DealMaker Meter

by DFIN

UNDERSTANDING RISK: THE DARK SIDE OF DATA

FALL 2022

Dark Data

|dährk dey-tuh|

Noun

Gartner defines dark data as the information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes (for example, analytics, business relationships and direct monetizing). Similar to dark matter in physics, dark data often comprises most organizations' universe of information assets. Thus, organizations often retain dark data for compliance purposes only. Storing and securing data typically incurs more expense (and sometimes greater risk) than value.

Understanding information security and privacy in 2022

Companies collect and store massive amounts of detailed information, but most of this big data transforms into dark data when it goes unused or remains unknown. Bad actors hiding in corners of the Internet battle with security professionals over access to company assets, so securing and protecting all data is essential.

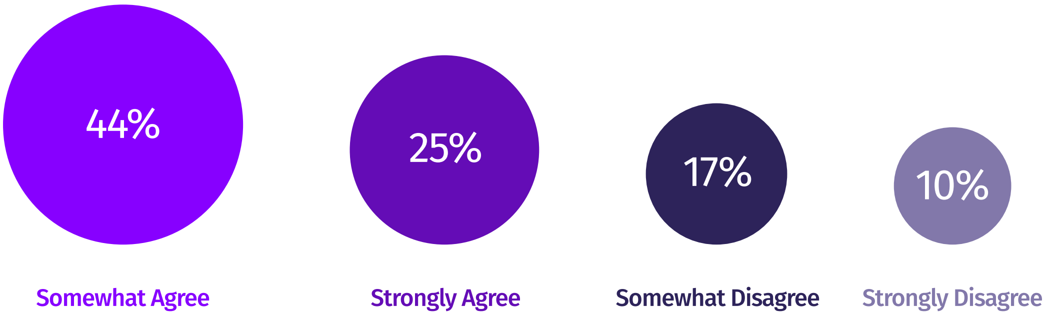
This affects Fortune 1000 companies, small- and medium-sized businesses, startups, private equity firms, and investment banks across the entire spectrum of industries. All face challenges when guarding confidential and sensitive information for governance and protecting employee and consumer privacy for compliance.

The Fall report explores and reports on cybersecurity experiences and expectations.

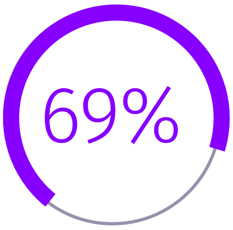
To store, protect or purge detailed records – that is the question

Although critically important to enterprises, data has its darker side. Data sometimes gets into the wrong hands – cybercriminals with ill will in mind or people who have no business viewing an enterprise's accumulated information. Nearly 7 of 10 enterprise leaders surveyed said storing detailed information presents more risk than value. Upgrading information technology should be considered to better secure, purge or protect such dark data.

Storing detailed information at our company sometimes presents more risk than value to the overall enterprise.



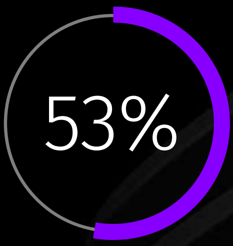
IT personnel are almost twice as likely (33%) as other departments (18%) to think storing such data creates more risk than value. U.S. and U.K. respondents see eye to eye on the subject at 26% and 25%, respectively.



say the risk outweighs the rewards of storing detailed data.

Dark data – an urgent issue

C-level leaders and IT professionals are more aware that storing dark data is a pressing concern, potentially opening the company up to vulnerabilities, risks and legal issues stemming from a security incident breach. However, other departments (51%) aren't as tuned in to these concerns. Public company respondents were either slightly knowledgeable (28%) or not at all knowledgeable (23%).

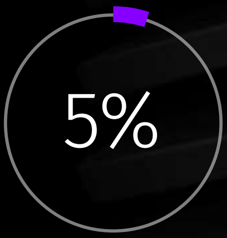


of combined IT and C-level respondents say dark data is an extremely pressing issue.

Cyber event frequency continues going up

Data incidents are rising, and respondents believe they will continue to do so over the next 24 months. In fact, most organizations surveyed faced multiple cybersecurity incidents in the past year.

52% of respondents said phishing incidents had greatly or somewhat increased and were also the most common form of potential breach. However, cybersecurity-related events are on the rise, including data breaches, data fraud and regulation changes. The more lucrative a company, the higher the chance it will be targeted more frequently. But no company is without risk.



Just 5% of respondents are unconcerned about phishing incidents.

Data breaches are slightly more concerning than phishing

Phishing, data breaches and data fraud are top concerns among decision-makers, jockeying for a close #1, #2 and #3 spot. It turns out, perhaps surprisingly, that data breaches (96%) are slightly more concerning than phishing and data fraud (both at 95%).

Overall, respondents from the U.S. are much more likely than those from the U.K. to be "very concerned" with data breaches, data fraud, phishing and cybersecurity regulations. For example, 49% of U.S. respondents said data breaches had them "very concerned," whereas just 20% of their U.K. counterparts felt the same.

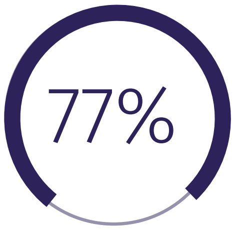
Overall, U.S. respondents worry more about data breaches than those in the U.K.

New tech tools are top of mind

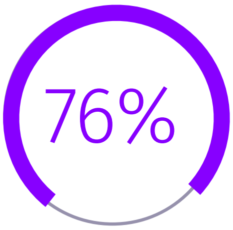
So, the challenges are unveiled but what are companies doing to improve their cybersecurity posture?

Updating or acquiring technology is critically important – more so than hiring people to throw at the problem. 83% of decision-makers would choose new technology tools over adding more team members (17%). This is likely because nearly half the survey's respondents said they don't have the right technology to adequately protect their data.

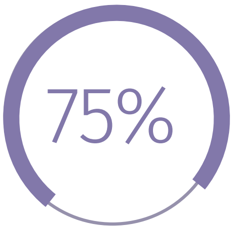
Companies aren't ignoring the ever-evolving cybersecurity landscape, however. The top three ways enterprises are preparing for upcoming cybersecurity changes are:



Enacting New Policies or Departmental Practices

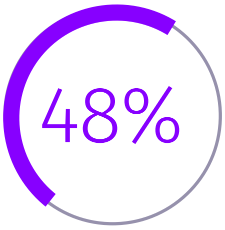


Investing in Additional Data Oversight / Review



Evaluating New Tools / Software / Capabilities / Services

Allocating additional budget and new reporting mechanisms for data (both at 72%) and new restrictions on data access (70%) are not far behind.



of respondents strongly or somewhat disagree they have the tech tools they needed to adequately do their job – to protect against dark data.

Action steps

Shine the light on your dark data

The best way to understand what data you have and how it should be protected is to bring it to light. Select software that shines the spotlight into the dark recesses of your enterprise to identify and surface dark data.

Don't fall prey to hook, line and sinker

Phishing is becoming more prevalent, so much so that services now exist that allow scammers to easily target and exploit audiences. Ensure that your most sensitive information is properly secured and even redacted to safeguard it from falling into the wrong hands.

Diligently scrub assets before disposal

When disposing of or donating dated hardware and devices, ensure that they are properly scrubbed of all business information. Familiarize yourself with Secure IT Asset Disposition processes and identify an appropriate partner to manage this for your organization.

Limit access to personal information

Avoid giving the keys to the kingdom to everyone. Increase security around and even redact sensitive information, like Social Security numbers and credit card information, making them only accessible to chosen high-level employees. Doing so helps decrease the chance that such dark data purposefully or inadvertently leaks.

Educate employees on potential cyber threats

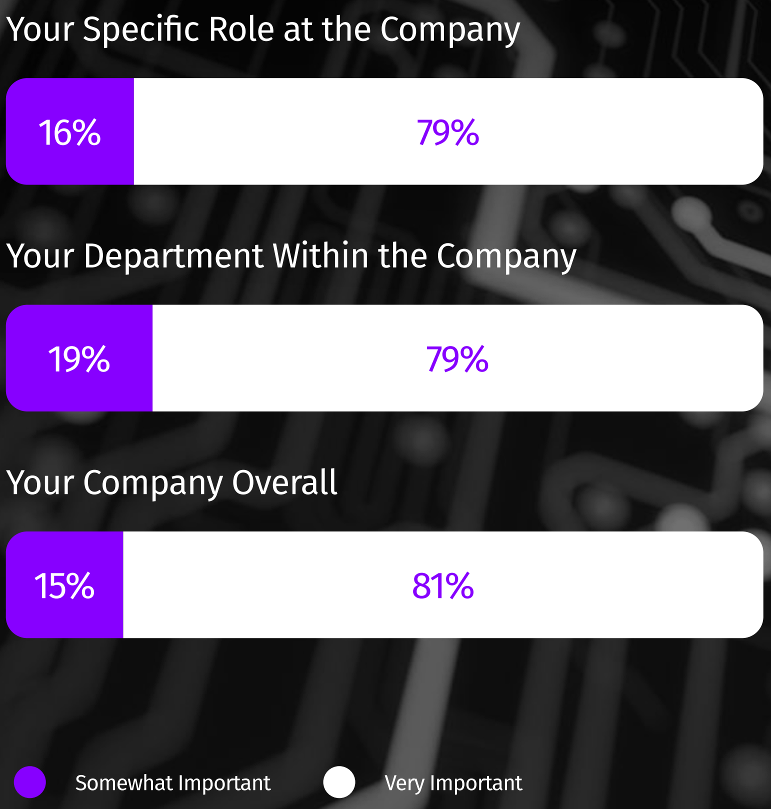
No matter where you do business, data privacy regulations are tightening, and enterprises can suffer multi-million dollar fines for non-compliance. Protect your assets by raising awareness company-wide and by investing in software that automatically redacts personally identifiable information (PII) and other sensitive data.

Choose a partner that understands your security posture

Your brightest stars cannot shine 24/7, but your cybersecurity software can. Choose a software provider that understands and can meet and even exceed your cybersecurity needs – one that keeps you safe and sound.

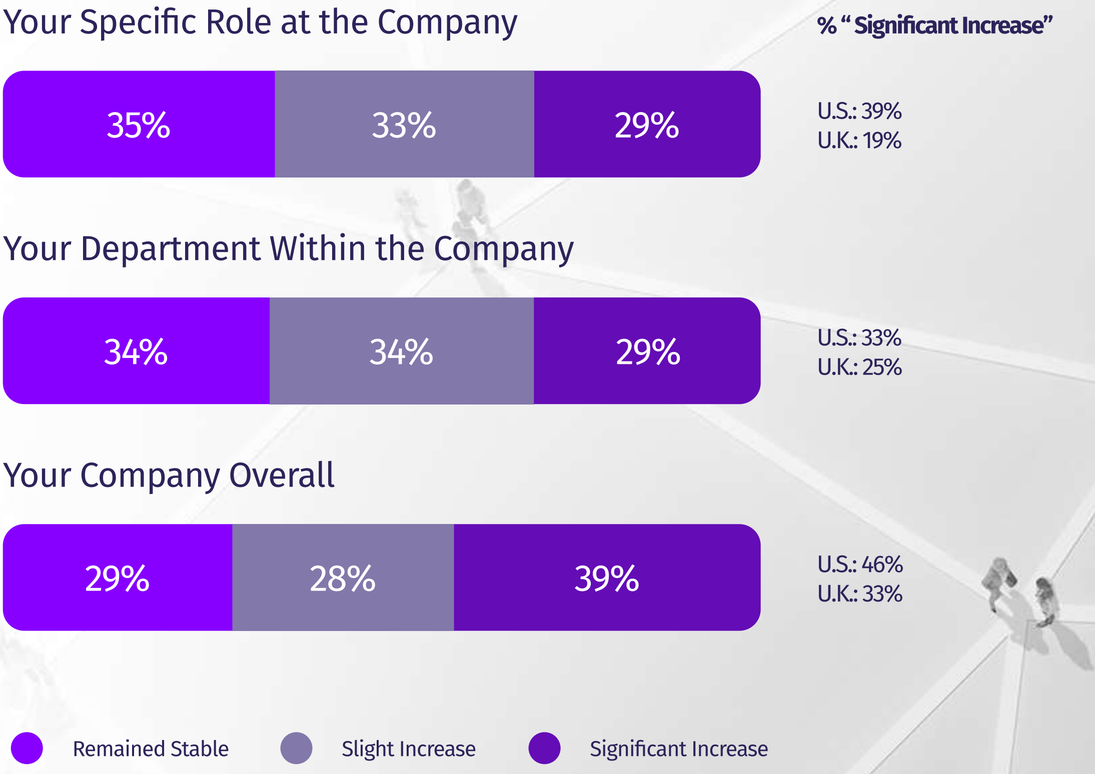
The majority of decision-makers surveyed say **data protection / privacy is very important to all aspects of their company,** reflecting the industry's current focus on this area. Those working in an IT role are slightly more likely to show this importance.

What is the overall importance of data protection / privacy?



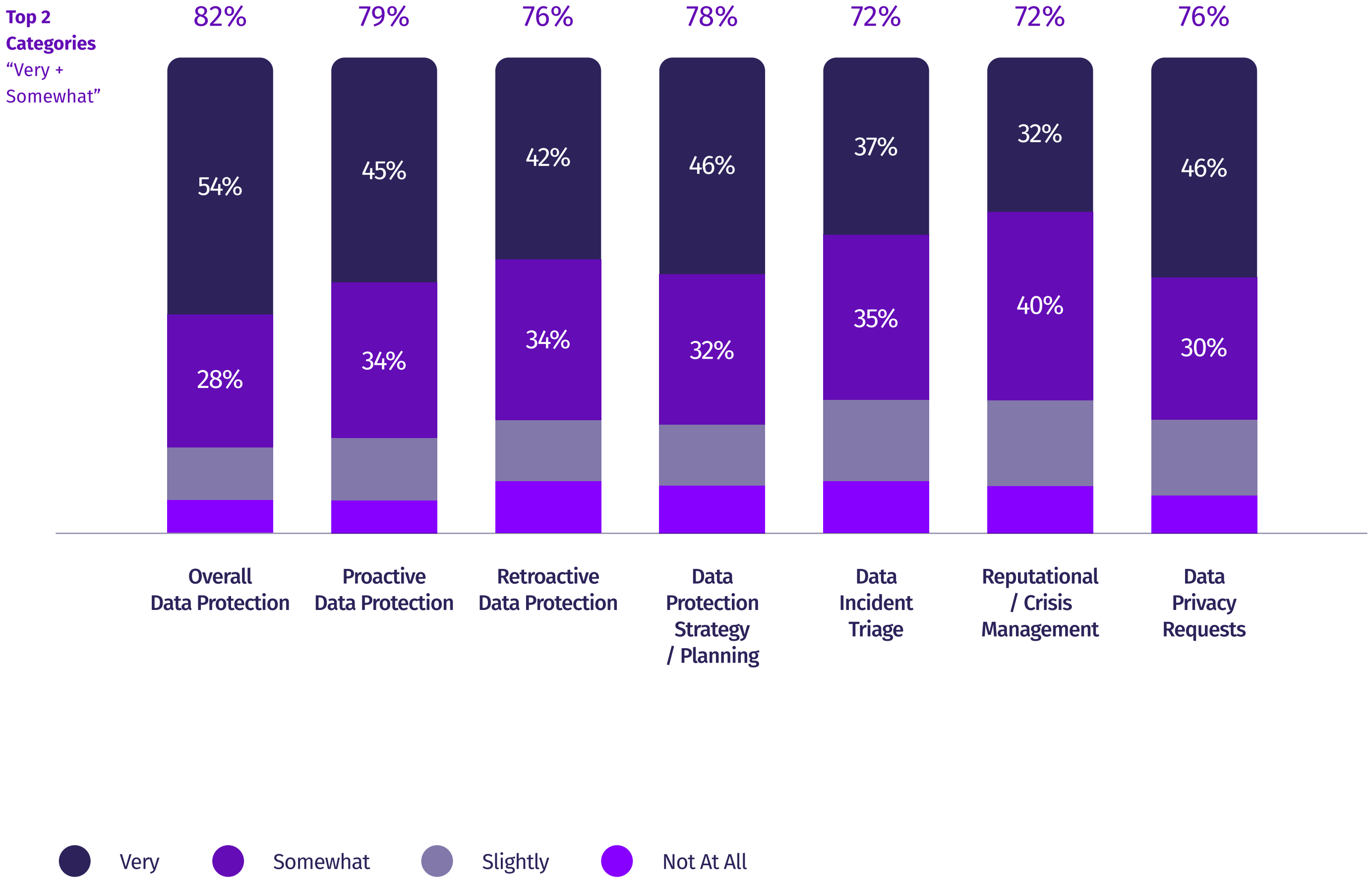
Although data protection / privacy is very important to decision-makers now, the focus on this area has significantly increased at a company-level in the past year. Respondents in the U.S. show a larger increase in emphasis compared to the U.K.

To what extent has the importance of data protection / privacy changed for the following entities in the past 12 months?



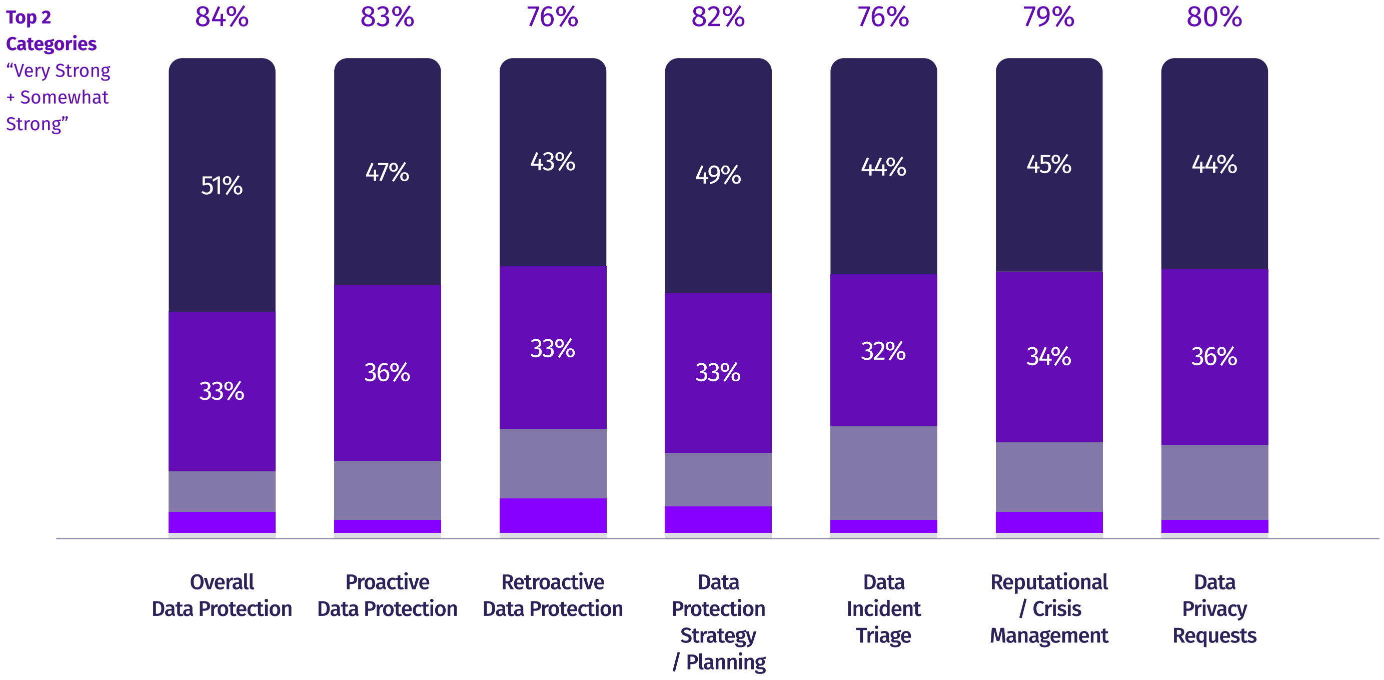
Most decision-makers claim involvement with cybersecurity within their role; however, respondents in the U.S. or working in an IT role are likely to be more involved in all areas of cybersecurity.

To what extent are you involved with the specific cybersecurity areas listed?



About half of decision-makers rate their company's cybersecurity performance as very strong, suggesting there's room for improvement to tighten these measures, especially among lower revenue companies.

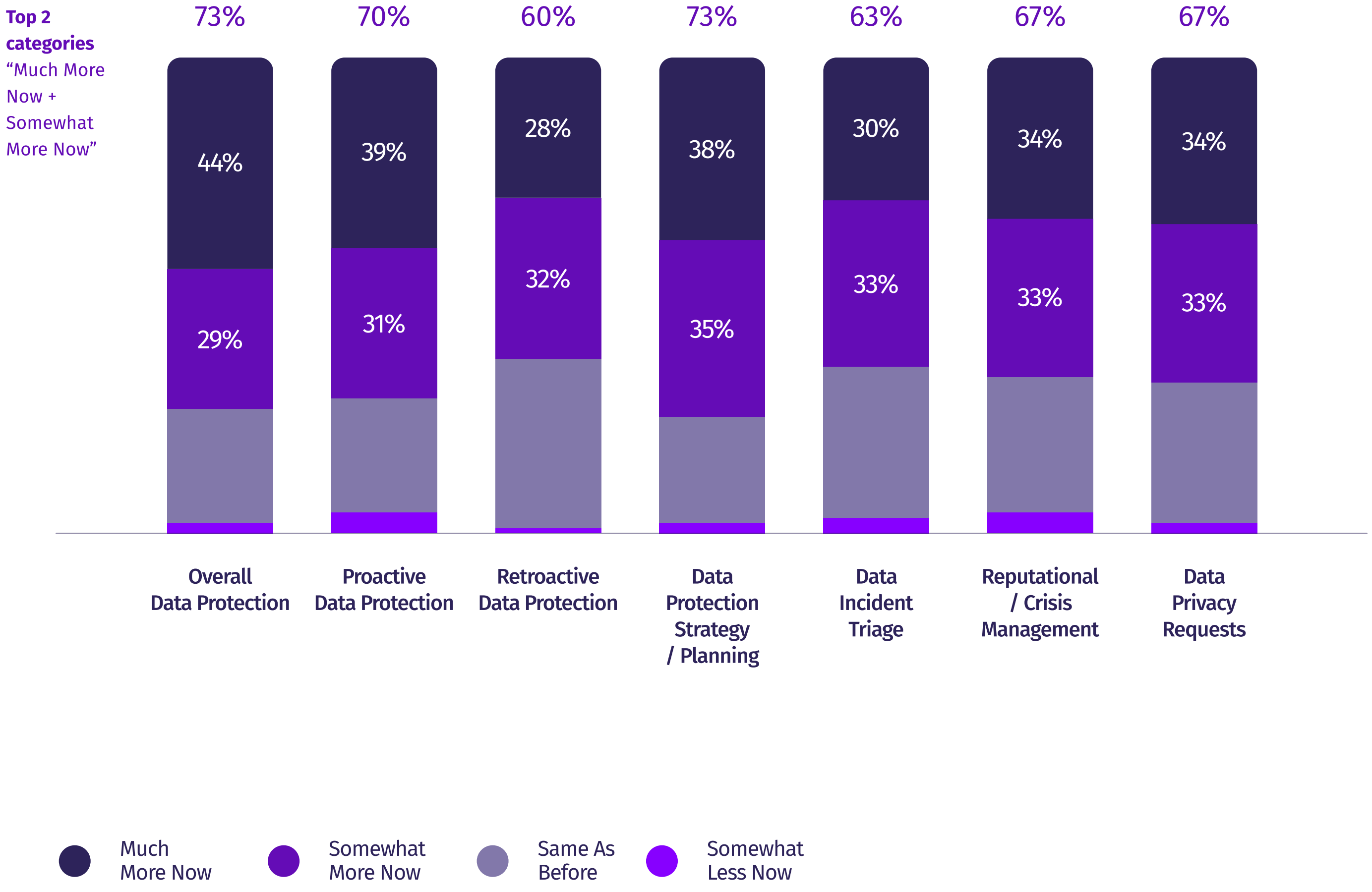
How would you rate your company's overall level of competency regarding?



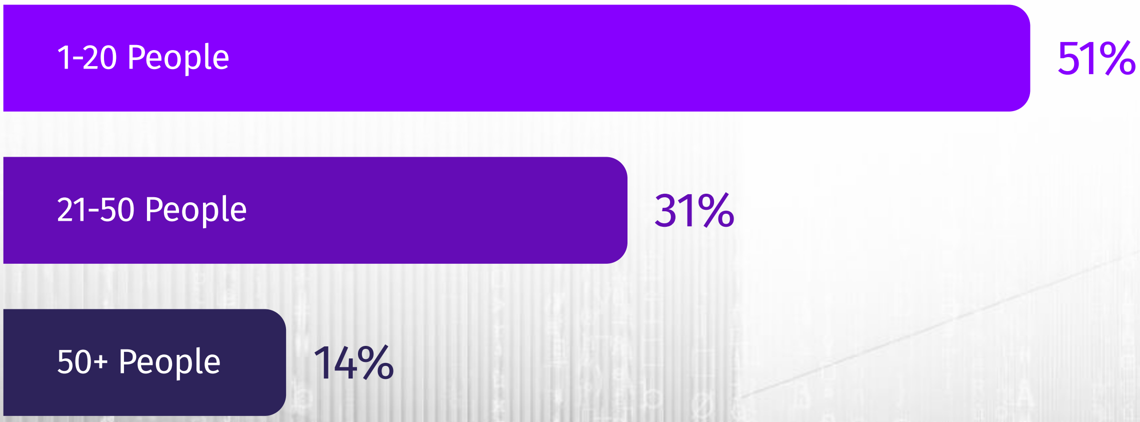
● Very Strong ● Somewhat Strong ● Average ● Somewhat Weak ● Very Weak

Overall data protection has seen an increased focus in the past year, with added emphasis on planning for the future. Proactive data protection and data protection strategy and planning are two areas that are a much bigger focus for companies this year.

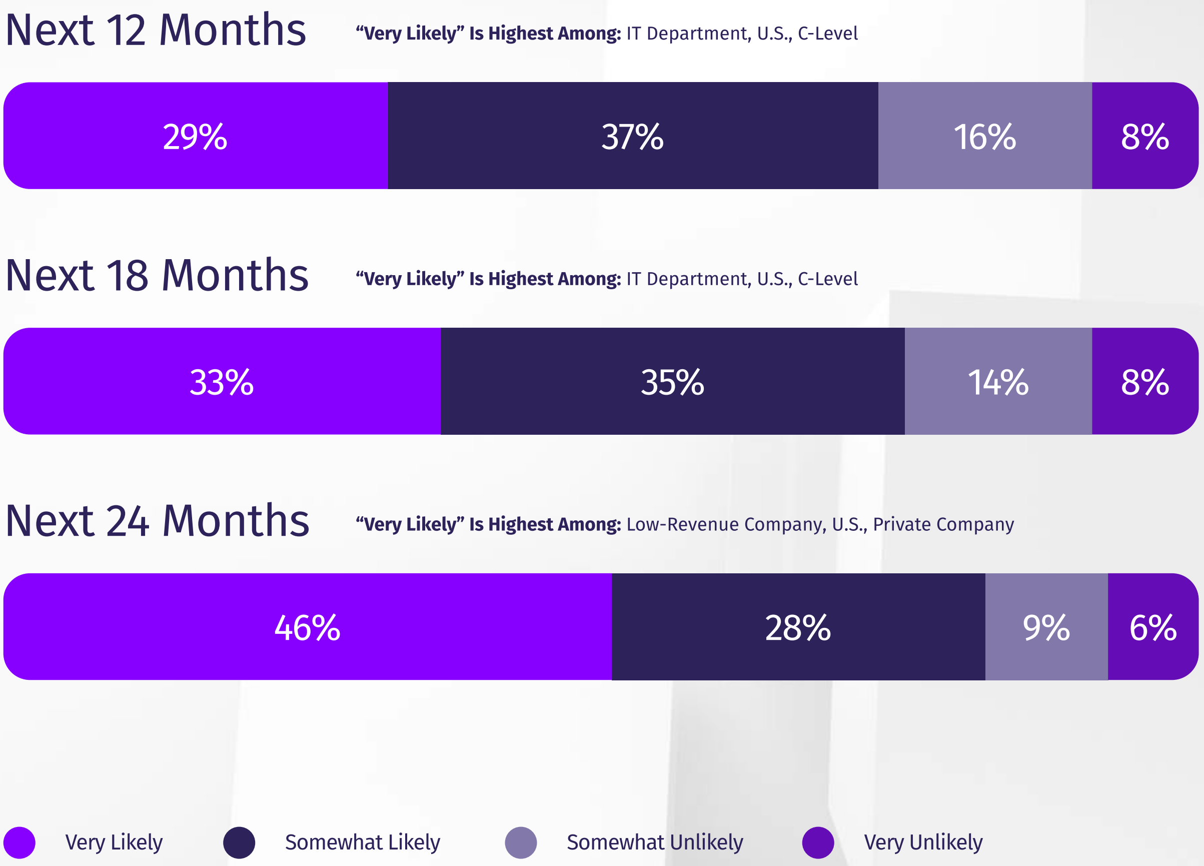
To what extent have each of the following areas changed in focus for your organization in the past 12 months?



How many people are on your organization's data protection / privacy teams?

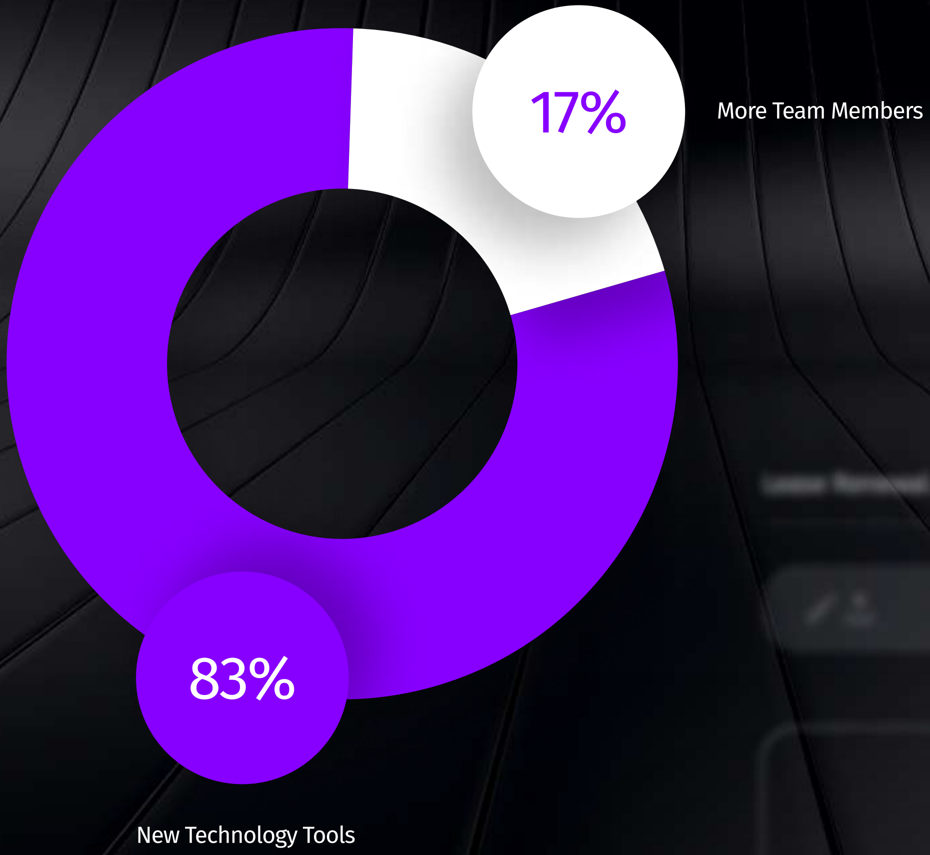


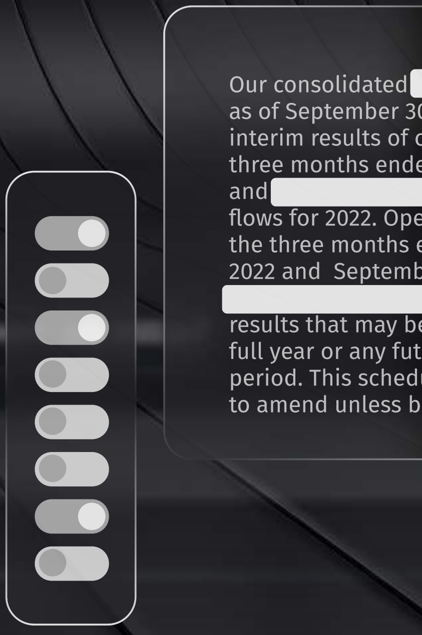
How likely is it that you will increase headcount for data protection / privacy within each of the following time periods?



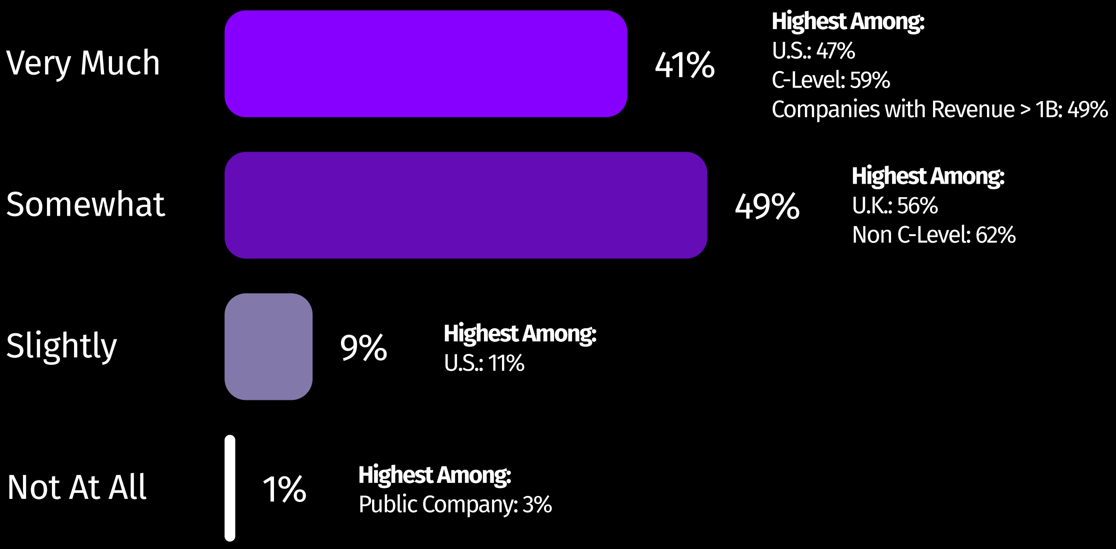
DealMaker Meter by DFIN

If you had to choose between adding more team members or adding new technology tools to support your department in the realm of data protection / privacy, which would you choose?





To what extent does your team utilize automation to support data protection / privacy functions?



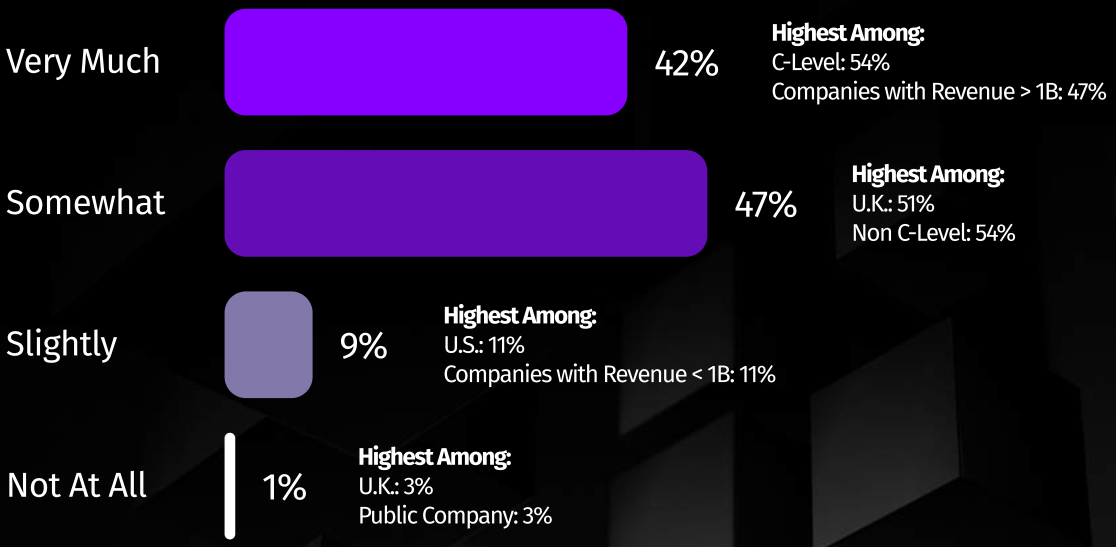
Highest Among:
U.S.: 47%
C-Level: 59%
Companies with Revenue > 1B: 49%

Highest Among:
U.K.: 56%
Non C-Level: 62%

Highest Among:
U.S.: 11%

Highest Among:
Public Company: 3%

How much do the technology tools you currently use for data protection / privacy magnify your capabilities?



Highest Among:
C-Level: 54%
Companies with Revenue > 1B: 47%

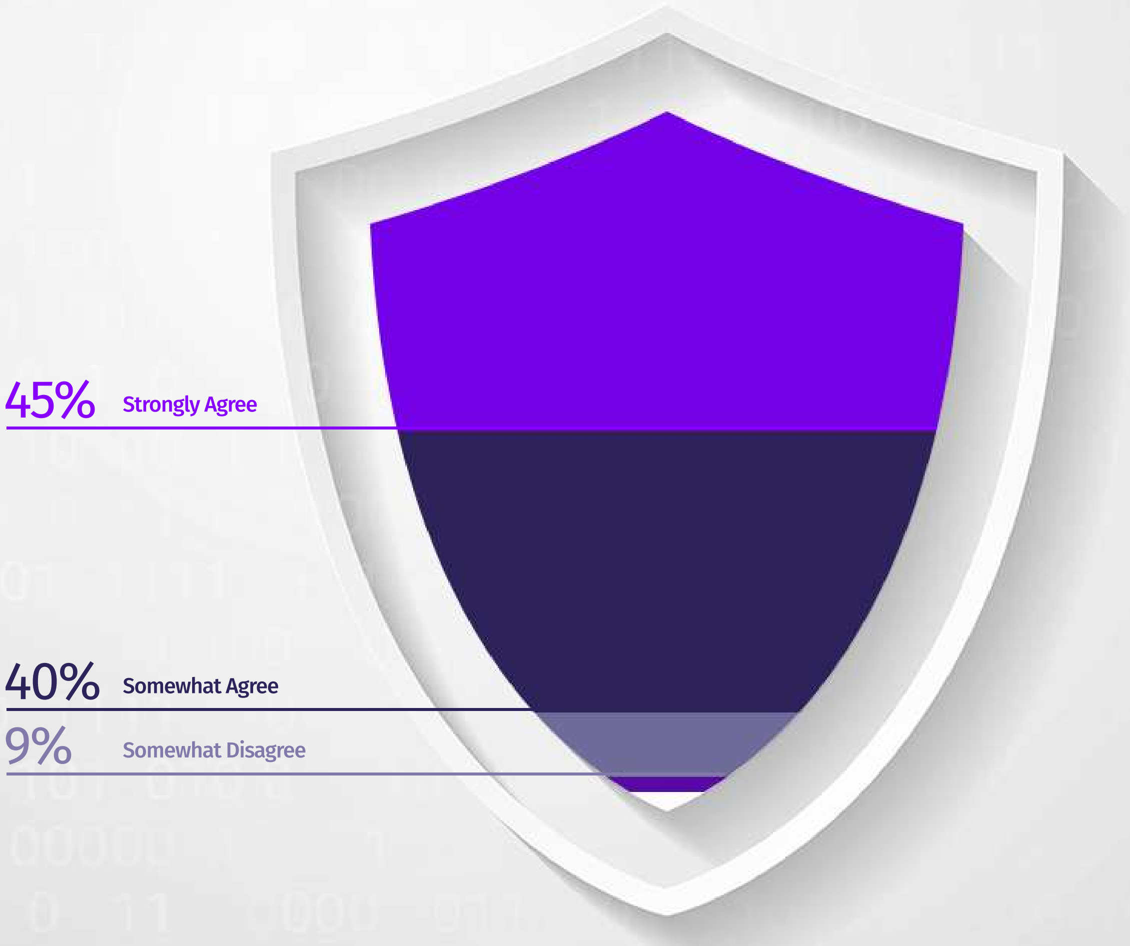
Highest Among:
U.K.: 51%
Non C-Level: 54%

Highest Among:
U.S.: 11%
Companies with Revenue < 1B: 11%

Highest Among:
U.K.: 3%
Public Company: 3%

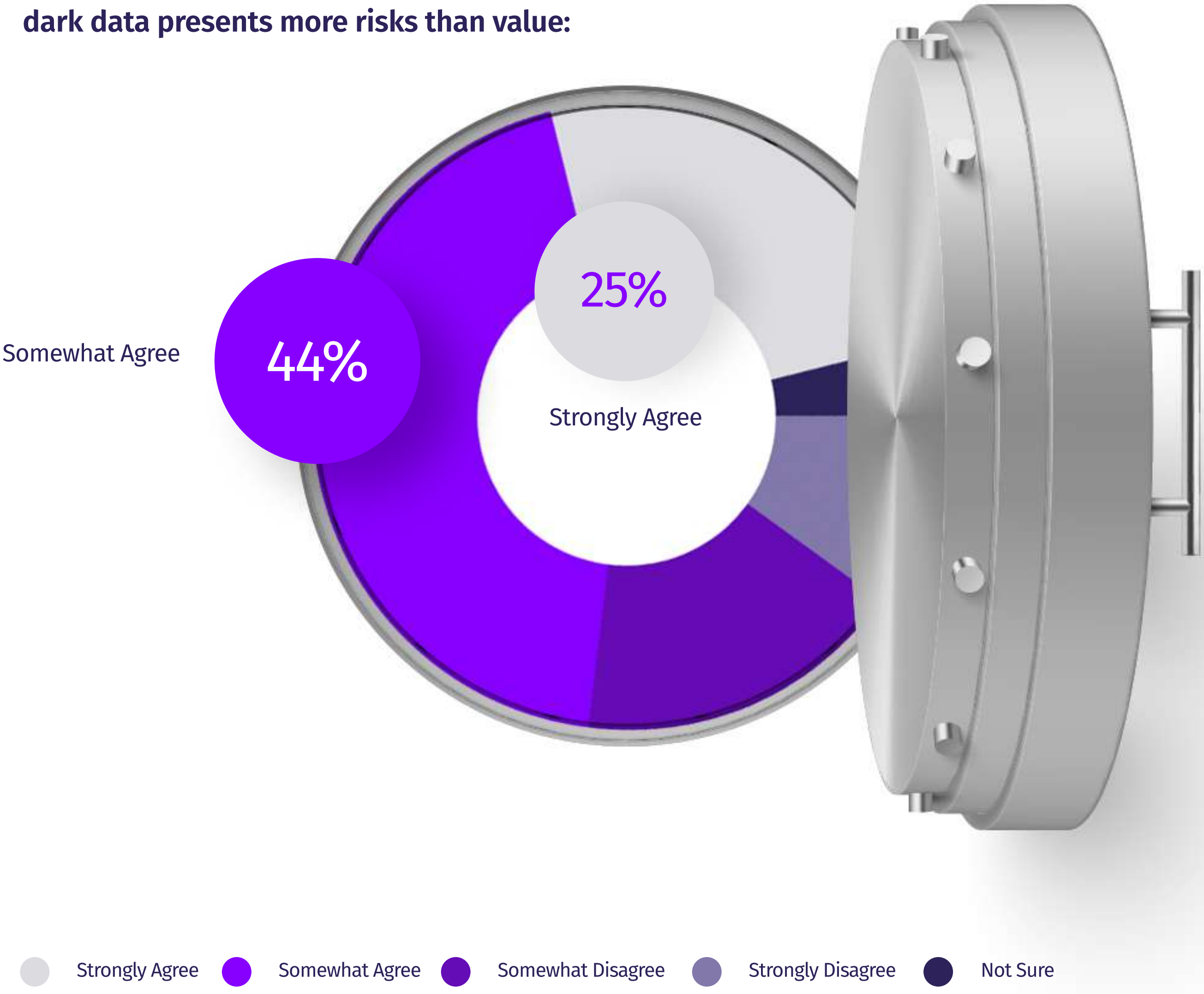
Our board members are aware and supportive of information security and data privacy initiatives.

Please indicate the extent to which you agree or disagree with the above statement:



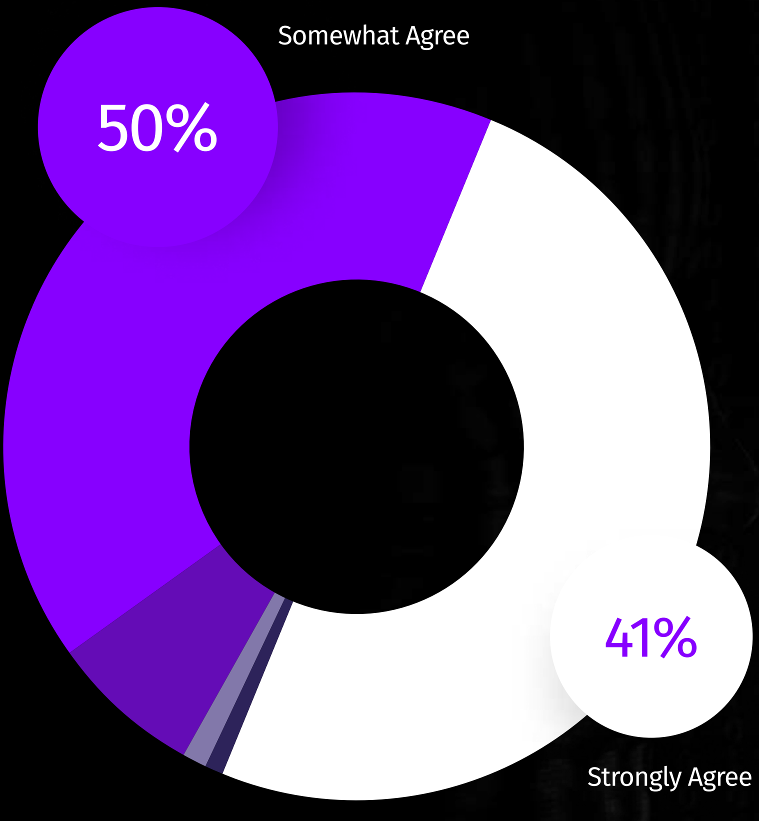
Storing detailed information (dark data) presents more risk than value say nearly 7 in 10 enterprise leaders.

Please indicate if you agree or disagree that dark data presents more risks than value:



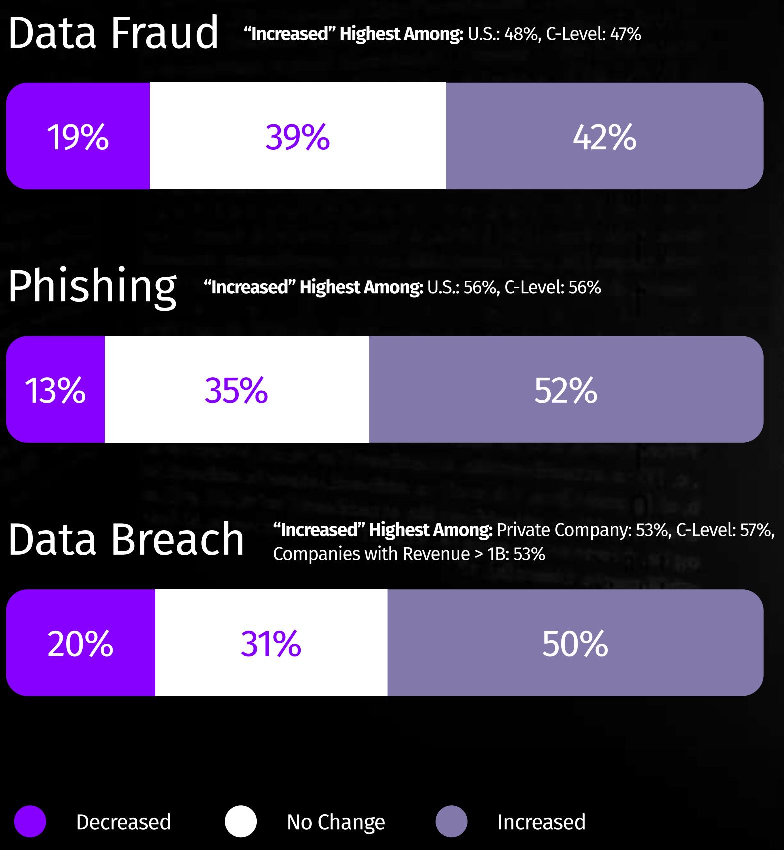
“I have the right technology tools to do my job effectively.”

Please indicate the extent to which you agree or disagree with the above statement:



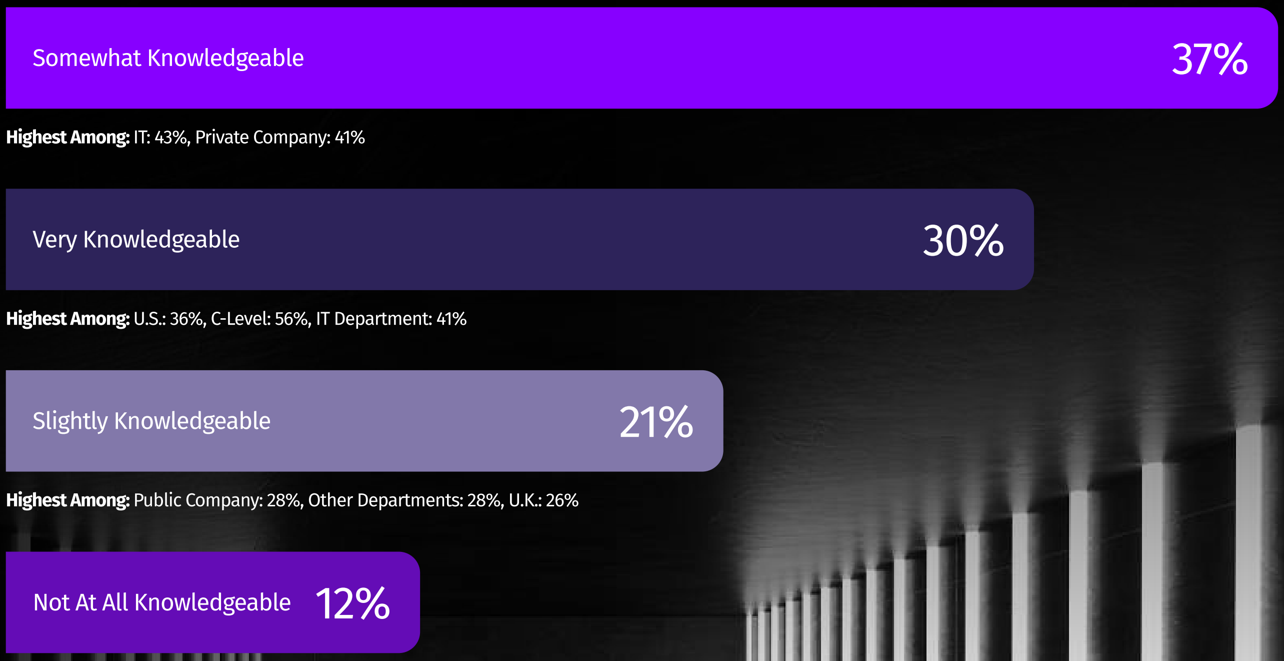
Data incidents are on the increase and will continue to grow over the next 24 months.

To your knowledge, has the number of data privacy / cybersecurity incidents in these areas changed in the past 12 months?



C-level and IT are the only groups of enterprise leaders that understand dark data is a risk.

To what extent are you knowledgeable about the potential security and legal issues associated with your department's dark data?



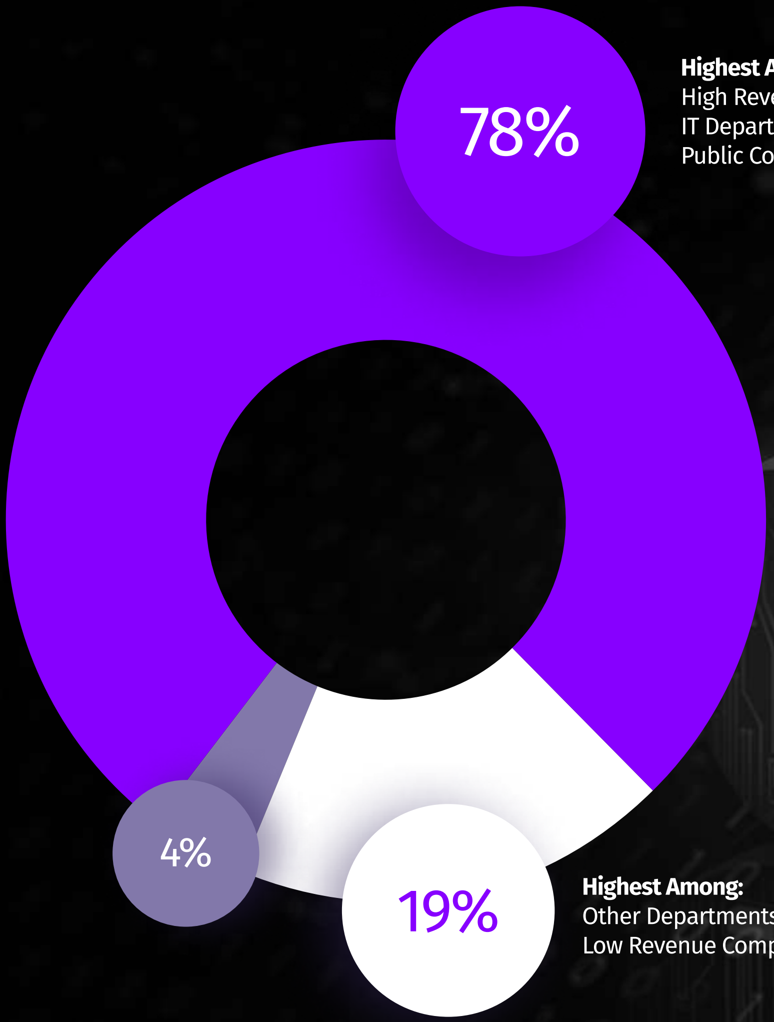
Highest Among: IT: 43%, Private Company: 41%

Highest Among: U.S.: 36%, C-Level: 56%, IT Department: 41%

Highest Among: Public Company: 28%, Other Departments: 28%, U.K.: 26%

Highest Among: Public Company: 23%, Other Departments: 23%

3 in 4 companies have a named head of information / data protection, with this being more common among high revenue and public companies.



Highest Among:
High Revenue Companies: 87%
IT Department: 83%
Public Company: 80%

Highest Among:
Other Departments: 23%
Low Revenue Companies: 22%

● Yes ○ No ● Don't Know

What is the DealMaker Meter?

Keeping your finger on the financial pulse, the DealMaker Meter compiles quarterly answers to questions about everything from activities in sectors / industries to geographies and impacts. This special edition focuses on cybersecurity and dark data.

Who answers?

A blue-ribbon panel made up of top global DFIN dealmakers / partners (advisors, corporate clients, lawyers, bankers, etc.). Respondents for this special edition were finance, legal, HR and IT professionals at large public and private companies in the U.S. and U.K.

How should I use it?

To gauge the global outlook – and plan your next move.

The Dealmaker Meter is a 2021 Platinum Award winner of the Marcom Awards honoring excellence in marketing and communication.

MarCom is administered by the Association of Marketing and Communication Professionals (AMCP). The international organization, founded in 1995, consists of several thousand marketing, communication, advertising, public relations, digital, and web professionals.

2021 MARCOM
PLATINUM
WINNER

About the survey

DFIN, along with Morning Consult, surveyed 300 professionals at large U.S. and U.K. public and private companies on Aug. 15-17, 2022. Within each evenly split market, half were IT professionals, with the other half being HR, Legal and Finance specialists.

DFIN conducted the survey to further expand its thought leadership among cybersecurity decision-makers, while at the same time gathering their input to better understand today's market.

Survey results have a margin of error of +/-6 percentage points. At the market or department level, the margin of error rises to +/-8 percentage points. As such, data should be interpreted as directional, particularly when examining subgroups within the U.S. or U.K., respectively.

About DFIN

DFIN is a leading global risk and compliance solutions company. We provide domain expertise, enterprise software and data analytics for every stage of our clients' business and investment lifecycles.

Markets fluctuate, regulations evolve, technology advances, and through it all, DFIN delivers confidence with the right solutions in moments that matter.

DealMaker Meter

by DFIN

Get in touch

DFINsolutions.com

US: +1 800 823 5304
APAC: +852 2522 3803
EMEA: +44 203 047 6100

Explore Venue