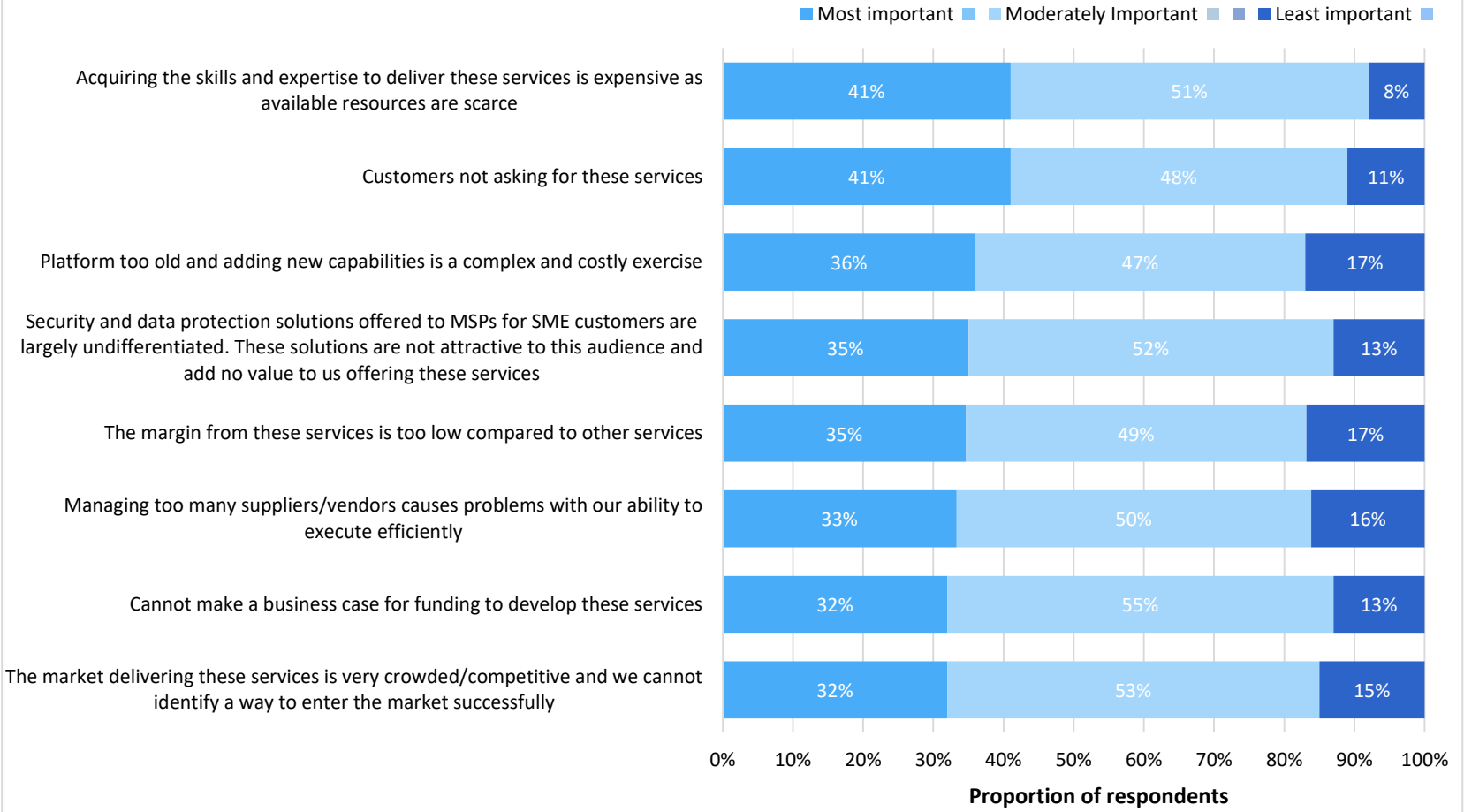
Differences between current and future backup capabilities

- ***Protection against ransomware*** becomes the most important capability
- Biggest growing capability of interest is ***rapid RTO and RPO***, which shows a 5% increase in MSPs putting it as most important – organizations are recognizing that speed and completeness of protection is important.
- Second biggest growing capability of interest is ***recover to dissimilar hardware environments***, which shows a 4% increase in MSPs putting it as most important.
- Only 2 capabilities show a decline in interest; ***visibility*** and ***backup of SaaS applications***



Key Business Obstacles Preventing MSPs from Executing

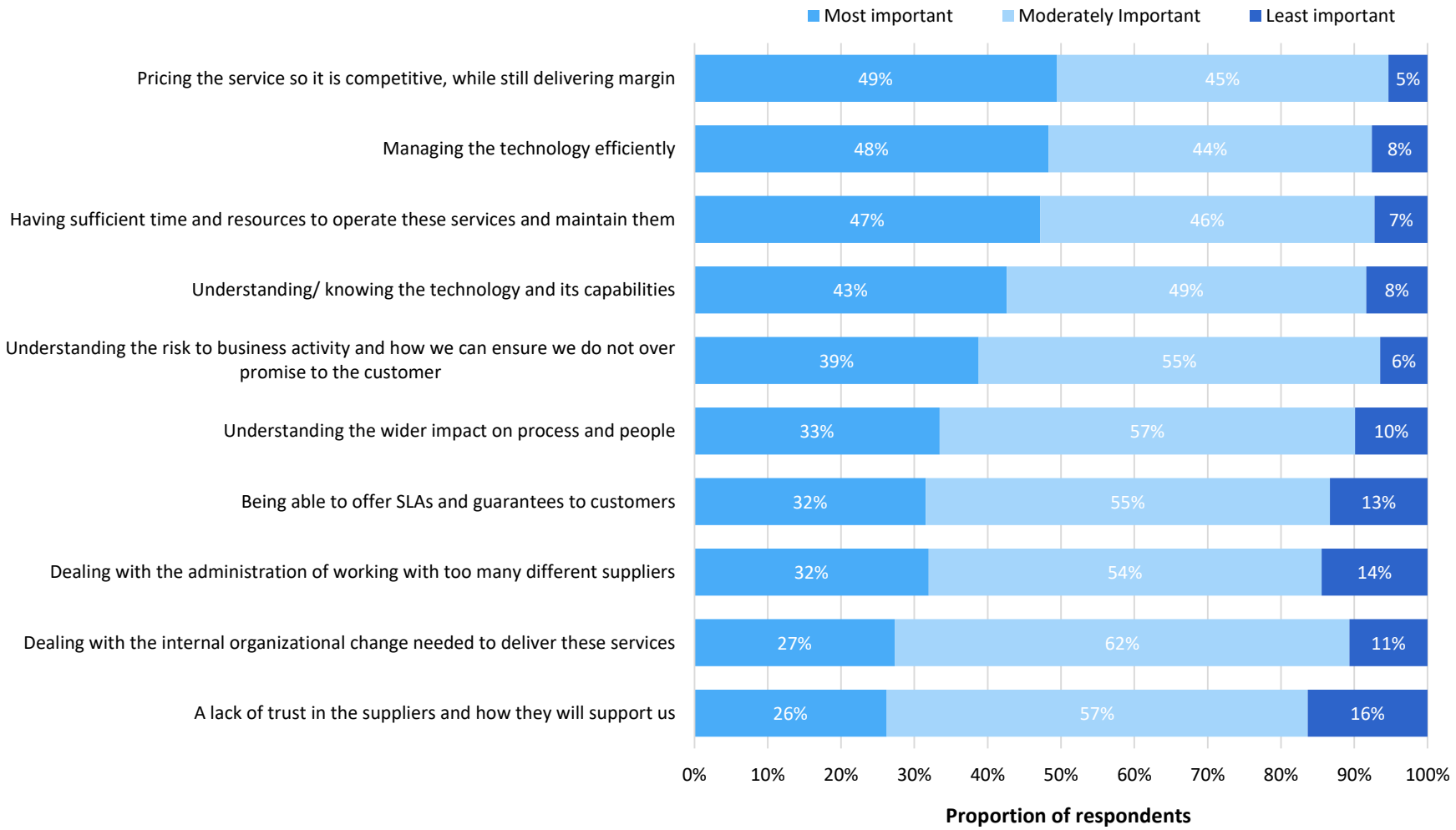
Q3: What are the key business obstacles preventing you from offering/ or successfully delivering security services and/or data backup/data protection capabilities?



- ***Lack of skills*** was most common obstacle irrespective of MSP size; in fact it was the top response in all size groups. It also shows the biggest variance between most and least important, demonstrating that the skills shortage is a real concern for MSPs
- ***Lack of skills*** more of a challenge in UK than US – likely due to Brexit and the uncertainty about the status of EU workers living in UK
- ***Managing too many suppliers*** is more a challenge in UK than US; however, in 50-99 employees MSPs this was #2 most important – 22% citing it as a problem
- Responses varied markedly by size of MSP – as such, no one size solution will meet all needs

Key Organizational Obstacles Preventing MSPs from Executing

Q6: What are the main organizational obstacles to delivering data protection and security services?



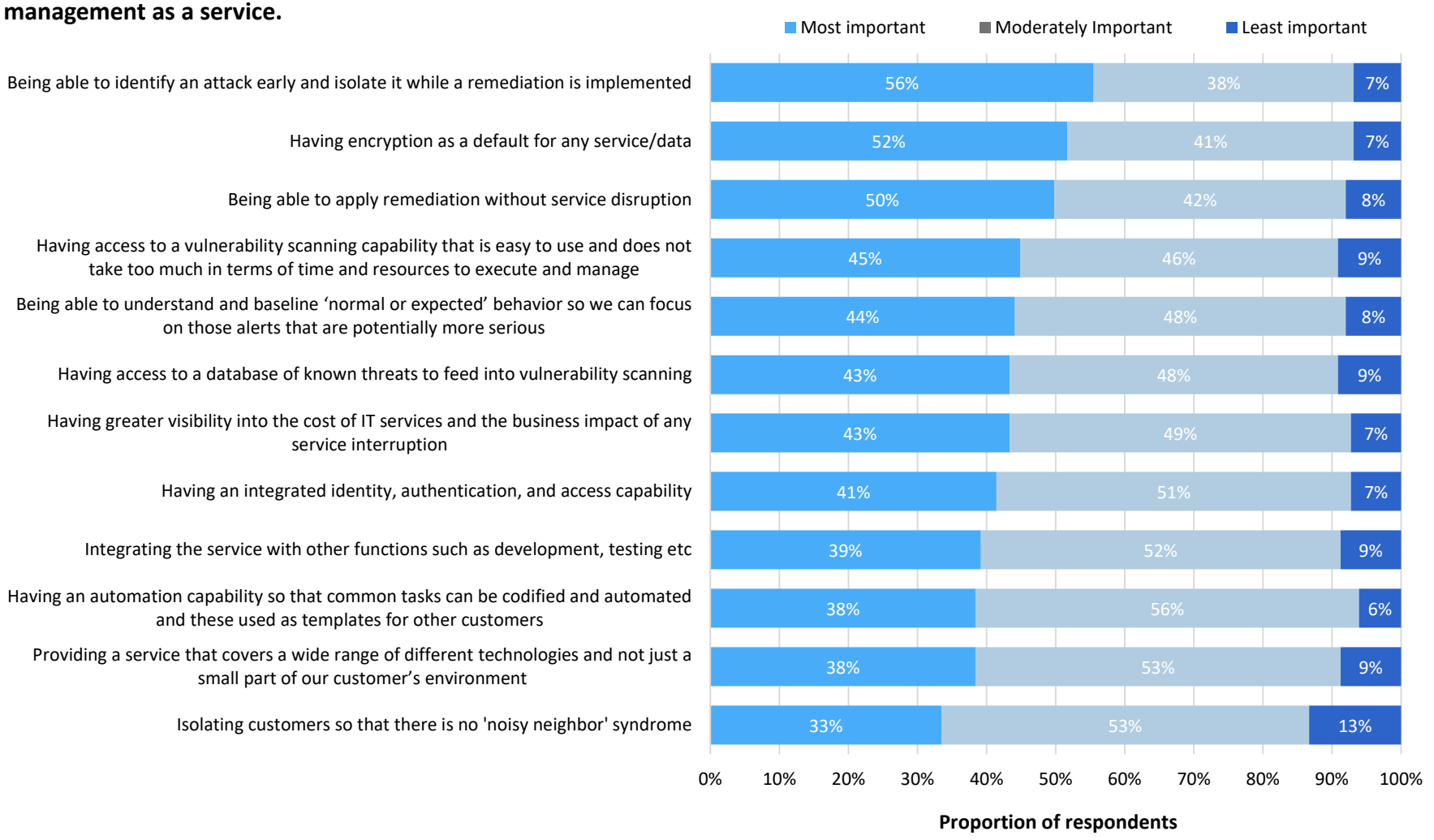
Top 3 (combining top 2 answers)

1) Pricing the service
2) Managing technology efficiently
3) Having time and resources to operate and maintain the services

- For MSPs with less than $1M in revenue, ***managing the technology efficiently*** was rated the biggest obstacle listed
- Those MSPs operating in two or more regions put ***pricing the service*** as most important – 36% of respondents – whereas only 18% of those MSPs operating in one country have ***pricing the service*** as most important – seemingly pricing in more than one currency is a challenge

Key Technical Challenges Preventing MSPs from Executing

Q9: Please rate the technical challenges you perceive/have experienced in delivering security management as a service.



Top 3 Technical Challenges (top 2 answers combined)

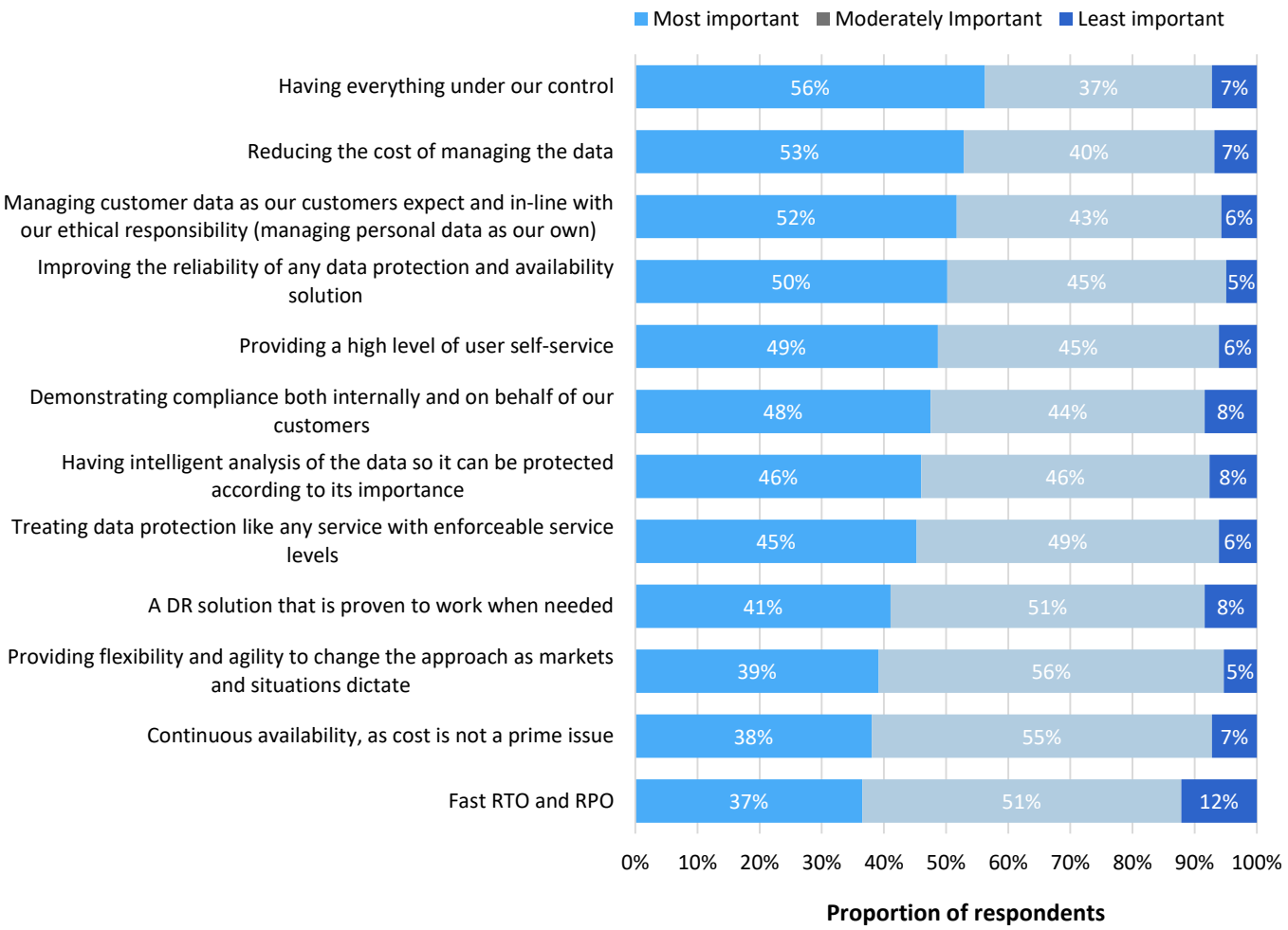
1) Early identification and isolation (56%)
2) Encryption as a default (52%)
3) Apply remediation without service disruption (50%)

US vs UK Differences

- UK MSPs place a ***database of known threats*** as the only technical challenge where it is more important than US MSPs
- Top UK technical challenge is ***encryption by default*** with 27% putting as most important
- ***Broad coverage of technologies*** is the technical challenge with the biggest difference between UK and US responses

Most Important Considerations When Deciding on a Supplier

Q7: Which of the following are the most important considerations in your organization's decisions on a data protection and availability supplier?



Top 3 Most Important (Top 2 answers combined)

1) Having everything under our control
2) Reducing cost of managing data
3) Managing data ethically (as if our own)

US vs UK Highlight

- In US ***having everything under our control*** is clearly most important(1) with over 30%, while in UK ***improving reliability*** is most important (1) with 30%

MSP Size Differences

- By MSP employee size the **1-4 employee** MSPs were most in favour with 35% putting it as most important. Only the 5-19 employee MSPs did not put as the top response in most important category.
- MSPs with 5-19 employees put ***cost reduction*** across all markets most important consideration with 28%
- ***Managing data like it is our own*** is more significant to smaller MSPs. 1-4 employees put it second most important with 30% compared to 24% in the 100-499 employee MSPs

Thank You!

[Download the full 45-page report HERE]

Sponsored By

Acronis

Learn more about Acronis Cyber Protect Cloud, the AI-powered integration of data protection and cybersecurity.

OMDIA