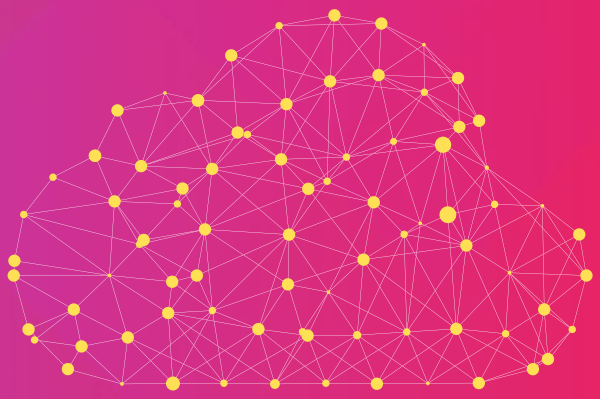
iomart

CYBER SECURITY INSIGHTS REPORT 2020



iomart

INTRODUCTION

The purpose of the *iomart* Cyber Security Insights Report is to gather insights from large-to-medium businesses to reveal the level of understanding around cyber security and data protection in the workplace.

The survey consists of 10 questions and 1,167 responses, which are broken down into job category and company location where relevant.

Of the 1,167 respondents surveyed:

91	were C-level employees (those who hold top positions in a company)
22	were directors
312	were employees
230	were managers

iomart

INTRODUCTION

Continued

Of the replies:

256	responses were from businesses that operate in Europe
711	were from businesses that operate in the UK
243	came from businesses that operate in the U.S.

It is important to note that some of the surveyed businesses operate in more than one region.

iomart

INTRODUCTION

Continued

The survey found that businesses are concerningly complacent about cyber security and data breaches, with the respondents indicating that a lack of training and inadequate disaster recovery policies are key factors behind this.

The findings highlight that businesses need to place more focus on providing cyber security training and cementing recovery processes, particularly in the UK, as respondents reported a significant increase in data breaches and phishing attacks following the shift to remote working.

Continue reading the iomart Cyber Security Insights Report for a detailed breakdown on the survey results and for expert advice on how businesses can avoid a cyber attack.

iomart

KEY FINDINGS

52%

More than half (52%) of respondents said that cybersecurity was not a priority for the business

20%

Almost 20% of respondents said they had seen an increase in cyber attacks due to remote working

70%

A huge 70% of respondents said that the business does not currently offer cyber security training to all employees

42%

Just 42% of respondents said the business offers some training to select employees

46%

Almost half (46%) of the C-level respondents claimed they do not have any backup policies in place in the event of an incident, but said implementing them is on their 'to-do' list

iomart

KEY FINDINGS

Continued

25%

A quarter (25%) of respondents said they do not have a disaster recovery policy

60%

While 60% of those surveyed claim they do conduct cyber security due diligence on their IT suppliers, a further 20% of respondents claimed that they either cannot confirm having done so, or that their company does not conduct due diligence.

The survey also found that...

- The main reason for businesses not offering cyber security training to employees was a lack of budget
- Directors also had the least faith in their colleagues' abilities to identify a scam or data breach, yet were also least likely to consider cyber security a key business concern

iomart

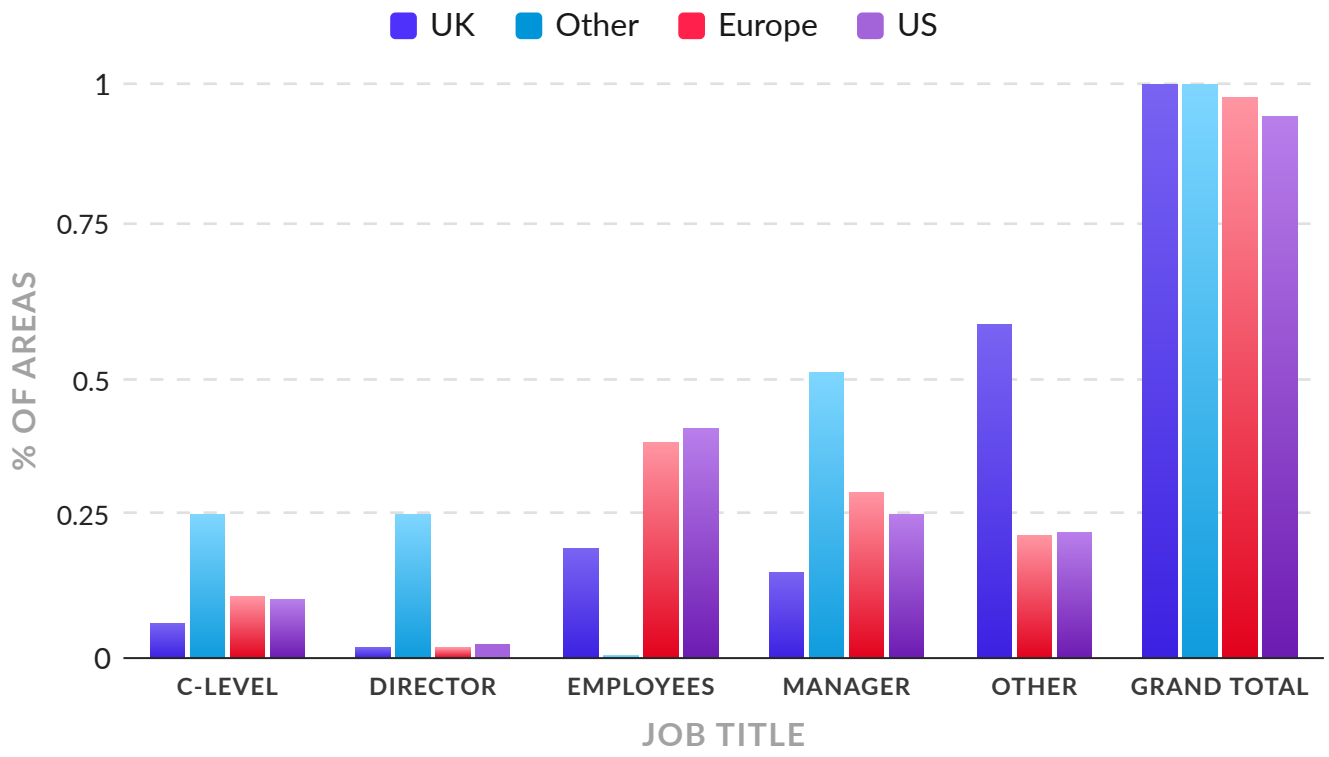
QUESTION ONE

In which area[s] does your business currently operate/serve?

The majority of respondents operated in the United Kingdom, with other prevalent markets being the U.S. and Europe. Of those surveyed in the U.K:

- 16% of respondents were managers
- 6% held C-level roles
- 2% held director roles
- The rest were either employees or held non-technical job roles

Similarly, the U.S. and European market also consisted of 11% of C-level respondents, while almost 40% of workers held employee positions across both markets. Furthermore, 26% of those surveyed in the U.S. and 29% of those in Europe held a managerial role.

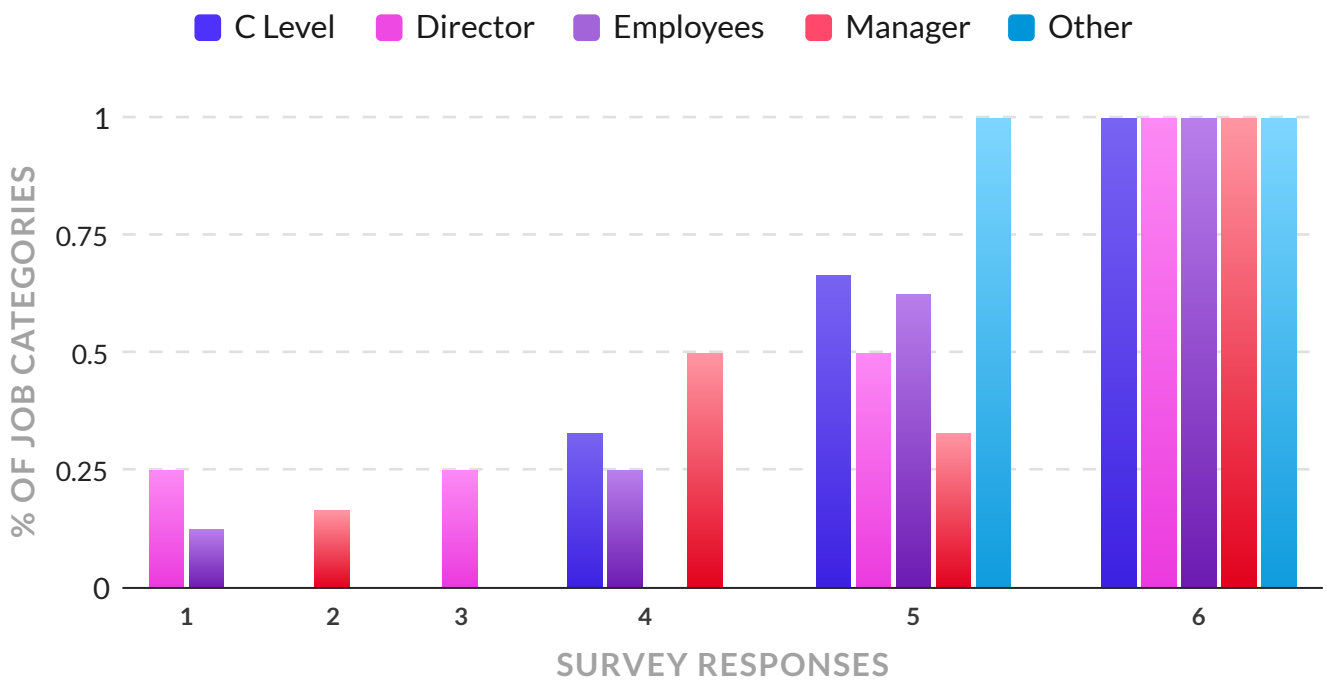


iomart

QUESTION TWO

Does your business monitor its cyber security 24/7?

Of the respondents who occupied C-level positions, 33% claimed that cyber security was outsourced to a third party. While half of those in managerial roles responded saying they were managing cyber security internally, 13% of employees reported not monitoring systems for threats at all.



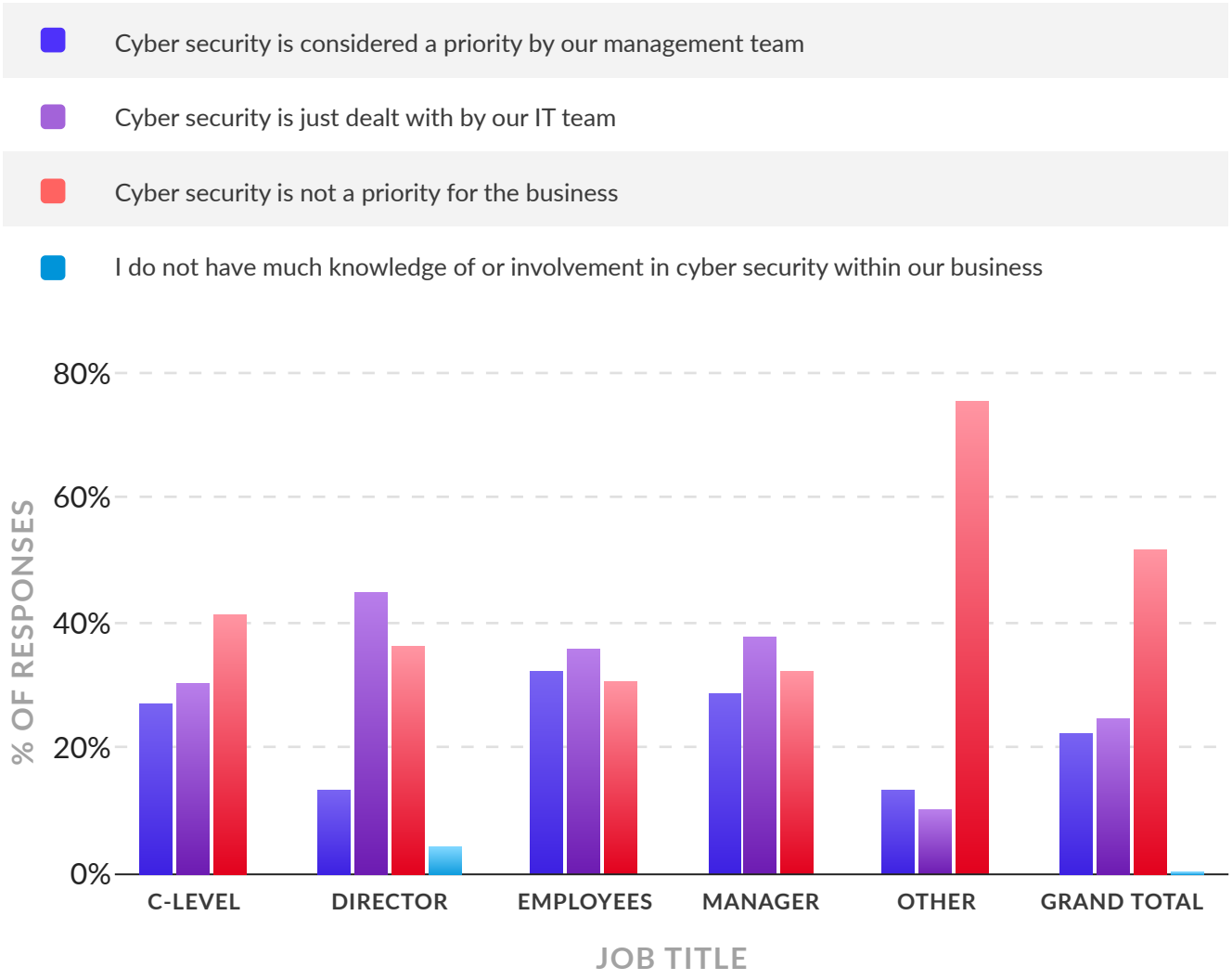
1	No, we do not monitor our systems for threats
2	We periodically check firewall for threats
3	We use all cloud based systems
4	Yes, it's outsourced to a third party
5	Yes, we manage this internally
6	Grand total

iomart

QUESTION THREE

Which of the following statements do you agree with in regards to how security is handled in your company?

Concerningly, more than half of respondents (52%) claimed that cyber security was not a priority for the business. This included 37% of directors, 42% of those in C-level positions, and 33% of managers. Those in director roles also admitted having the lowest level of involvement in business cyber security compared to any other position.

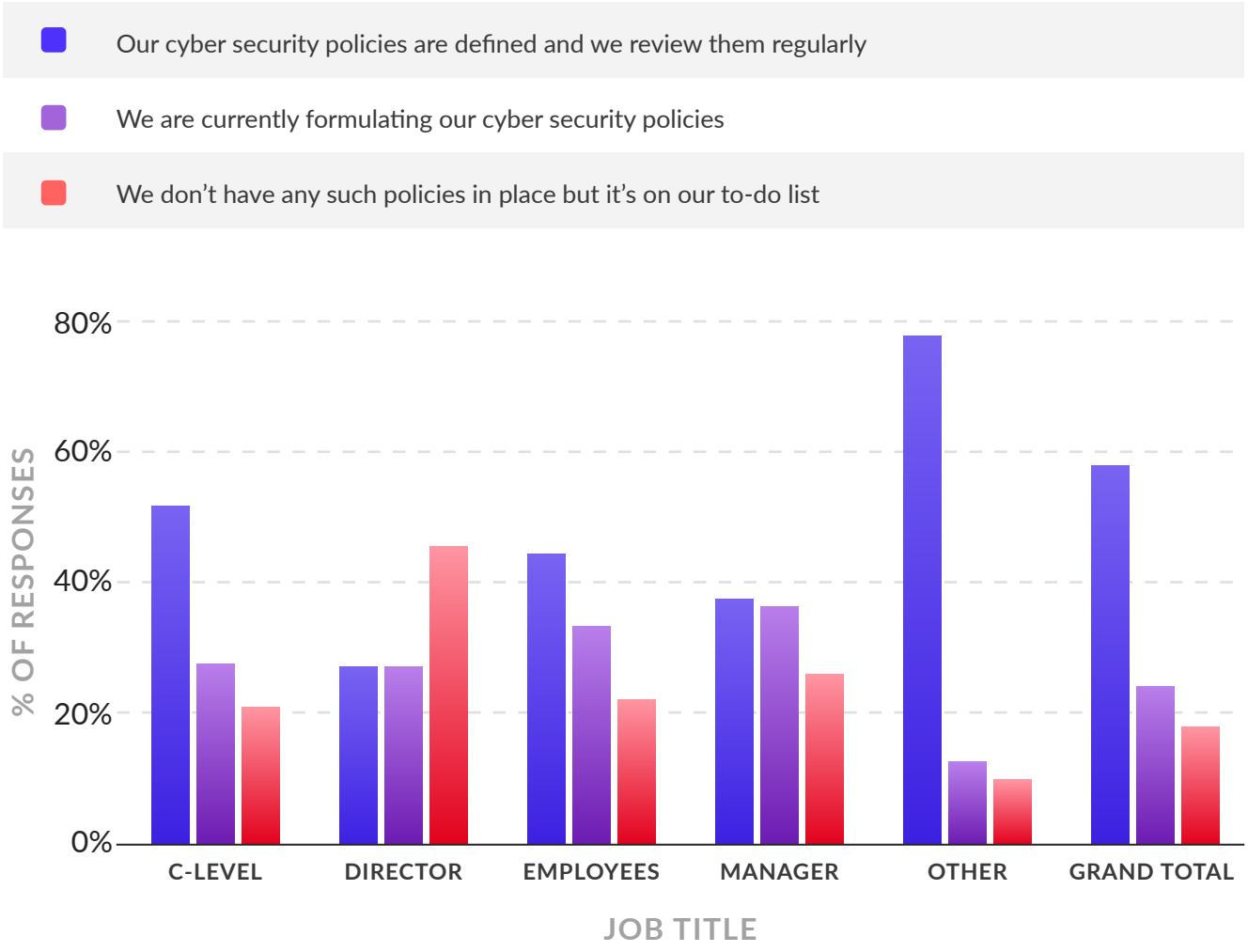


iomart

QUESTION FOUR

Which of the following statements do you agree with regarding the security policies you have in place?

While over half (52%) of respondents in C-level positions claimed their cyber security policies were defined and regularly reviewed, a staggering 46% of directors admit not having such policies in place.



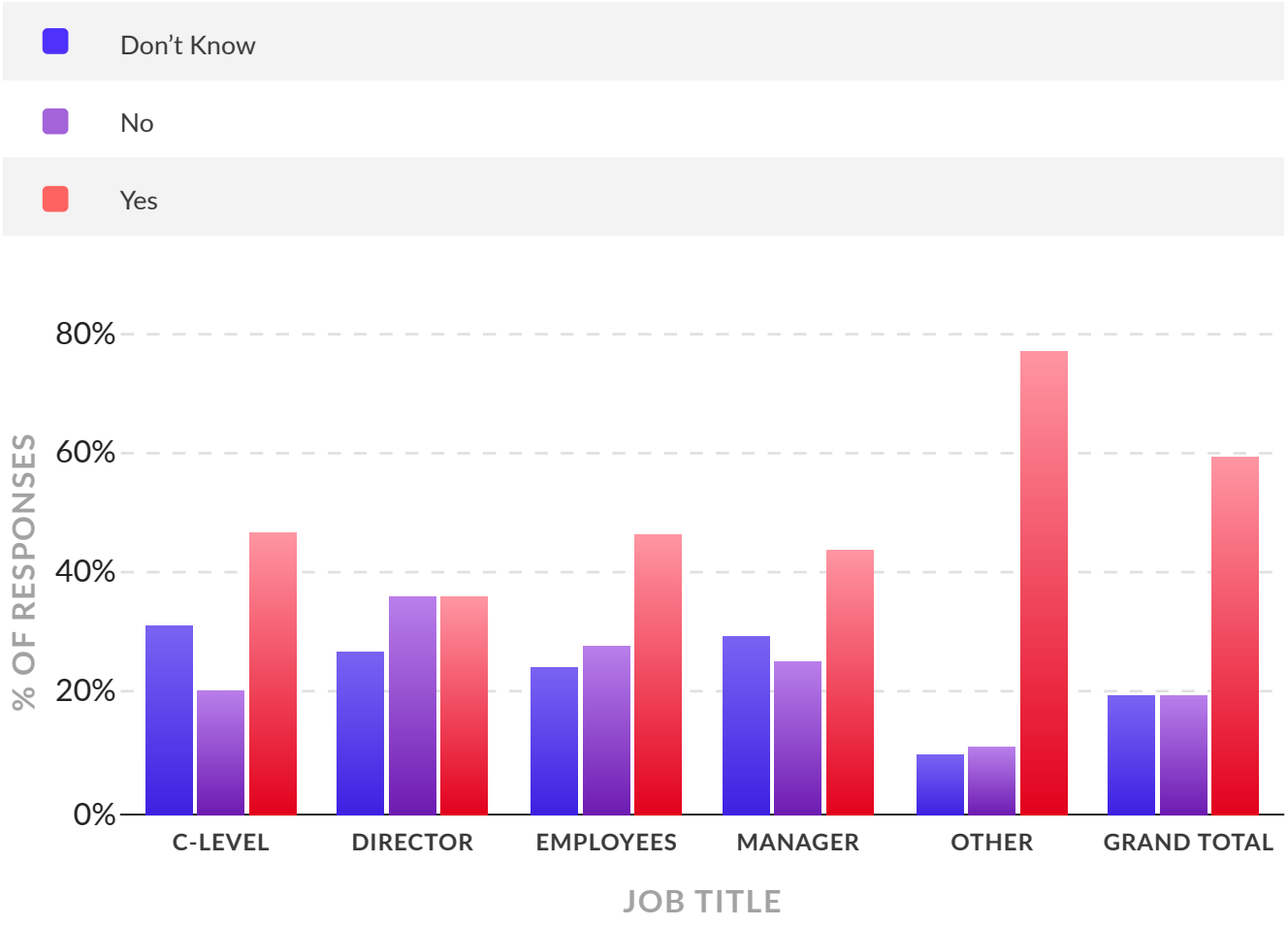
Overall, 25% of the respondents stated they were currently formulating their cyber security policies, while 18% revealed they had no such policies in place but were planning to implement them at some stage.

iomart

QUESTION FIVE

Do you conduct cyber security due diligence on your IT suppliers?

Of those surveyed, around 60% of respondents admit not conducting cyber security due diligence on their IT suppliers, while a further 20% claimed they either did not know or did not conduct due diligence.



iomart

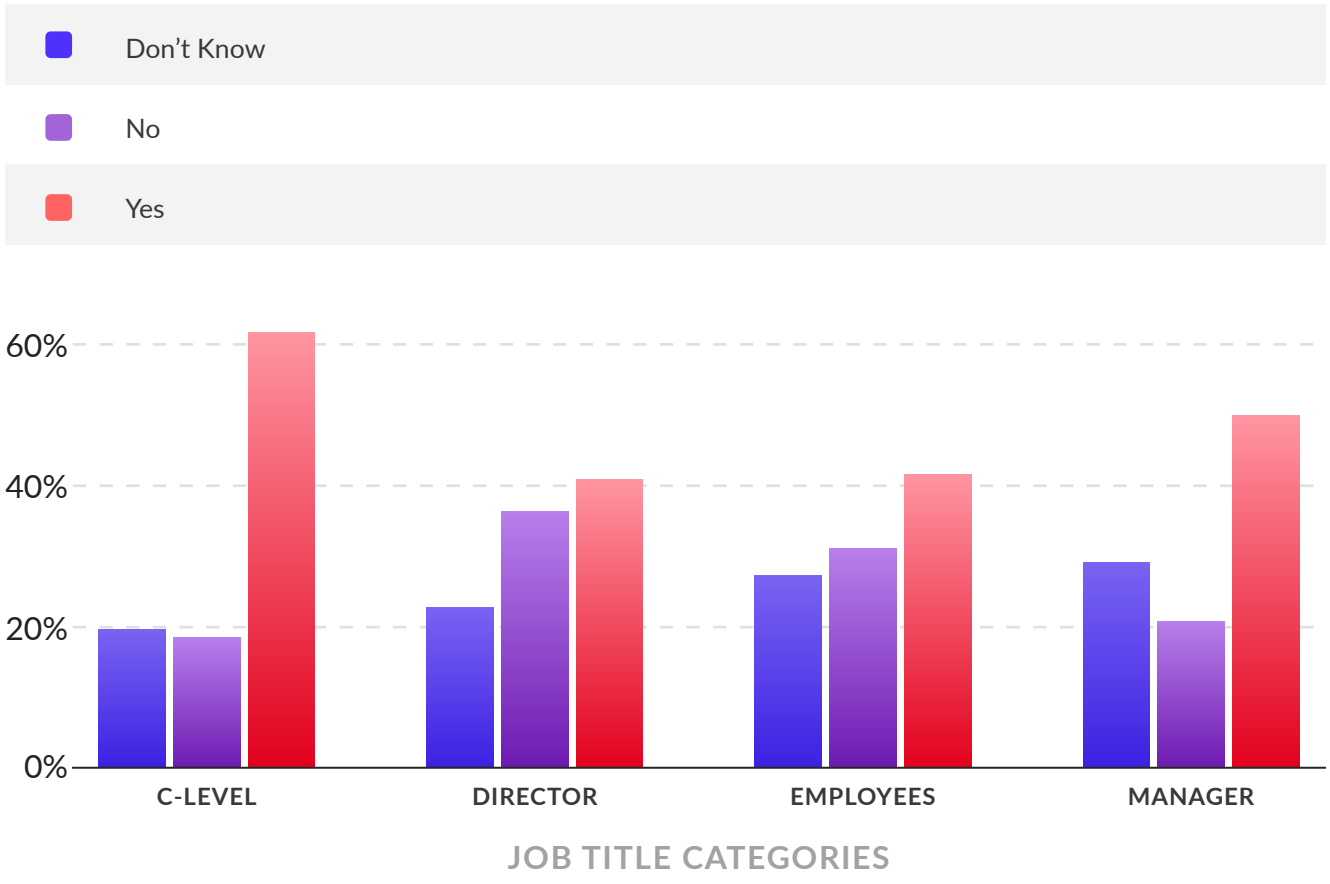
QUESTION SIX

Do you have a defined backup policy for your critical business data?

47% of respondents said they had a backup policy have a backup policy in place

27% of respondents said they did not know whether there was one in place

26% of respondents said they did not have a backup policy in place



iomart

QUESTION SIX

Continued

Role Breakdown

The role that was the most out of the loop regarding data backups was managers with more than a quarter (29%) of them admitting they did not know whether a policy was in place.

Meanwhile, the position with the most knowledge around data backups was the C-suite, but 20% of those respondents still stated they did not know about a policy.

Region Breakdown

The businesses that operated in the U.K. were found to be both more certain of their position on data backups and had the greatest proportion with backup plans in place. In contrast, businesses that operated in the U.S. showed the least certainty around their data backups, with 31% of respondents admitting to having no knowledge of a policy.

iomart

QUESTION SEVEN

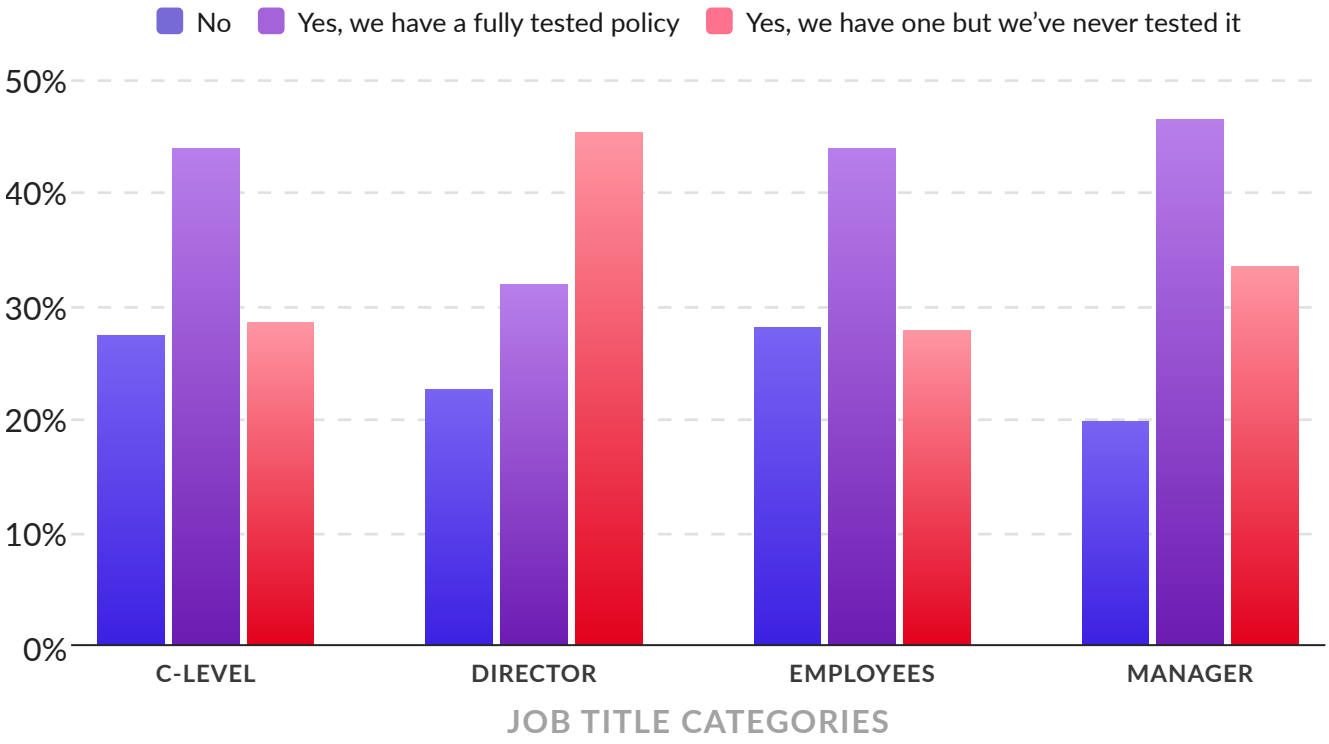
Do you have a disaster recovery policy?

Worryingly, a quarter (25%) of respondents said they did not have a disaster recovery policy, while a further 31% said they had one but that they had never tested it.

Role Breakdown

The largest proportion of those surveyed (28%) who admitted having no disaster recovery policy operate at employee level.

Theoretically, if a company did have a policy in place and all of the workforce is aware of it then the distribution of answers for each role should be similar. It is therefore possible that lower level employees were the least aware of company policies and so answered no, rather than this indicating that 28% of companies have no disaster recovery plan.

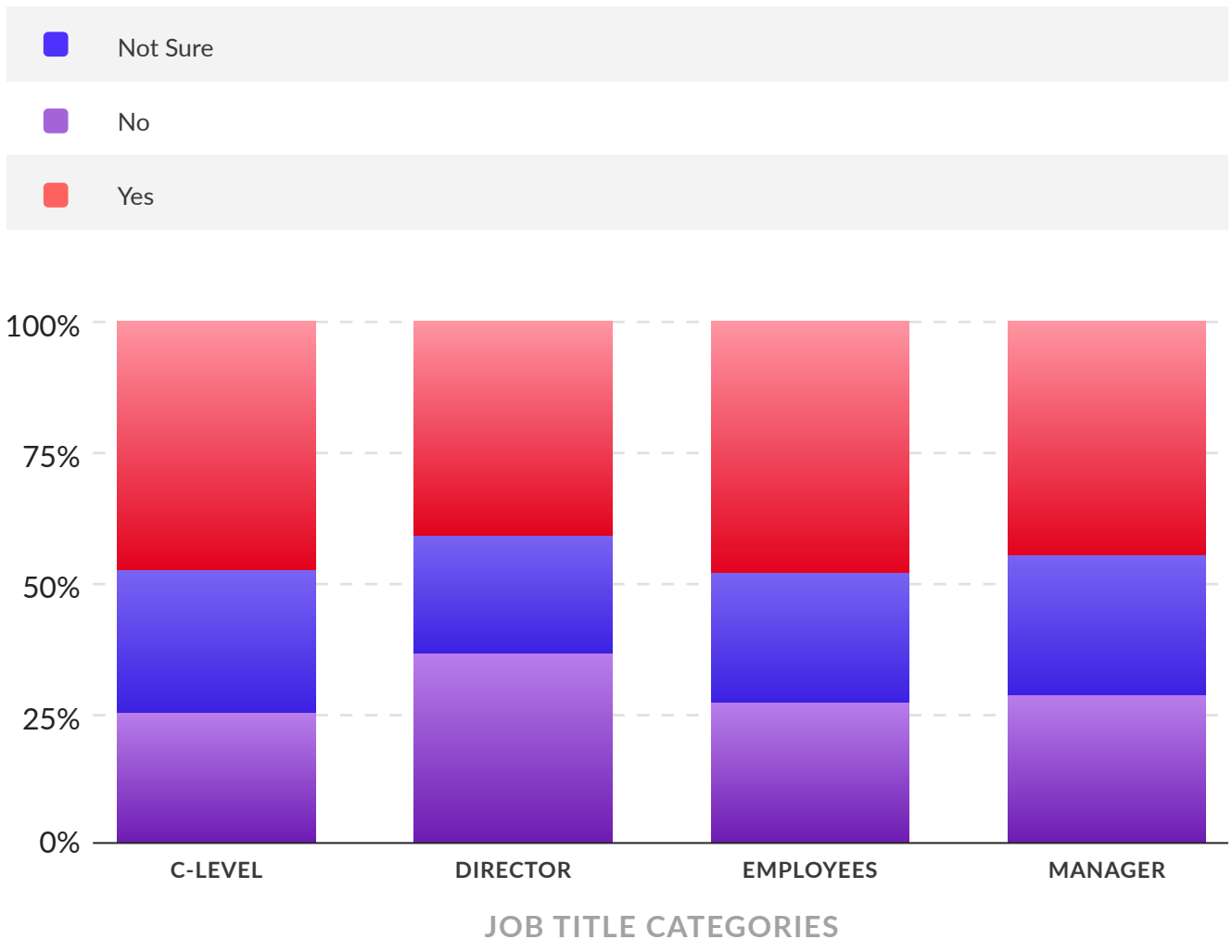


iomart

QUESTION EIGHT

Does the business currently provide cyber security awareness training to its employees?

Less than half (46%) of those surveyed said they did provide cyber security awareness training, while over a quarter of respondents (28%) admitted to not offering training at all.



iomart

QUESTION EIGHT

Continued

Role Breakdown

Surprisingly, the largest proportion of 'not sure' responses came from C-level employees, as 28% of those surveyed admitted being unsure as to whether their company offered cyber security awareness training.

Location Breakdown

UK led the way for security awareness training with 77% of respondents in that market confirming they offered training. The U.S. fell behind with just 35% having received training and 32% of respondents claiming the business offers no training at all.

iomart

QUESTION EIGHT A

If the business offers cyber security training, what does this include?

Of the respondents who confirmed receiving training, a huge proportion (82%) admitted this training consisted of a short briefing rather than a comprehensive course. Only 17% of those who were offered training, had regular sessions relating to cyber security.

This means that out of all those surveyed, just 8% of respondents received regular cyber security training.

Role Breakdown

The only standout finding in the role breakdown was the proportion of managers that claimed the business provided regular in-house training at 18%. It is possible that different levels of the workforce receive different intensities of training, with managers likely requiring the most on-going sessions.

iomart

QUESTION EIGHT B

If the business does not offer cyber security training, what are the main reasons for not doing so?

This question yielded multiple-choice answers with the following options available:

- Lack of budget
- Cyber security training for staff is not a priority for the business
- We do not have the technical expertise to implement it

Interestingly, the majority (88%) of respondents who claimed their business offered no training did not select one of the above options.

Of those who did select one of the above options, 8% of respondents said the main contributing factor was that the business lacked technical expertise, 7% attributed insufficient training to a lack of budget, and 5% said cyber security training was not a main priority for the business.

Role Breakdown

A quarter of directors believe budget was the main factor behind a lack of cyber security training, while just 4% of C-level employees think the same. Furthermore, directors were also most likely to believe cyber security was not a business concern and that a lack of training can be attributed to a lack of technical expertise.

This could indicate a lack of awareness in companies with employees trusting both their own and their colleagues expertise, whereas directors and those at higher levels do not possess this trust.

iomart

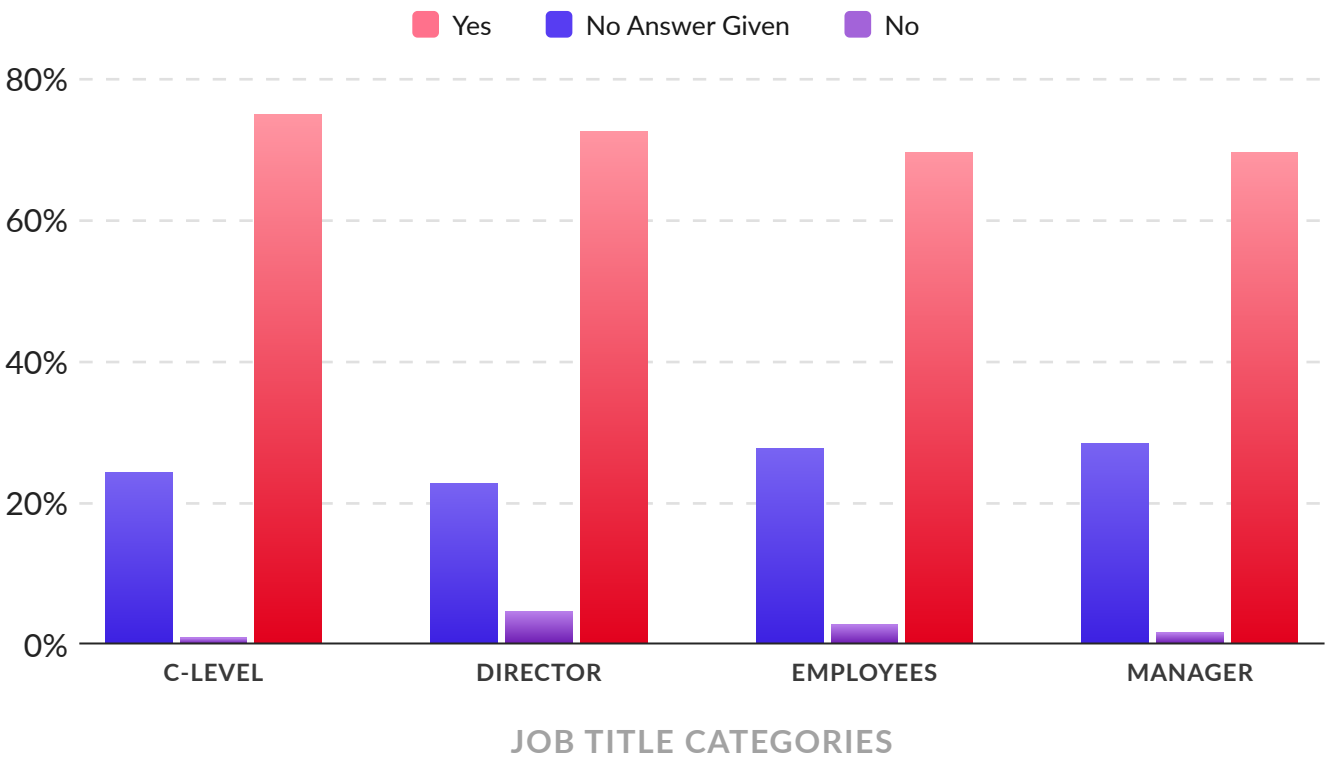
QUESTION NINE

Do you believe that the majority of your current employees have enough knowledge to identify a phishing email attack against the business?

Of those surveyed, 79% of respondents believed their employees could identify a phishing attack, while a further 20% did not respond.

Role Breakdown

Those at director level had the least faith in their colleagues with 5% believing they could not identify a phishing email, compared to 75% of C-level executives who believed their employees were capable of identifying an email attack.



iomart

QUESTION 10

Which of the following statements do you agree with?

Question 10 was a multiple-choice question that allowed for multiple selections, with the following options:

- The business does not currently offer cyber security training to all of its employees
- The business only offers cyber security training to some employees
- Cyber security and its importance is often overlooked within the business
- Cyber security and its importance should be a bigger priority for the business
- Cyber security is not a priority for the business and won't be for a long time
- The business has seen an increase in cyber/ data hacks due to remote working

Of those surveyed, 20% did not select one of the above options. 71% said the business does not currently offer cyber security training to all of its employees, while a further 43% said the business only offers cyber security training to select employees.

Concerningly, almost a quarter (22%) of respondents said cyber security was not a priority for the business. This is problematic given that 19% of respondents said they had seen an increase in cyber attacks due to remote working

Role Breakdown

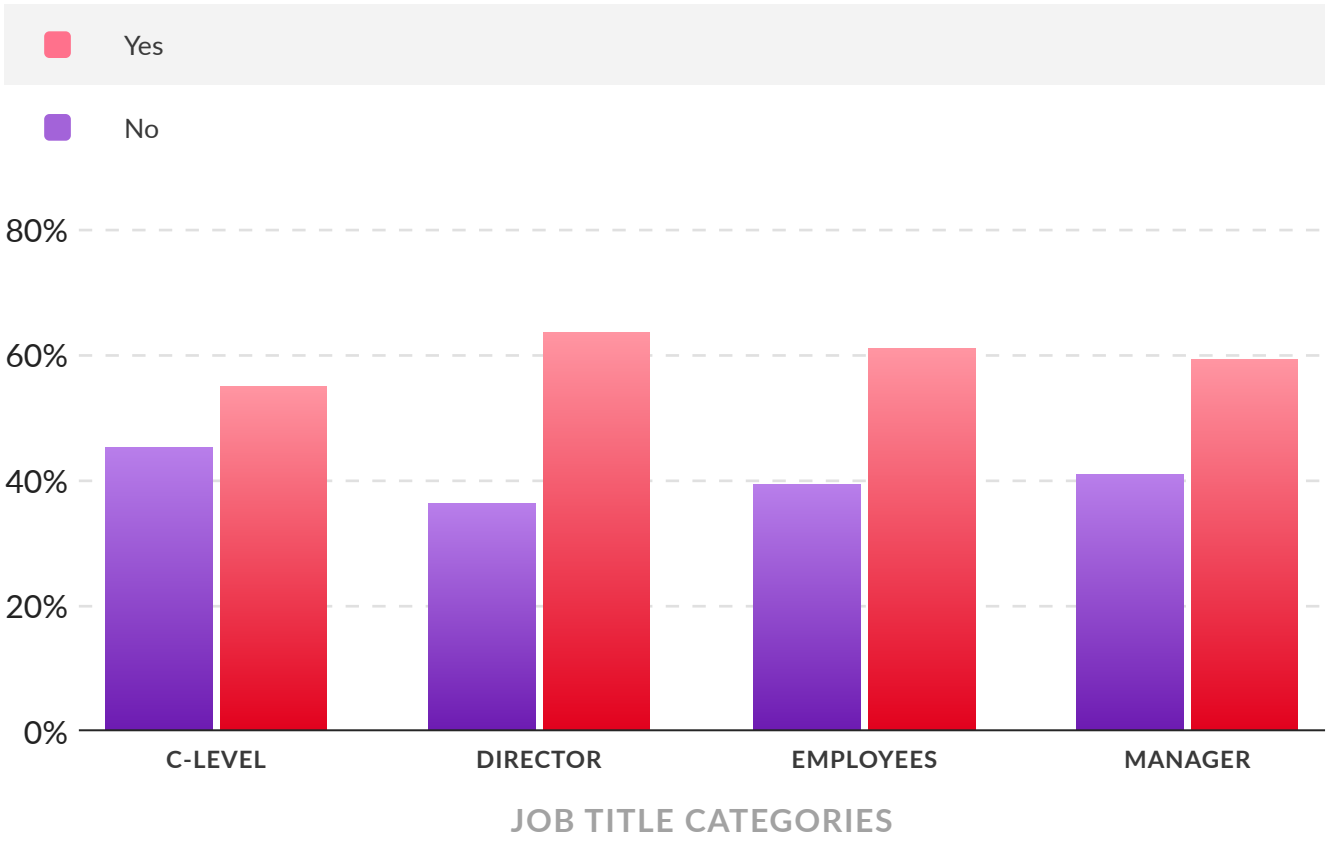
More than half of respondents across all job roles believed the business did not currently offer cybersecurity training, with directors accounting for the highest proportion at 64%. When it comes to the businesses that offer training to select employees, C-level employees accounted for the highest proportion of respondents that believed this was not the case, while 62% of employees claimed some of the workforce received training.

iomart

QUESTION 10

Continued

The business does not currently offer cyber security training to all of it's employees



Of those who believed cyber security and its importance was often overlooked in the business, directors accounted for the highest proportion at 9% - three times the proportion of employees who felt the same at 3%.

Despite this, only 6% of respondents said cyber security should be a bigger priority for the business. Directors were the least in agreement with that statement, while almost a fifth (20%) of C-level employees felt cyber security should be more of a priority.

This demand for increased focus on cyber security training is particularly important given that 19% of respondents witnessed an increase in cyber attacks while working remotely.

iomart

SUMMARY

It is clear that there is a lack of awareness around the importance of cyber security across the board and in all markets - even for the businesses who prioritise disaster recovery processes and workforce training. In order to combat an increased incidence of phishing attacks and related incidents that have resulted from remote working, adequate training needs to be given to those in all job roles, including directors and managers as well as employees and C-level workers.

What the experts say

Bill Strain, security director of iomart, warns that businesses are at risk if they do not have a secure back-up plan and solutions in place, stating:

"It's clear that many organisations still don't consider cyber security and data protection to be a top priority. They need to understand what the potential threats are and build resilience into their business strategy so they can react quickly and maintain operations if their IT systems are compromised. Many businesses would not survive the operational, let alone the financial impact of a successful cyber attack or data breach."

"By understanding the potential risk and introducing positive behaviour around cyber awareness throughout the business they have a much better chance of protecting it if the worst does happen."

SUMMARY

Continued

To reduce the pressure of monitoring complex systems and handling time-consuming backup policies in-house, businesses should consider investing in *data protection* and *security solutions* from managed services specialist iomart.

Secure data backup, disaster recovery, and security as a service provide organisations with the safety blanket they need to survive in the event of a breach.