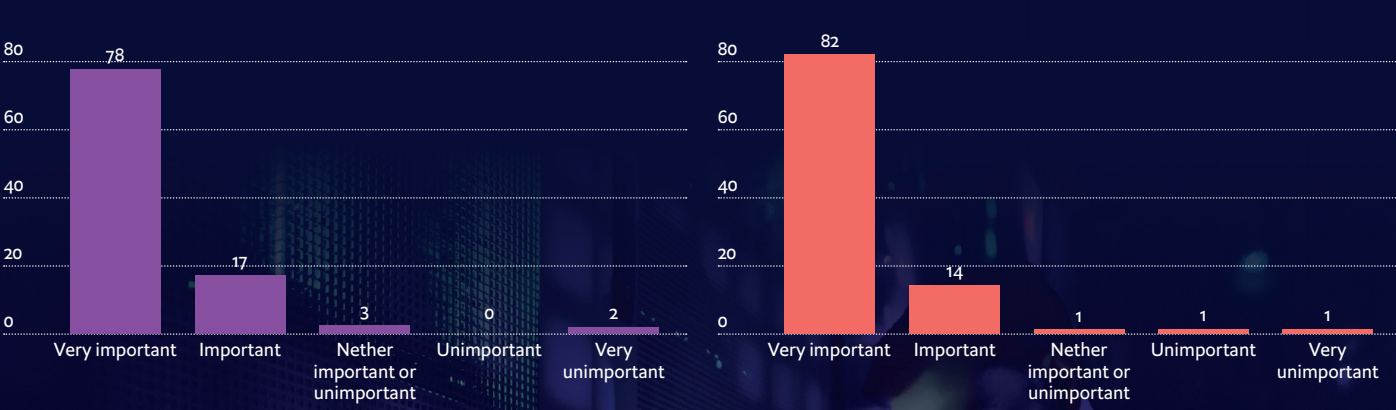# WhatsApp

Data protection ecosystems:
Unlocking strong digital economies

Daily life = data

From demographics and health information to credit card details and addresses, consumers today regularly share valuable pieces of their life through the data they exchange with companies in their transactions. How this data and the people who provide it are protected is vital to the development of a healthy digital economy.

Awareness of data protection's critical nature is growing.
Almost 8 in 10 of survey-takers (78%) say data protection is very important to their organisation. Looking toward the future, even more (82%) say it will become very important in three years.

Today
(%)

Very important	78
Important	12
Neither important or unimportant	3
Unimportant	1
Very unimportant	1

In three years
(%)

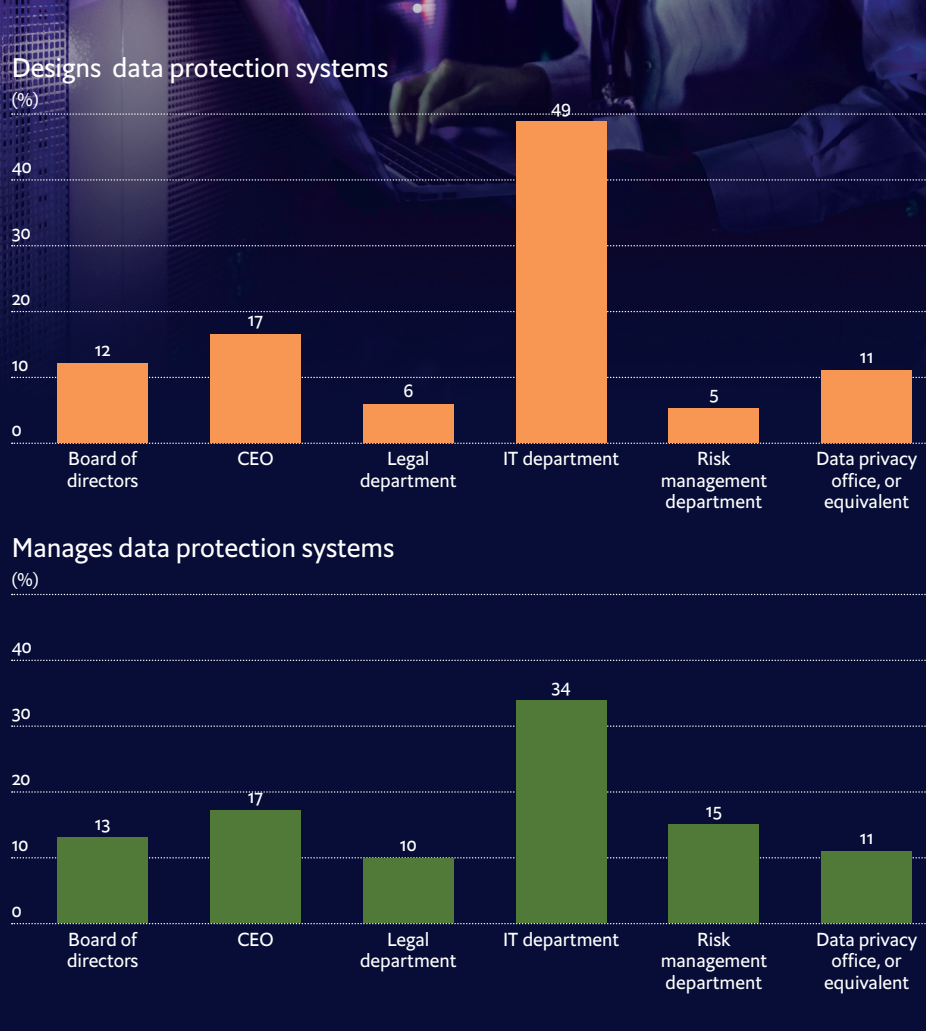|	
Very important	81
Important	14
Neither important or unimportant	1
Unimportant	1
Very unimportant	1

Not just for IT departments anymore

Data is used today more than ever to find new business opportunities. But data protection was often a second thought left to a team well outside the C-suite. However, that's changing. The issue is emerging as a key responsibility for top corporate leaders.

The awareness means senior management is involved in design and management of data protection systems.

Besides IT Departments, the CEO was the second-most involved stakeholder in designing data protection systems.

German, Brazilian and Mexican CEOs were seen as most involved.

Designs data protection systems
(%)

Board of directors	CEO	Legal department	IT department	Risk management department	Data privacy office, or equivalent
10	17	10	49	5	11

Manages data protection systems
(%)

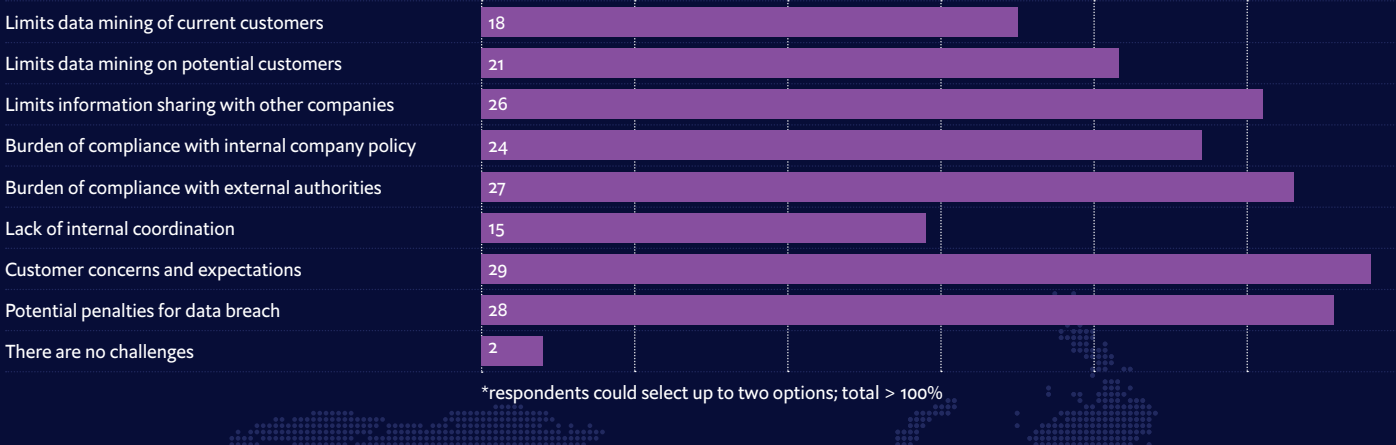| Board of directors	CEO	Legal department	IT department	Risk management department	Data privacy office, or equivalent
13	17	10	34	15	11

Challenges are vast and varied...

Regulations and customer expectations can vary greatly among jurisdictions, leading to a complex environment for all kinds of organisations to leverage data while managing it properly.

Top concern overall in the survey

"Customer concerns and expectations" was a top concern among organisational leadership. Fear of fines was close behind.*
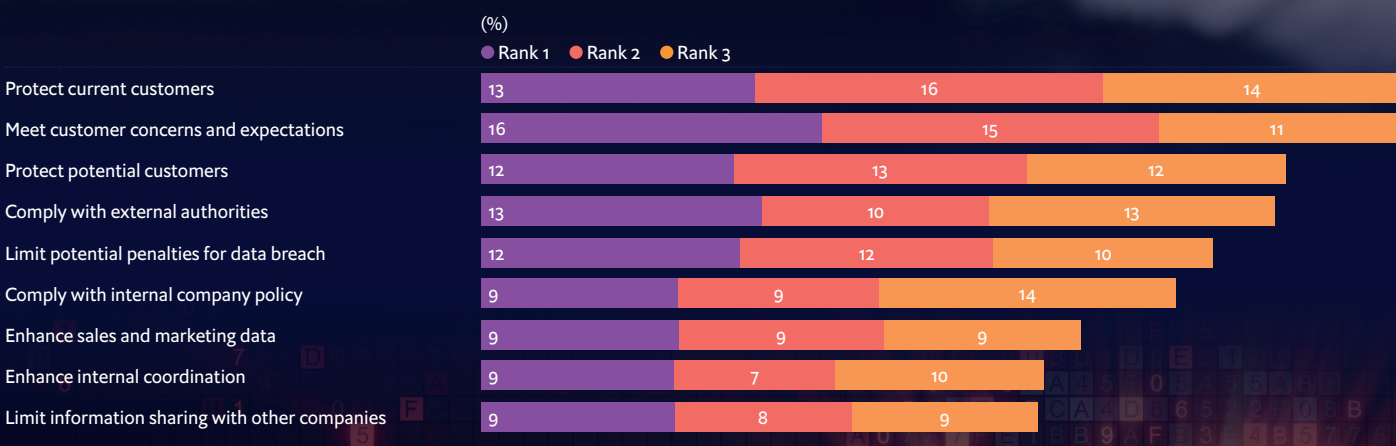
	(%) 0 5 10 15 20 25 30
Limits data mining of current customers	21
Limits data mining on potential customers	21
Limits information sharing with other companies	16
Burden of compliance with internal company policy	24
Burden of compliance with external authorities	27
Lack of internal coordination	16
Customer concerns and expectations	29
Potential penalties for data breach	28
There are no challenges	3

*respondents could select up to two options; total = 100%

Top concern by country in the EIU survey

United Kingdom
Burden of compliance with external authorities

Germany
Limits data mining on potential customers

United State of America
Burden of compliance with internal company policy

Mexico
Customer concerns and expectations

India
Customer concerns and expectations

Indonesia
Limits information sharing with other companies

Brazil
Burden of compliance with external authorities

Australia
Customer concerns and expectations

...and focused on customer satisfaction more than regulation

The customer is king. Protecting current and potential customers and meeting their concerns and expectations are seen as the top three aims of data protection in organisations.

Survey respondents were asked what are the three top aims of their organisation's data protection measures. A rank of 1 indicates "most important" and 3 "least important".

(%) Rank 1 Rank 2 Rank 3

Protect current customers	
Meet customer concerns and expectations	
Protect potential customers	
Comply with external authorities	
Limit potential penalties for data breach	
Comply with internal company policy	
Enhance sales and marketing data	
Enhance internal coordination	
Limit information sharing with other companies	

Frequent and lengthy: digital threats are a new normal

Attacks are frequent. About one-in-five survey takers (22%) say they occur daily with another one-in-five (20%) stating they occur weekly. The most common form of attack is malware (41%), followed by phishing and spear phishing (19%).
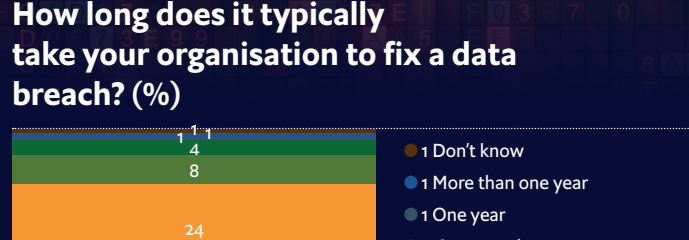
India reported the highest rate of daily attempted breaches.

Recoveries can be time consuming, costing organisations days or weeks of lost time or customer service.

How often does your organisation experience an attempted and confirmed data breach? (%)

Prefer not to know
Don't know
Every year
Every month
Every week
Every day

Attempted data breach
Confirmed data breach

How long does it typically take your organisation to fix a data breach? (%)

Don't know
More than one year
One year
One month
Two to three weeks
Two to three days
One day

Protecting data is a business's business

Increased attacks have also driven increased awareness, almost all organisations (93%) keep track of time and resources in developing, testing and securing data protection software, including encryption. Given the complexities involved they primarily do so through a mix of qualitative and quantitative data (57%). This could be the reason why 90% of EIU survey respondents say "Privacy Control" is a core organisational requirement in their country.

Those rating privacy control as a core business requirement in their country. (%)

1 Strongly disagree 2 Disagree 6 Neither disagree or agree 37 Agree 53 Strongly agree

Response was strongest in Brazil where 98% agree or strongly agree

Percent of respondents who say their organisation tracks the time and resources needed to develop, test and securing data protection software. (%)

5 No
2 Don't know
93 Yes
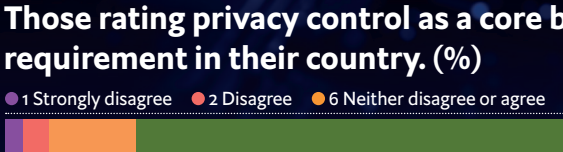
Primary methods respondent organisations use to track time and resources for developing, testing and securing data protection software. (%)

1 Don't know
19 Quantitative
57 A mix of quantitative and qualitative
23 Qualitative