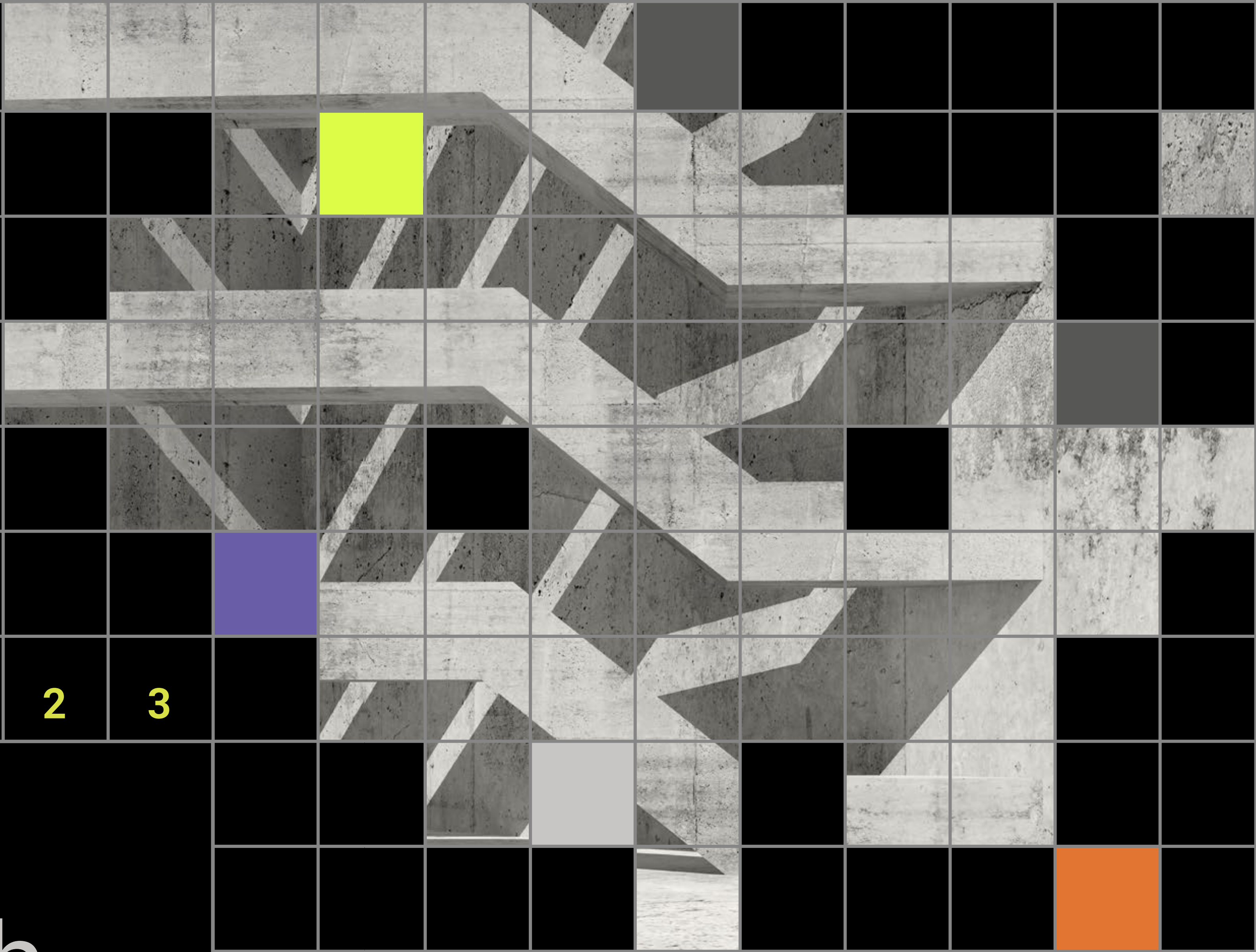
Databarracks



2023

Data Health Check

In 2023, cyber is the leading cause of IT downtime – and data loss

Last year, cyber took over as the leading cause of data loss. This year, it has also become the leading cause of IT downtime.

Now, cyber is undeniably the top concern for IT professionals from a continuity and resilience perspective.

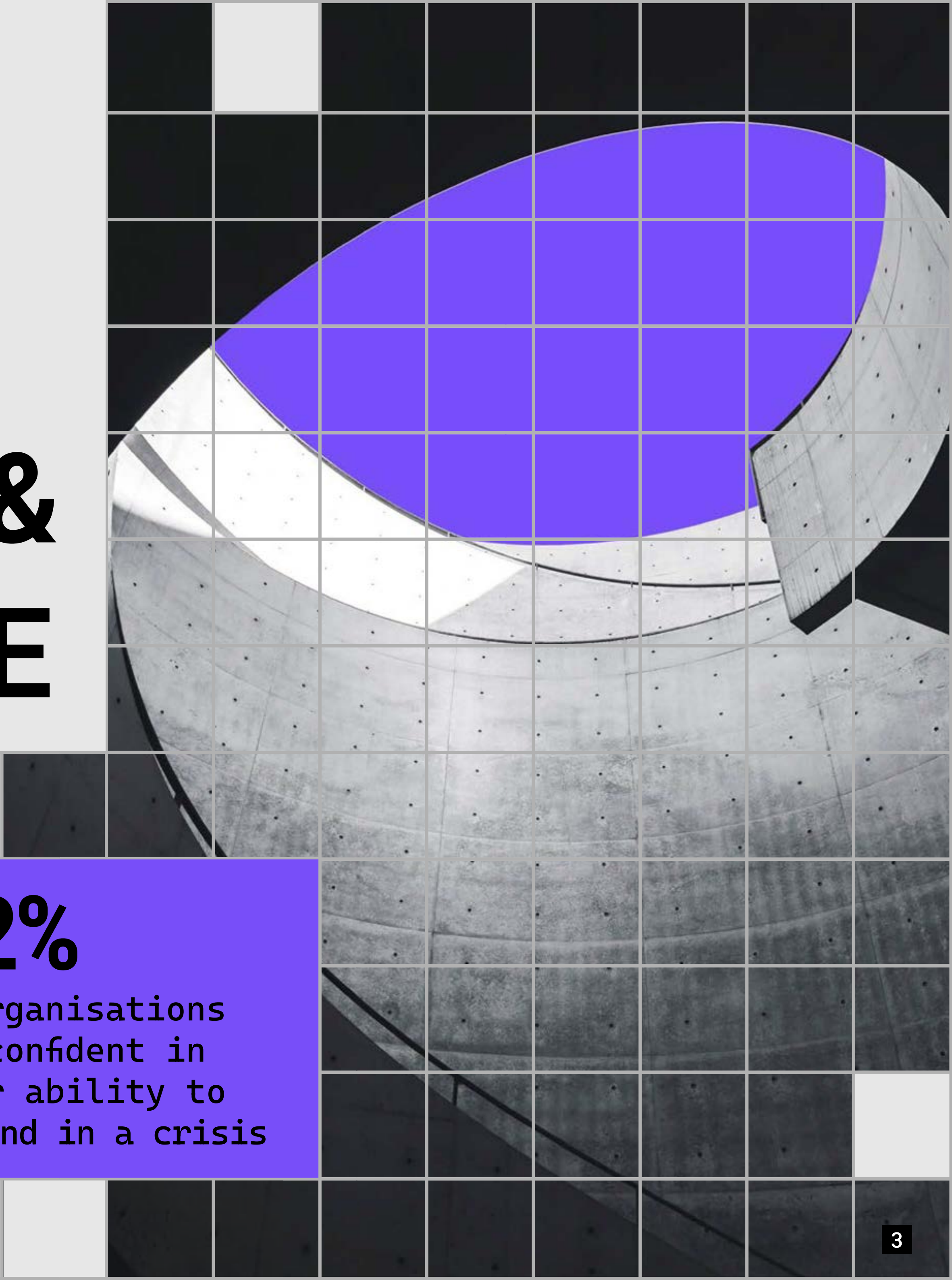
In this year's Data Health Check, we're focusing on the growing importance of cyber insurance. As cyber incidents become increasingly prevalent, we look at how companies are preparing to protect themselves from the financial and reputational damage that can result from a breach.

Ransomware remained a huge problem this year, costing UK organisations hundreds of millions of pounds. We reviewed what ransomware meant for IT professionals in 2023, and the challenges it presented.

Finally, we're continuing to provide valuable insights on Business Continuity, Data Protection, and Disaster Recovery. These elements have been the backbone of the Data Health Check since our first survey in 2008. We break down how organisations responded to cyber crises this year – and how companies in different industries fared in these key areas.

Welcome to the 2023 Data Health Check.

BC, DISASTER RECOVERY & RESILIENCE



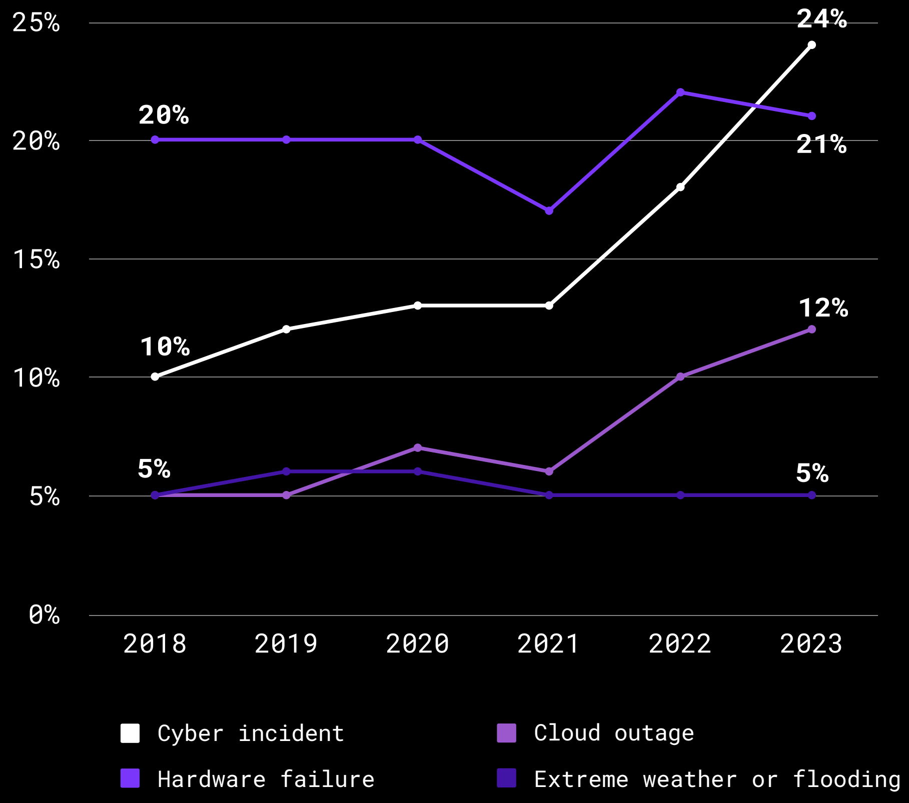
82%

of organisations are confident in their ability to respond in a crisis

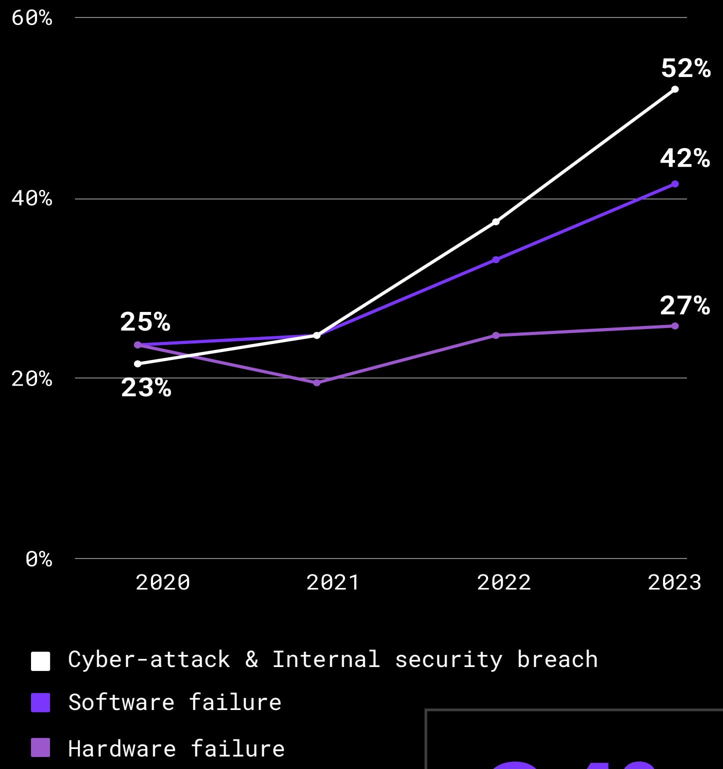
Cyber-attacks are now the leading cause of downtime and data loss

Last year, cyber became the top cause of data loss. This year, it also takes on the top spot for IT downtime.

What was the biggest cause of IT downtime for your organisation?



What were the causes of data loss?



24%

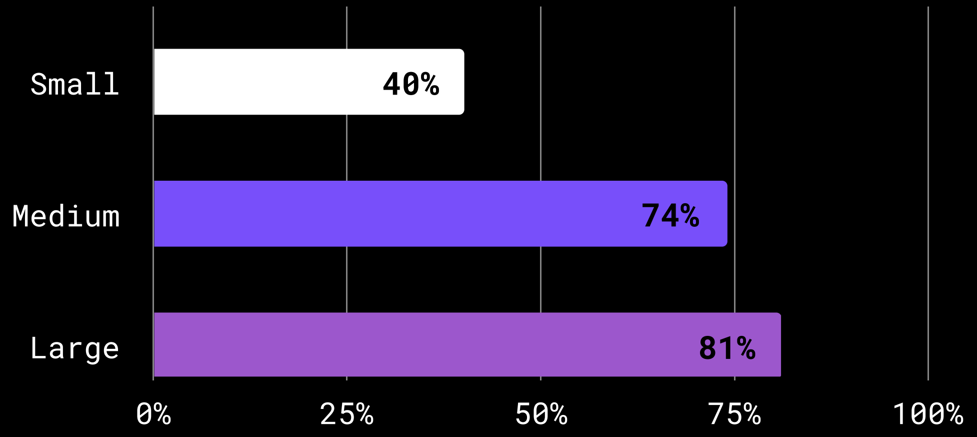
Cyber incidents were the leading cause of IT downtime last year.

Small businesses are coming up short

There has been a steady uptake in Business Continuity Plans throughout our past surveys.

Smaller organisations, however, stand out with a significantly lower uptake compared to medium and large organisations.

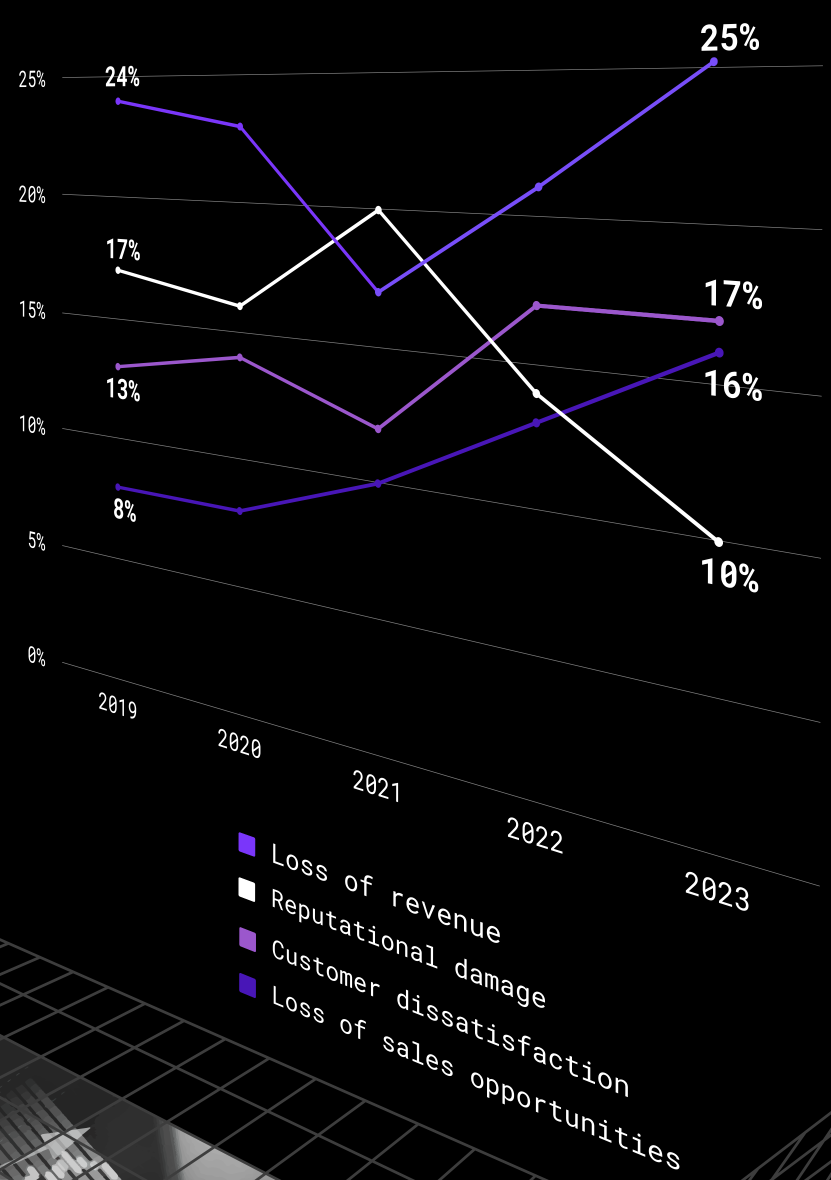
Presence of BC Plan, by organisation size

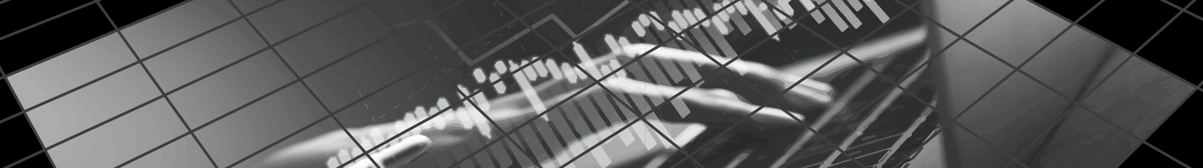


Loss of revenue is the #1 worry for businesses facing a disaster

Current economic conditions have precipitated a shift in organisations' primary worries when facing a crisis. Commercial considerations are up. Reputation concerns are down.

What is your biggest worry in a disaster?

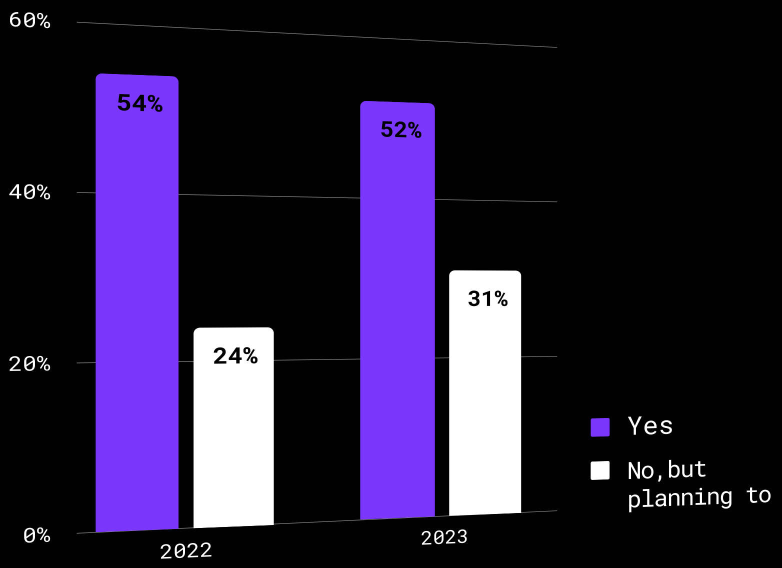




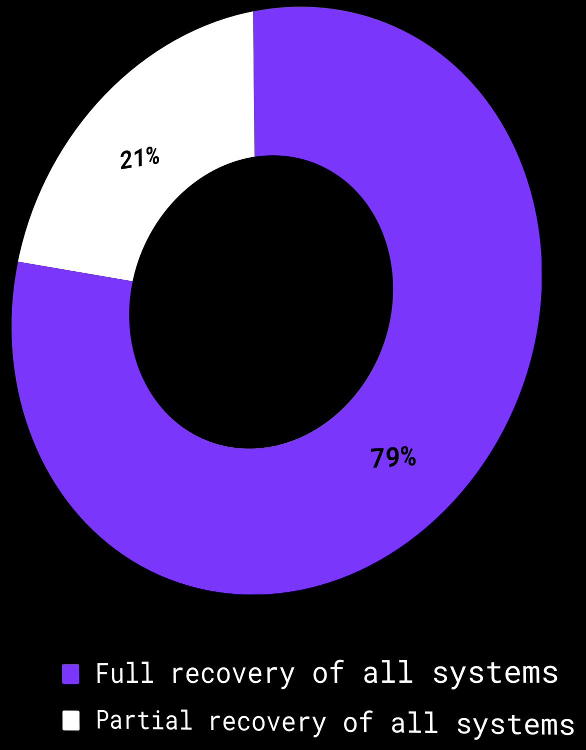
Disaster Recovery testing top of the wish list

The number of organisations that have tested their Disaster Recovery has decreased. This year, however, the number that haven't tested, but are planning to in the next 12 months, has increased significantly.

Have you tested your Disaster Recovery in the last 12 months?



What type of recovery did you conduct?

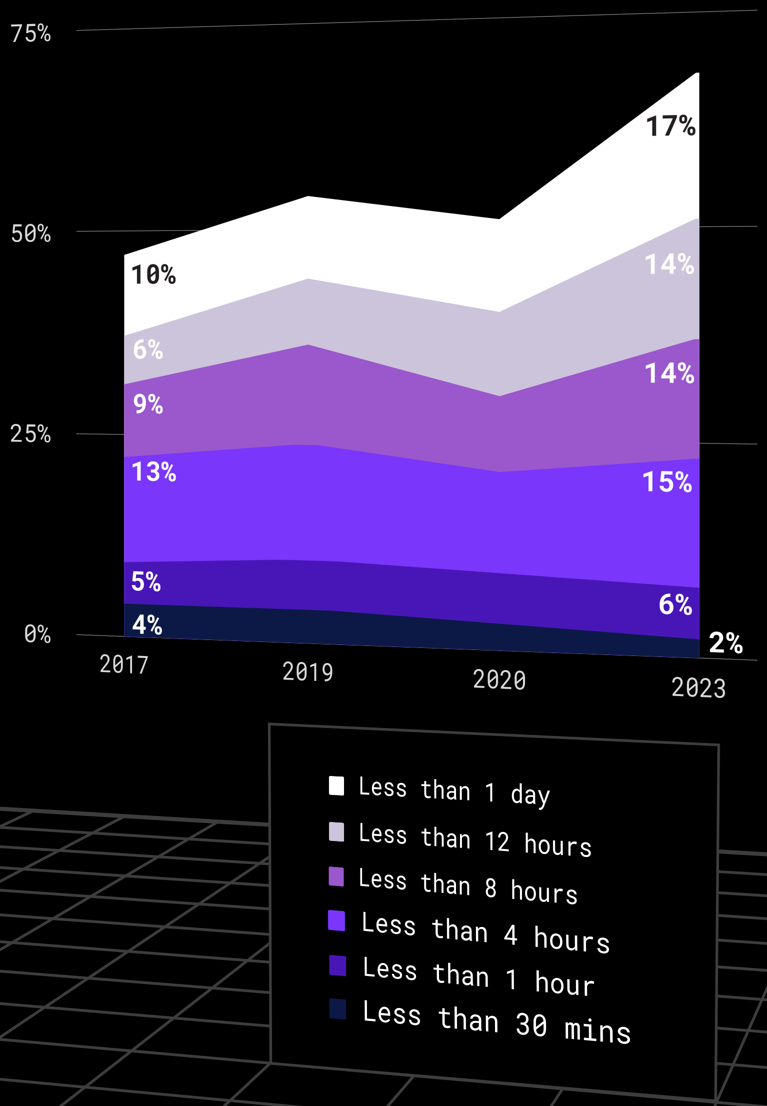


A higher-than-ever reliance on IT systems

The importance of IT systems in business operations has never been greater. More than two-thirds of companies have reported they could only survive less than one day without their crucial IT systems. A clear trend is emerging as the Maximum Tolerable Period of Disruption reduces year-on-year.

In 2023, **68%** could survive less than one day without IT systems. That compares to just 46% in 2017.

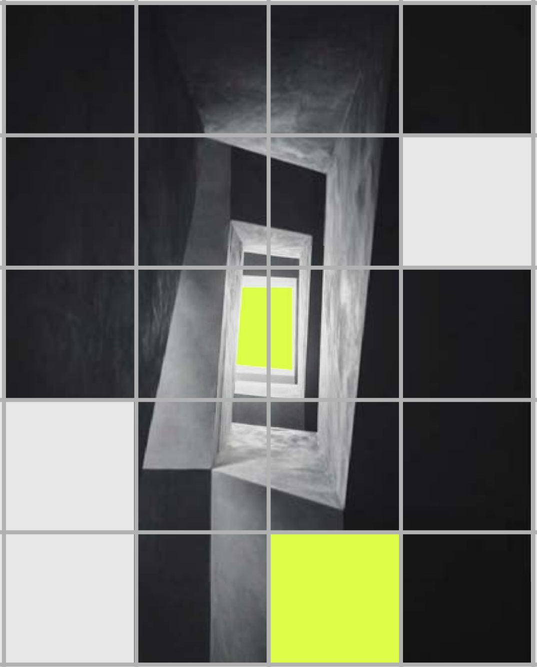
How long could your organisation survive without its crucial IT systems?



CYBER

→ **54%**

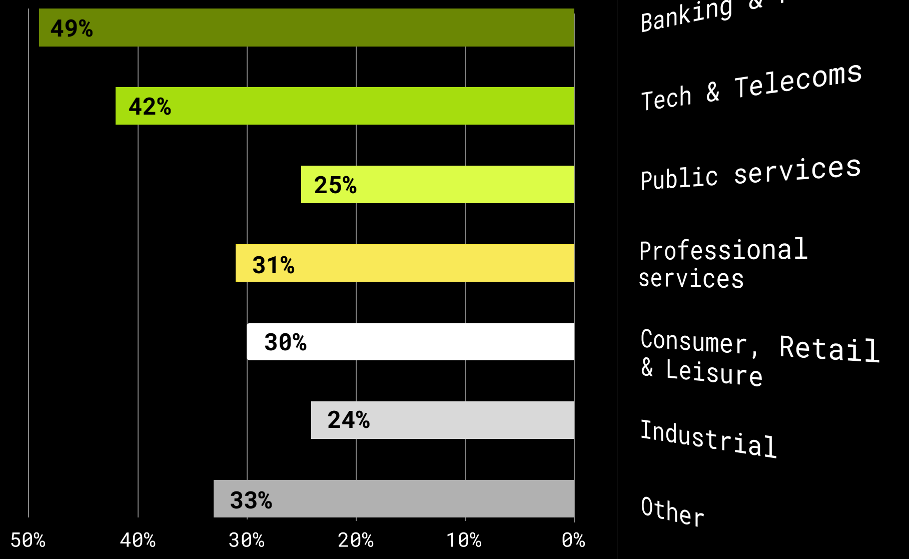
More than half of organisations experienced a cyber-attack last year



More than a third of organisations suffered a supply chain cyber-attack in the last 12 months

But digging a little deeper, the data tell another story. The Banking and Finance and Tech and Telecoms industries were hit hardest by cyber-attacks – significantly more than counterparts in other sectors.

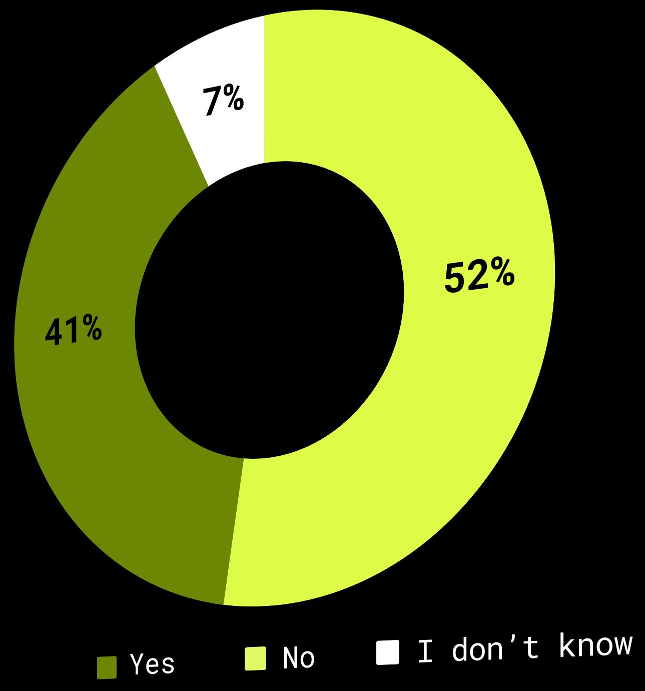
Has your supply chain experienced a cyber-attack in the last 12 months?



Managing supply-chain vulnerability

The challenge in managing the security and resilience of your supply chain is that it is outside your direct control. Just over half of all organisations reviewed their supply chains for vulnerabilities.

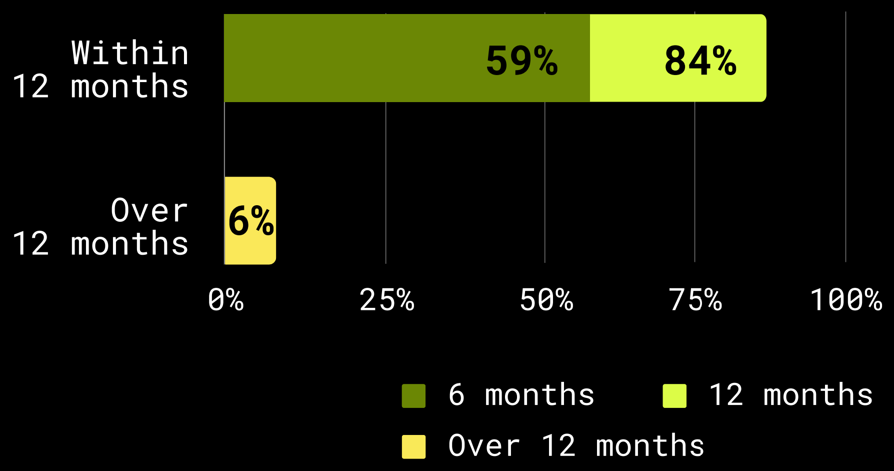
Have you reviewed your supply chain’s vulnerabilities in the last 12 months?



Cyber security training alone is not enough

However, of the companies that carried out training in the last 12 months, almost three-quarters (71%) have been impacted by cyber threats.

Have you carried out cyber awareness training in the last 12 months?



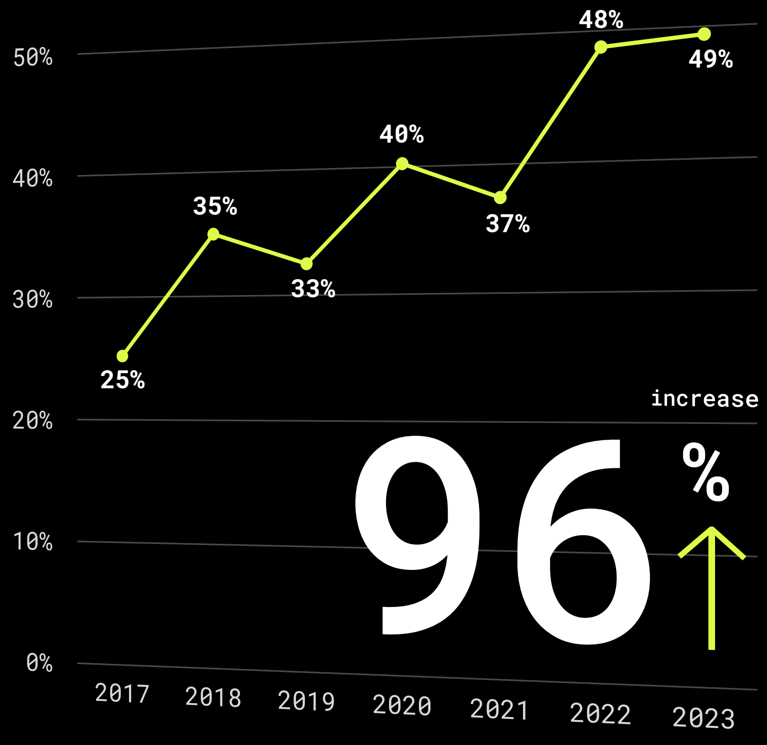
84%

have carried out cyber security awareness training in the last 12 months.

IT security budgets continue to increase

The trend of increasing IT security budgets over the past six years continues. This year, almost half of companies reported increases.

Our IT Security budget has increased

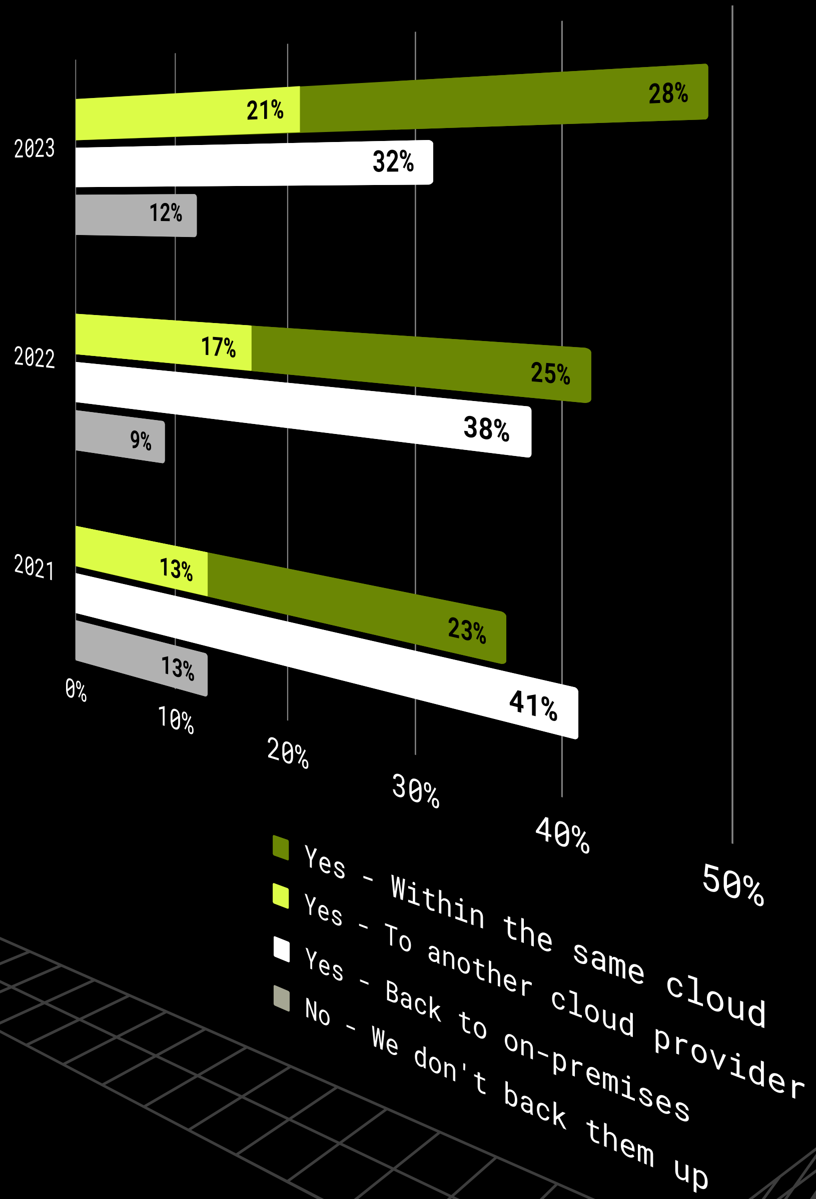


Databarracks

The most popular way to back up cloud data? In the cloud

In the last two years, organisations backing up their cloud data have shifted from sending that data back to their premises, to also using the cloud.

Do you use additional backup solutions for your cloud data?



Databarracks

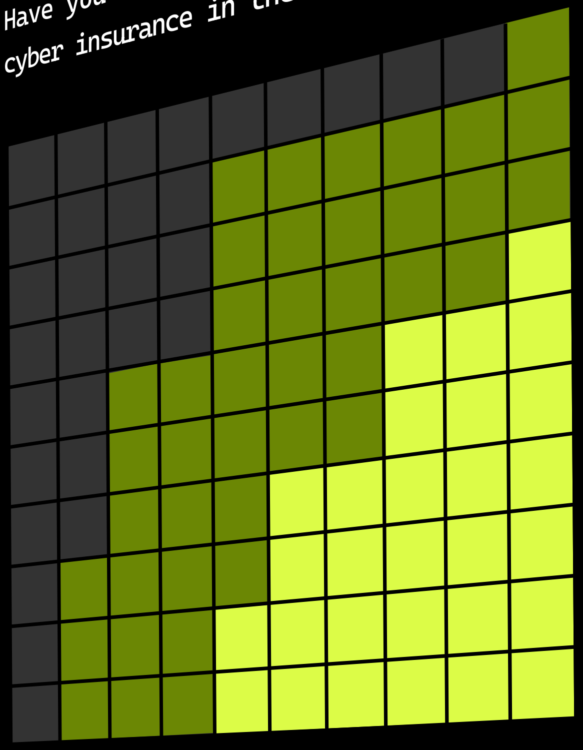
The changing landscape of cyber insurance

7 in 10 reported changes in their cyber insurance in the last 12 months – either higher cost or increased requirements for cover.

57% ↑ Demand for cyber insurance

In the last year, the number of organisations with cyber insurance has increased from 51% to 57%, despite the harder demands and increasing costs.

Have you experienced changes in your cyber insurance in the last 12 months?



🟩 41 % saw a higher requirement for cyber security tools

🟨 29 % experienced cost increase

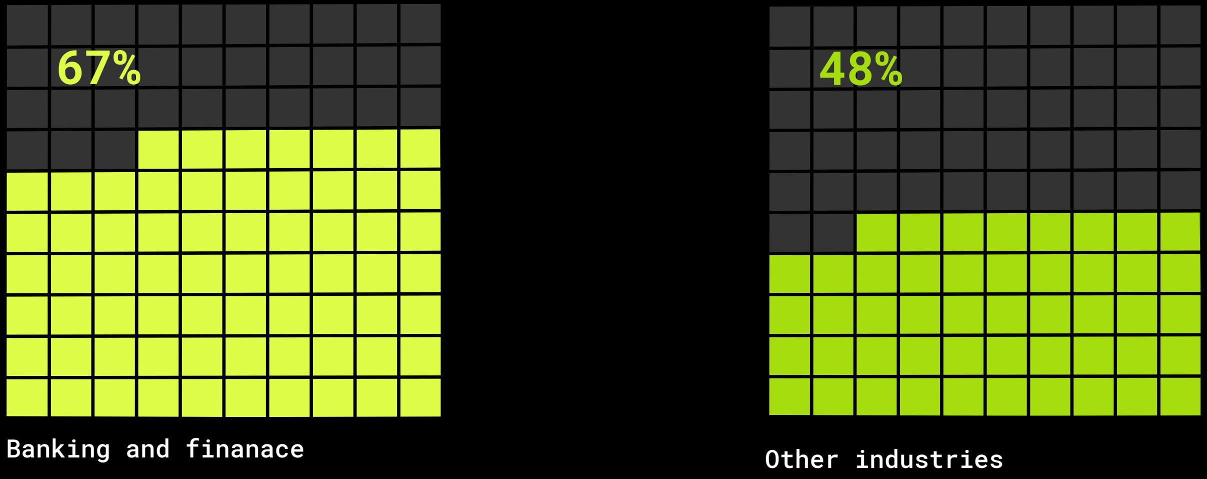
Have you made a claim on your cyber insurance this year?

The Banking & Finance industry has had the highest number of claims from cyber insurance across all industries in 2023.

57%

of those who had a cyber incident in the last 12 months made a claim on their insurance.

Claims over £1m



Databarracks

→ **37%**

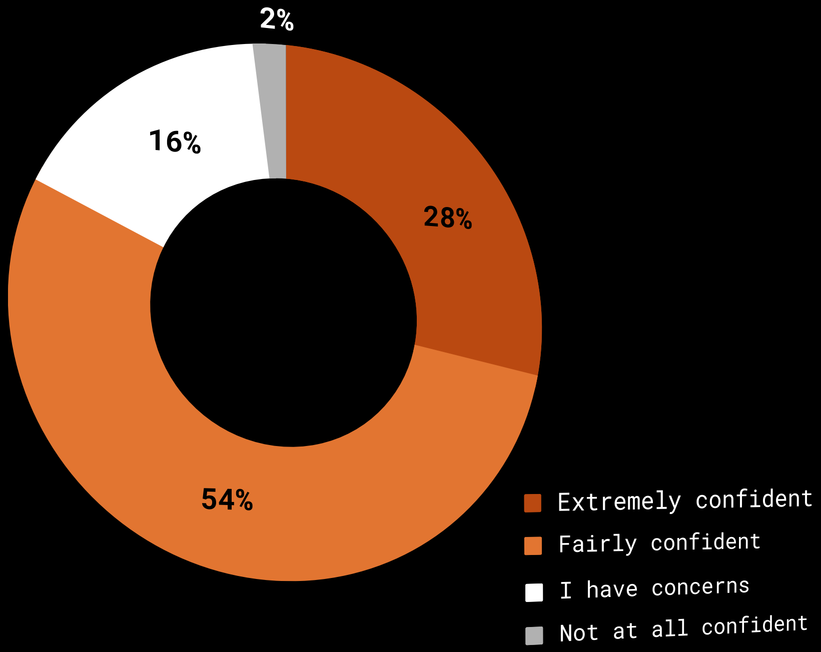
Over a third of organistaions experienced a ransomware attack in the last 12 months

RANSOMWARE

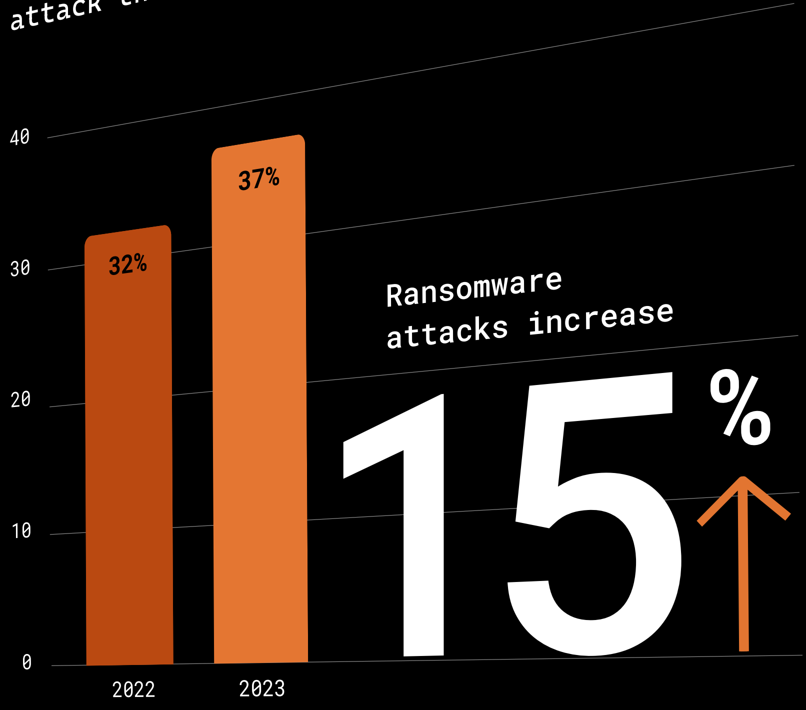
The growing risk of ransomware

Organisations reported an increase in the number of ransomware attacks compared to 2022, but only a quarter are extremely confident in their team's ability to respond to a ransomware event.

How confident are you in your team's ability to respond to a ransomware event?



Our organisation experienced a ransomware attack this year

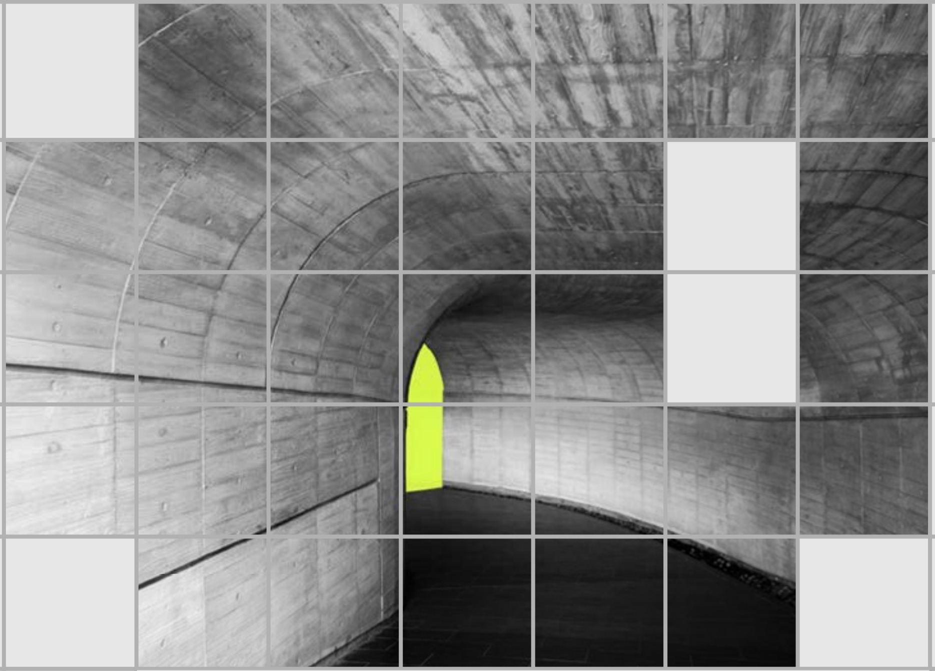


Conclusion

While the prevalence of cyber threats continues to grow, we have seen some major wins this year.

Compared to previous years in the Data Health Check, more organisations have cyber insurance, cyber security training is more frequent, and more are bing proactive in their defence against cyber threats.

Other findings raised interesting questions. For example, with the number of companies wanting to test their disaster recovery plans this year but not actually doing so, are there adequate avenues and resources available within the industry to this end?

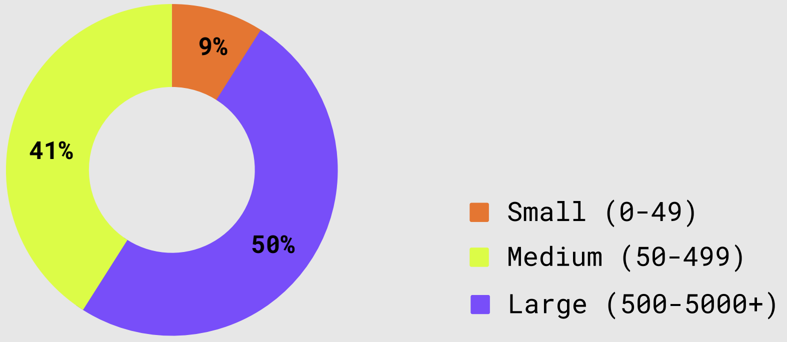


Looking ahead, the rate of growth in cyber-attacks is unlikely to slow. That is why it's imperative that we have the right security measures in place. So, when it does happen, we're ready to respond quickly and efficiently.

Thank you for reading the Data Health Check 2023. We look forward to seeing you again next year.

Appendix

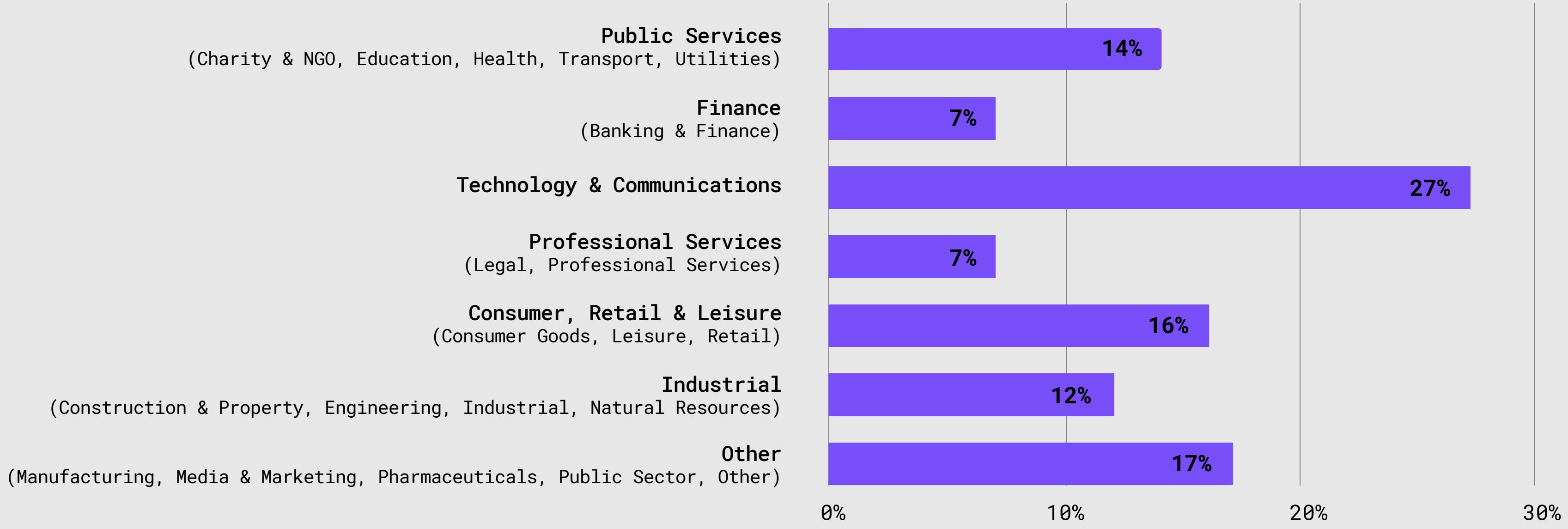
Organisation size



Total respondents

500

Respondents split by industry



What best describes your business sector?

Banking & Finance	7.00%
Charity & NGO	0.60%
Construction & Property	3.60%
Consumer Goods	2.60%
Education	4.60%
Engineering	4.80%
Health	3.80%
Industrial	3.40%
Legal	2.60%
Leisure	2.60%
Manufacturing	10.80%
Media & Marketing	1.60%
Natural Resources	0.60%
Pharmaceuticals	0.40%
Professional Services	4.40%
Public Sector	3.20%
Retail	10.60%
Technology	20.80%
Telecommunications	6.00%
Transport	3.60%
Utilities	1.40%
Other	1.00%

What is your position within the business?

Corporate / Board-level responsible for IT	19.80%
Director-level responsible for IT	27.80%
IT Manager	32.80%
IT Technical Specialist	16.20%
IT Consultant	3.40%

How many employees does your company have?

< 25	5.60%
25-49	3.00%
50-99	5.40%
100-249	18.40%
250-499	26.20%
500-999	21.00%
1000-4999	12.20%
5000+	8.20%

How many employees in your IT department?

< 5	7.00%
5-10	14.40%
11-15	29.40%
16-30	25.80%
31-100	11.40%
100+	12.00%

Where is your UK head office located?

North East	1.80%
North West	8.80%
Yorkshire and The Humber	3.60%
East Midlands	6.40%
West Midlands	8.60%
East of England	15.60%
London	30.80%
South East	9.00%
South West	5.20%
Scotland	4.20%
Wales	1.80%
Northern Ireland	4.20%

What is your annual turnover?

< £5m	8.40%
£5 - 9.9m	5.00%
£10 - 24.9m	7.60%
£25 – 49.9m	15.00%
£50 – 99.9m	19.40%
£100 – 249.9m	22.00%
£250 – 499.9m	11.00%
£500 – 999.9m	4.80%
> £1bn	6.80%

What were the causes of any data loss over the last 12 months?

Hardware failure	26.40%
Software failure	42.00%
Data corruption	38.80%
Human error	34.00%
Internal security breach (member of staff)	23.40%
Cyber-attack	28.60%
Extreme weather or flooding	11.20%
Theft	7.40%
None	15.40%
Other (please specify)	0.20%

Do you have a Business Continuity Plan?

Yes, and it is up to date	49.20%
Yes, but it is not up to date	24.40%
No, but we will within the next 12 months	13.40%
No, and we don't intend to implement one within the next 12 months	8.80%
I don't know	4.20%

Who is involved in the writing of your business continuity plan?

IT Manager	45.92%
IT Director	45.92%
CIO	33.42%
CFO	22.83%
CEO	24.46%
Finance Director	16.03%
Individual department heads (HR Manager, Marketing Manager, etc.)	17.39%
Business Continuity Manager	16.30%
Operations Manager	14.67%
Board	7.34%
I don't know	1.90%
Other	0.54%

In your organisation, who is ultimately in charge of the business continuity plan?

IT Manager	26.90%
IT Director	36.68%
Business Continuity Manager	19.57%
Operations Manager	7.88%
Board	6.52%
I don't know	2.17%
Other	0.27%

Within your Business Continuity Plan, do you have a specific IT disaster recovery plan?

Yes	73.37%
No, but we're planning to write one in the next 12 months	21.74%
No, and we have no intention of writing one	3.80%
I don't know	1.09%

Have you tested any elements of your disaster recovery process in the last 12 months?

Yes	52.20%
No, but we're planning to within the next 12 months	31.20%
No, and we're not planning to	13.20%
I don't know	3.40%

What type of recovery did you conduct?

Full recovery of all systems	78.93%
Partial recovery of all systems	21.07%

Have you tested your disaster recovery process specifically against cyber threats?

Yes	68.58%
No, but we are planning on making it the focus of our next test	27.97%
No, and we're not planning to	1.15%
I don't know	2.30%

What was the biggest cause of IT downtime for your organisation in the last 12 months?

Extreme weather or flooding	4.80%
Hardware failure	20.20%
Cyber incident	24.00%
Upgrades/patches	18.80%
Cloud outages	12.40%
Connectivity issues	9.80%
I don't know	2.80%
We didn't experience any downtime in the last 12 months	6.60%
Other	0.60%

How long could your organisation survive without its crucial IT systems (i.e. what is your Maximum Tolerable Period of Disruption)?

Less than 30 mins	2.20%
Less than 1 hour	5.80%
Less than 4 hours	14.80%
Less than 8 hours	13.60%
Less than 12 hours	14.40%
Less than 1 day	17.20%
Less than 2 days	12.00%
Less than 3 days	6.40%
Less than 1 week	5.00%
Less than 2 weeks	1.40%
Less than 1 month	1.60%
I don't know	5.60%

Did you make a claim on your cyber insurance this year?

Yes	56.79%
No	42.16%
I don't know	1.05%

How long would it take for you to recover your IT from a disaster (your current Recovery Time Objective?)

Less than 5 minutes	2.80%
Less than 1 hour	13.00%
Less than 4 hours	22.80%
Less than 8 hours	22.20%
Less than 12 hours	17.40%
Less than 24 hours	12.40%
Less than 48 hours	2.60%
More than 48 hours	0.60%
I don't know	6.20%

How confident are you in your organisations ability to respond in a crisis?

Very confident	26.40%
Fairly confident	55.60%
I have concerns	15.00%
Not at all confident	3.00%

What is your biggest worry in a disaster?

Reputational damage	10.20%
Loss of revenue	25.20%
Loss of sales opportunities	16.20%
Customer dissatisfaction	17.00%
Regulatory penalties	11.60%
Employee dissatisfaction	7.00%
Lost productivity	7.40%
I don't know	3.20%
None	2.00%
Other	0.20%

What were the causes of any data loss over the last 12 months?

Hardware failure	26.40%
Software failure	42.00%
Data corruption	38.80%
Human error	34.00%
Internal security breach (member of staff)	23.40%
Cyber-attack	28.60%
Extreme weather or flooding	11.20%
Theft	7.40%
None	15.40%
Other (please specify)	0.20%

How confident are you in your team's ability to respond to a ransomware event?

Extremely confident	27.60%
Fairly confident	54.20%
I have concerns	16.00%
Not at all confident	2.20%

Have you experienced a ransomware attack this year?

Yes	36.60%
No	60.80%
I don't know	2.60%

How did you detect the ransomware?

Users notified IT that files were encrypted	16.94%
Network monitoring	35.52%
Use of honeypots	27.32%
Anti Malware software	15.85%
Anti ransomware tool	4.37%
Other	0.00%

How did you respond to the ransomware attack?

Recovered from backups and didn't pay	32.24%
Paid ransom	43.72%
Used ransomware decryption tool	21.86%
I don't know	2.19%

Does your organisation have a policy for paying-out on a ransomware attack?

No - we don't have a policy	21.00%
Yes - we pay if the ransom is lower than the cost to recover systems	30.80%
Yes - we pay if the ransom is covered by cyber insurance insurance	19.80%
Yes - we pay only as a last resort if there is no other way to recover data	9.60%
Yes - our policy is to never pay a ransom	11.60%
I don't know	7.20%

Have you been impacted by any cyber threats in the last 12 months?

Yes, on one occasion	39.40%
Yes, on multiple occasions	14.00%
No	46.60%

Which of the following cyber threats have you been affected by in the last year?

Virus	21.72%
Spyware	26.22%
Ransomware	27.34%
Adware	19.10%
KeyLogger	20.60%
Bots	20.22%
DDOS	23.97%
Phishing	23.97%
Spear Phishing	16.10%
Nation State Attack	8.61%
Social Engineering	8.61%
I don't know	1.50%
None	0.37%
Other	0.37%

How many cyber attacks did you experience this year (either successful or unsuccessful)?

0	2.25%
1-5	23.60%
6-10	19.85%
11-25	28.09%
26-50	16.85%
51-100	4.49%
100+	3.00%
I don't know	1.87%

Have any of your suppliers suffered a cyber attack in the last 12 months?

Yes	33.80%
No	54.60%
I don't know	11.60%

How many employees in your IT department?

< 5	7.00%
5-10	14.40%
11-15	29.40%
16-30	25.80%
31-100	11.40%
100+	12.00%

Have you reviewed your supply chain for vulnerabilities to cyber attacks?

Yes	52.40%
No	40.80%
I don't know	6.80%

When was the last time you carried out cyber security awareness training?

Within 3 months	23.40%
Within 6 months	35.40%
Within 12 months	24.80%
Over 12 months ago	6.40%
I don't know	4.20%
We don't carry out any kind of cyber security awareness training	5.80%

Do you feel like you've got sufficient cyber security skills in your team to deal with the current threat landscape?

Yes	60.00%
No, but we are actively trying to improve the level of cyber security skills we have in-house	32.40%
No, and we are not planning to invest in improving these skills in-house	7.60%

Does your organisation have a board member responsible for cyber security?

Yes	55.60%
No	36.20%
I don't know	8.20%

Has your IT security budget increased within the last 12 months?

Yes, our IT security budget has increased	49.40%
No, our IT security budget has stayed the same	38.40%
No, our IT security budget has decreased	6.00%
I don't know	6.20%

Have you evaluated your continuity risks for cloud services compared with on-premise IT?

Yes	46.00%
No, but we're planning to in the next 12 months	28.20%
No, and we're not planning to in the next 12 months	17.00%
I don't know	6.00%
We don't use any cloud services	2.80%

Do you use any additional backup or recovery capabilities for any cloud services, beyond the standard default options?

Yes - Within the same cloud	28.40%
Yes - Back to on-premises	32.20%
Yes - To another cloud provider	20.60%
No - We don't back them up	12.20%
I don't know	6.00%
Other	0.60%

Have you reviewed you security policies in the last 12 months in response to recent cyber threats?

Yes, we have reviewed our security policies and have made changes	45.20%
Yes, we have reviewed our security policies and made no changes	34.40%
No, we have not reviewed our security policies	15.20%
I don't know	5.20%

If you reviewed or renewed your cyber insurance in the last 12 months, were there any changes?

Increased cost	29.40%
Increased requirement for cyber security tools (such as MFA or Endpoint Detection and Response)	41.20%
No changes	22.60%
I don't know	6.80%

Does your organisation have cyber insurance?

Yes	57.40%
No	33.80%
I don't know	8.80%

How much did you claim from your cyber insurance?

£0-£10,000	2.45%
£10,001-£100,000	12.27%
£100,000-£1,000,000	37.42%
£1,000,001-£10,000,000	41.10%
£10,000,001-£100,000,000	5.52%
£100,000,000+	1.23%

Databarracks

0800 033 6633

contact@databarracks.com
www.databarracks.com