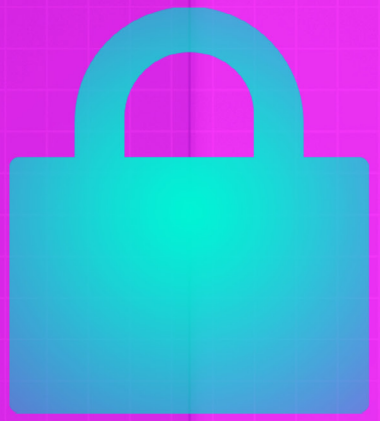
eBook

datto
A Kaseya COMPANY



Datto SMB Cybersecurity for MSPs Report

A world of opportunity for MSPs

Small and midsize businesses (SMBs) face mounting cybersecurity challenges resulting in many SMBs increasing their commitment to security and their security budgets. There's room for MSPs to realize revenue growth in many areas including secure identity and access management, endpoint security, business continuity and disaster recovery (BCDR) and phishing protection. Today's world of growing cyberthreats for SMBs is a world of increasing security business opportunities for MSPs everywhere.

We spoke to 2,913 IT decision makers to learn about their security concerns, and we're sharing that data with you to help you grow your MSP.

7 Key Takeaways

IT professionals are concerned about security and ready to make investments to keep their organizations safe.

SMBs continue to experience significant security challenges and they recognize that they need to spend to solve them, with about half of our survey respondents planning to spend on email security, backup and antivirus protection.

Many SMBs need help preparing to recover from security incidents.

More than half of our survey respondents admitted that a successful phishing attack or even worse, a ransomware attack, would seriously wound their organization with some saying that it could be a fatal blow.

Few SMBs are cutting back on security spending, instead they're investing in security.

Four in 10 of our survey respondents said that their organization is increasing their cybersecurity spending, and most expect that to continue – excellent news for MSPs on today's challenging economy.

Phishing is the biggest security woe that SMBs face.

Business IT leaders are worried about phishing and the danger it brings in its wake. This creates revenue growth possibilities for MSPs around email security and security training with phishing simulations.

Downtime is costly, but many businesses don't have the right tools in place to minimize it.

MSPs have a golden opportunity to expand revenue and help their customers reduce expensive downtime with solutions like BCDR, managed SOC and incident response planning.

SMBs tend to rely on outsourced IT security.

Businesses need outside help to maintain and enhance their security, and almost half of the IT professionals that we surveyed said that their organization relies on an MSP or MSSP to get the job done.

A solid number of SMBs are not happy with their current defensive buildouts.

One-third of our respondents said that they're unhappy with their current array of security solutions, indicating there's room for MSPs to maneuver in the market.

Cybersecurity frameworks

NIST is not the most popular framework

Zero-trust is highly recommended by experts but only 14% of respondents said that their organizations use that framework and just 7% were concerned with it, leaving plenty of room for growth (and opportunity for MSPs) in this area.

Framework or Regulation	Level of Use	Level of Concern
CIS	34%	26%
CMMC	30%	26%
COBIT	27%	23%
NIST	22%	19%
ISO 27001	21%	15%
NCSC (National Cyber Security Centre)	18%	20%
HIPAA	18%	13%
Zero Trust	14%	7%
ASD Essential 8	14%	13%
PCI-DSS	12%	10%
SOC II	11%	7%
MITRE ATT&CK	9%	9%
Other	5%	N/A
None	3%	27%

CIS and CMMC are most frequently used and the most concerning cybersecurity frameworks.

SMBs are being proactive about assessing vulnerabilities

The majority of SMBs in all regions are interested in keeping an eye on their IT security vulnerabilities in such a volatile cybercrime climate. That makes them especially keen on user-friendly solutions that make the vulnerability assessment process quick and easy.

Frequency of Assessments	Responses
More than 4x year	13%
3–4x per year	24%
Twice per year	25%
Once per year	21%
Once every 2–4 years	12%
Once every 5 years or longer	3%
Never	1%
Don't know	2%

Over one-third of respondents run IT security vulnerability assessments three or more times per year.

SMBs aren't cutting back on security spending; budgets are rising instead

In the face of rising cybercrime rates and a growing awareness of the damage a cyberattack can do by non-tech decision-makers, IT security budgets have increased in the past year. SMBs are optimistic about them remaining steady or rising in 2023. This offers MSPs the opportunity to encourage customers to make comprehensive security improvements and upgrades.

IT Budgets	Responses
Increased	42%
Stayed the same	40%
Decreased	6%

Four in 10 (42%) of survey respondents reported a boosted IT security budget this year.

Security is a hefty chunk of most IT budgets

SMBs have money to spend on security

% of total IT budget	Responses
Less than 1%	1%
1% –5%	10%
6% –10%	19%
11%–15%	19%
16%–20%	20%
21%–30%	15%
31%–40%	8%
41% –50%	5%
More than 50%	3%

Almost one-third of SMBs devote 20% to 50% of their IT budget to security.

SMBs are in the market for IT security help

While many SMBs manage security internally, there are plenty of businesses looking to MSPs and MSSPs for their IT security needs. The tech talent shortage is a contributing factor, but lack of expertise is also an important motivator for businesses to outsource their tech work. MSPs can benefit from positioning themselves as knowledgeable, up-to-date experts for clients and prospects.

One in four outsource their security to an MSP, and one in six to an MSSP.

Who manages your IT security?	Responses
Partial internal IT	47%
Dedicated internal IT	50%
Individual outsource IT	28%
Company outsource IT that is IT service provider or MSP	26%
Company outsource IT that is an MSSP	16%
Company outsource IT, but not sure what type it is considered to be	5%

There's room for MSPs to maneuver in the market

Only 31% of respondents tell us that they're completely satisfied with their security solutions, creating opportunities for MSPs to grow.

Satisfaction Level	Responses
Completely satisfied	31%
Somewhat satisfied	54%
Neutral	12%
Somewhat dissatisfied	2%
Completely dissatisfied	1%

Only 54%

of businesses are somewhat satisfied with their security solutions.

Most businesses have absorbed the message that a recovery plan is a business essential

When it comes to having a recovery plan in place, over half of respondents said that they have a standard recovery plan ready to go. However, some businesses still need serious help making a recovery plan, creating opportunities for MSPs to help them be ready for trouble. That's also a ripe opportunity for MSPs to guide clients into investing in the resources they'll need to enact that plan, like BCDR or remote identity and access management tools.

Eight in 10 survey respondents (81%) said that their company has a recovery plan in place.

Recovery Plan Status	Responses
We have a best-in-class recovery plan in place	29%
We have a standard recovery plan in place	52%
We have solutions to protect us, but do not have a formal recovery plan in place	14%
We do not have any recovery plan in place	2%
I believe my service provider has a recovery plan in place, but I do not know the details	3%

Security products

A strong defense against ransomware leads the SMB priority list

In the ransomware era, it's no surprise that antivirus software (57%) and email security (53%) are at the top of businesses' implementation lists.

The security solutions that organizations are implementing over the next 12 months

Solution	Respondents
Antivirus software	57%
Email /spam protection	53%
File backup	49%
Managed firewall	49%
Cybersecurity training for employees	43%
Identity and access management	38%
Security operations center	28%
Managed detection and response	27%
Business continuity & disaster recovery (BCDR)	27%
Incident response	27%
Endpoint detection and response	25%
Automated software patching	25%
Mobile management platform	23%
Threat hunting	20%
Pentesting	14%
Forensics	12%

Only 43% of respondents conduct security awareness training.

SMBs are ready to invest in the cloud

The cybercrime surge in the last few years has businesses ready to invest in cloud security.

Top IT security areas SMBs plan to invest in the next 12 months

Area of Investment	Response
Network security	47%
Cloud security	45%
Cyber insurance	36%
Email/ collaboration tools security	29%
Endpoint security	27%
Vulnerability assessment	26%
Business continuity & disaster recovery (BCDR)	25%
Don't know	5%

Network security and cloud security are the top areas planned for investment in 2023.

Cyber threats

SMBs have a wide array of security woes

A look behind the curtain at the factors SMBs blame for their security problems can help you speak to their pain points confidently.

Main reasons SMBs feel they have had cybersecurity issues

Issue	Response
Phishing emails	37%
Malicious websites/web ads	27%
Weak passwords/access management	24%
Poor user practices/gullibility	24%
Lack of end-user cybersecurity training	23%
Lack of administrator cybersecurity training	19%
Phishing phone calls	19%
Lack of defense solutions (antivirus)	19%
Insufficient security support for different types of user devices	18%
Outdated security patches	18%
Lack of funding for IT security solutions	17%
Lost/stolen employee credentials	17%
Lack of executive buy-in for adopting security solutions	16%
Open remote desktop protocol (RDP) access	15%
Shadow IT	13%

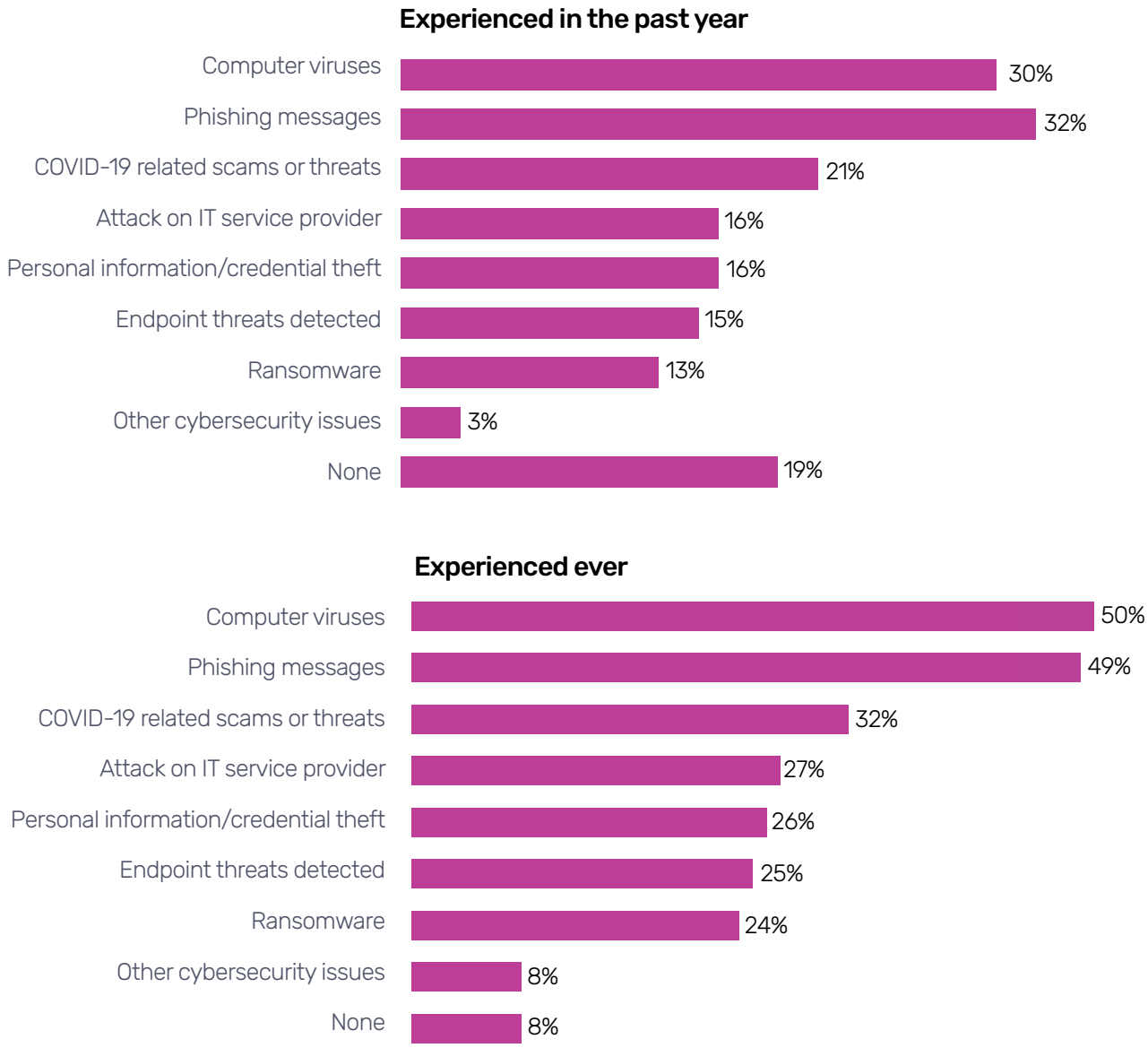
Around 42% of SMBs blame their security issues on lack of training.

SMBs are plagued by phishing

Many of our respondents saw phishing as the prime suspect for security issues, and more than one-quarter of respondents have experienced an attack on their IT service provider (16% in the past year). This is an opportunity for MSPs to provide highly secure service.

Cybersecurity issues that have affected SMBs business in the last 12 months.

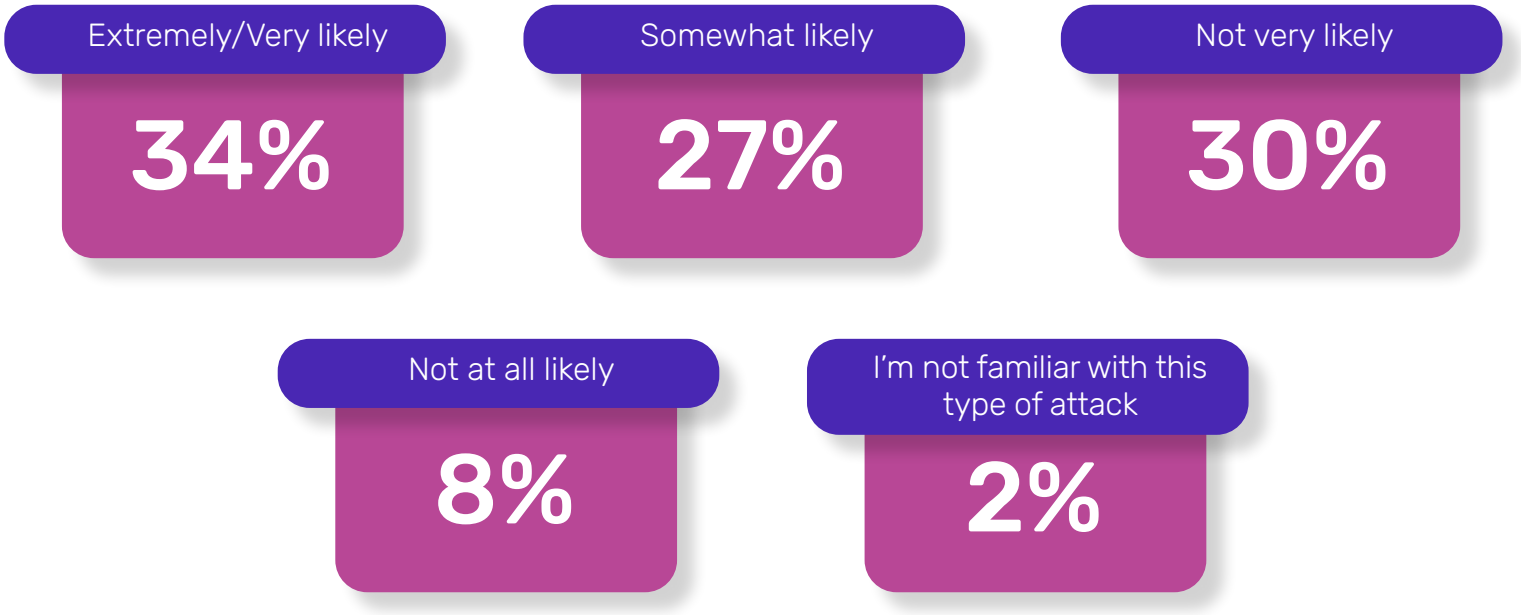
Almost one-third of respondents dealt with phishing and viruses last year.



Almost three-quarters of companies say that a ransomware attack would be a death blow

Businesses know that a ransomware attack could destroy them, and they're looking for ways to prevent it.

About 60% of respondents felt their organization might be hit by a successful ransomware attack in the next 12 months.



Around 70% of SMBs admitted that the impact of a ransomware attack would be extreme or significant.

Extreme impact - it would be difficult to recover

17%

Significant impact

53%

Minimal impact

28%

No impact

3%

Ransom demands vary widely

Presenting clients and prospects with a clear picture of the ransom demand they could face may help them wrap their heads around the actual hit to their bank accounts.

Almost one-third of SMBs faced $10,000–$50,000 in ransom cost.

Ransom Amount	Response
Less than $100	2%
$100 to less than $500	4%
$500 to less than $1,000	10%
$1,000 to less than $5,000	21%
$5,000 to less than $10,000	25%
$10,000 to less than $25,000	20%
$25,000 to less than $50,000	11%
$50,000 or more	6%

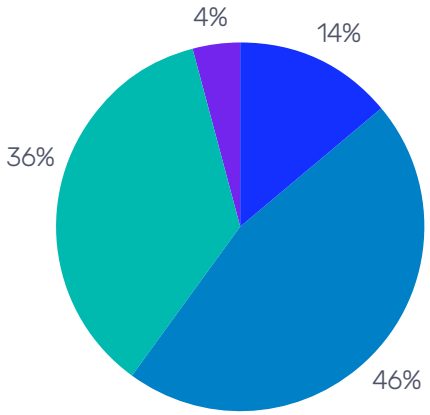
Most SMBs expect to be phished

Just under three-quarters of respondents think it's likely that their organization will experience a phishing attack in the next year, and here, too, they're looking for ways to mitigate that risk.

Around 72% of respondents expect a phishing attack in the next year.

Likelihood	Response
Extremely/very likely	41%
Somewhat likely	31%
Not very likely	22%
Not at all likely	7%

More respondents felt they'd fall victim to phishing in the next year than ransomware, but they believed that the impact of a successful ransomware attack would be greater for their organization than the impact of a phishing attack.



Almost half of respondents believe a phishing attack would have a significant impact on their business.

- Minimal Impact
- Significant impact
- Extreme impact – it would be difficult to recover
- No Impact

SMBs have faith in their ability to recover from a cybersecurity incident

Despite this confidence, there is ample opportunity for MSPs in this area to suggest new solutions to mitigate risk or upgrades to a client or prospect's security buildout to make it even stronger — 16% of respondents told us that their organization would be doomed in the event of a successful cyberattack or another damaging cybersecurity incident, and 47% said they believe recovery would be difficult.

Successful disaster recovery is easier said than done

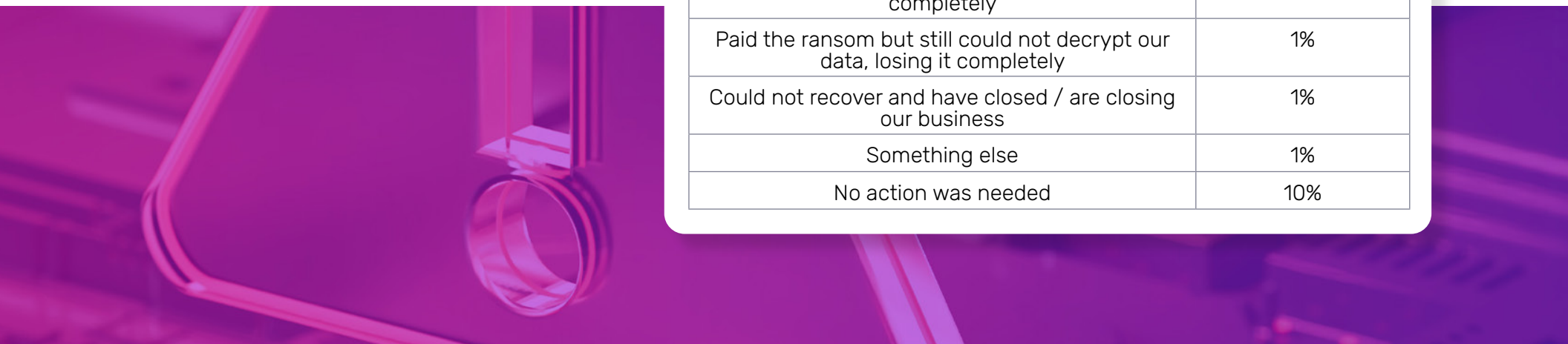
MSPs can provide SMBs with the help that they need to improve their backup and recovery processes.

One-fifth of respondents were forced to reinstall and reconfigure all systems from scratch to get back to work.

Just under half of the survey respondents (47%) said that their companies are likely to recover from a cyberattack or cybersecurity incident, but it would be painful.

Outcome	Response
Recovery would be easy	**37%**
Recovery would be difficult	**47%**
We would not recover	**16%**

Action taken to return to baseline	Response
Performed disaster recovery (DR) and restored everything from full backups	30%
Restored a portion of the systems, and reinstalled and reconfigured the rest	29%
Reinstalled and reconfigured all our systems from scratch	21%
Paid the ransom to have our data decrypted	2%
Did not pay the ransom and lost our data completely	2%
Paid the ransom but still could not decrypt our data, losing it completely	1%
Could not recover and have closed / are closing our business	1%
Something else	1%
No action was needed	10%



Downtime costs $126k on average

Downtime is an expensive problem that nearly half of our respondents contended with in the past year. The business impact and punishing expense of downtime present MSPs with a pathway to recommend solutions, like BCDR, that will reduce downtime in the case of a security incident. The cost of downtime is also a fact that can be used when talking about security awareness training and other preventative measures.

$126,000 is the average cost of the downtime, including lost revenue.

Cost of Downtime	Response
$1,000 to less than $250,000	84%
$1,000 to less than $250,000	8%
$1,000 to less than $250,000	4%
$750,000 to less than $1 million	3%
$1 million or more	1%

Manual backup is the top recovery method

Just under half of survey respondents (49%) said that their organizations relied on manual backup to recover data in their last cybersecurity incident. That means that half of the businesses we surveyed need to update to cloud backup and learn the benefits of BCDR — a big opportunity score for MSPs.

Top solutions or methods used to recover data.

Recovery Method	Response
Manual backup	49%
Copy from old systems	36%
Continuous availability	36%
Third-party BCDR	32%
Something else	11%
We didn't do anything and did not recover our data	2%
We didn't lose any data	13%

About half of SMBs that had a cybersecurity issue were up and running within a day

These days it's not if you have an incident, it's when and solutions that reduce recovery time will be appealing to businesses.

Around 45% of businesses endured more than two days of downtime.

Recovery Time	Response
None – we didn't have any downtime	12%
Less than 1 day	23%
1 day	20%
2–3 days	31%
4–6 days	10%
A week or more	3%
Don't know	1%
Prefer not to answer	1%

Cyber insurance

Most SMBs have or are in the market for cyber insurance

Respondents with cyber insurance are also likely to engage in other smart security practices. They generally have more IT support, more CSFs and more security solutions deployed. They are also more likely to have experienced a cybersecurity incident in the past.

Nearly three-quarters of respondents have cyber insurance.

A third of those without cyber insurance are highly likely to invest in it within the next 12 months.

Do you have cyber insurance?

Yes 69%

No 23%

Don't Know 8%

Likelihood	Response
Extremely/Very likely	37%
Somewhat likely	38%
Not very likely	22%
Not at all likely	4%

Survey methodology

The Datto SMB Cybersecurity Survey for MSPs Report was created from a subset of data collected in a survey of 2,913 IT decision-makers conducted in July and August 2022. Respondents were required to be an IT decision-maker at an SMB with 10–300 employees. The markets chosen for analysis were North America (U.S. and Canada), U.K., Germany, the Netherlands, Australia and New Zealand and Singapore.

datto
A Kaseya COMPANY

About Datto

Datto, a Kaseya brand, provides industry-leading cloud-based software and technology solutions delivered by managed service providers (MSPs). Datto offers Unified Continuity, Networking, and Business Management solutions and has created a one-of-a-kind ecosystem of MSP partners. These partners provide Datto solutions to over one million businesses across the globe. Since its founding in 2007, Datto continues to win awards each year for its rapid growth, product excellence, superior technical support, and for fostering an outstanding workplace. With headquarters in Norwalk, Connecticut, Datto has global offices in the United Kingdom, Netherlands, Denmark, Germany, Canada, Australia, China and Singapore. Learn more at datto.com.