

# UK business confidence in cyber security survey 2021

We asked business and technical leaders of midsize organisations in the UK to tell us how well prepared they are to mitigate and respond to cyber risk in 2022. Here's what they told us...

## RESULTS\*

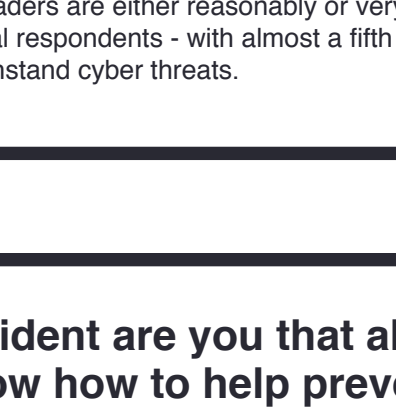
**norm.**<sup>TM</sup>

### Attitudes to cyber security

#### 1. How confident are you that your organisation is sufficiently protected against cyber threats?



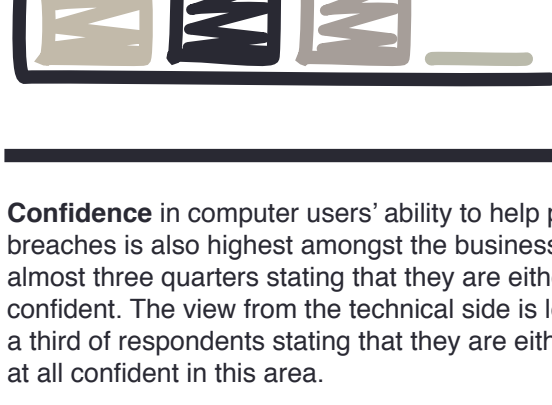
**Business personas**  
 Very confident 20%  
 Reasonably confident 72.5%  
 Not very confident 7.5%



**Technical personas**  
 Very confident 7.7%  
 Reasonably confident 73%  
 Not very confident 19.3%

Overall, confidence in levels of protection is higher amongst business leaders than technical. Over 92.5% of business leaders are either reasonably or very confident, with that number dropping to 80.7% amongst technical respondents - with almost a fifth of them not very confident about their organisation's ability to withstand cyber threats.

#### 2. How confident are you that all of your computer users know how to help prevent a cyber or data protection breach?



**Business personas**  
 Very confident 15%  
 Reasonably confident 57.5%  
 Not very confident 27.5%  
 Not at all confident 0%



**Technical personas**  
 Very confident 11.5%  
 Reasonably confident 50%  
 Not very confident 30.9%  
 Not at all confident 7.6%

Confidence in computer users' ability to help prevent cyber breaches is also highest amongst the business leader group with almost three quarters stating that they are either reasonably or very confident. The view from the technical side is less rosy, with over a third of respondents stating that they are either not very or not at all confident in this area.

#### 3. Does your organisation have a tried and tested cyber incident response plan?



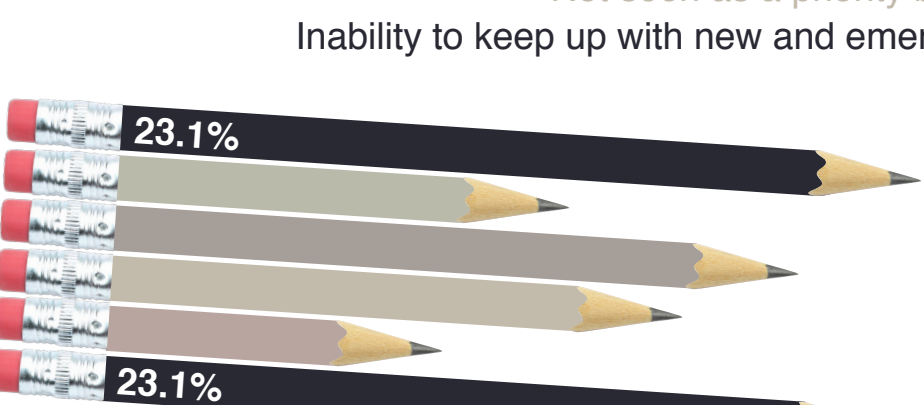
**Business personas**  
 Yes 75%  
 No 17.5%  
 Don't know 7.5%



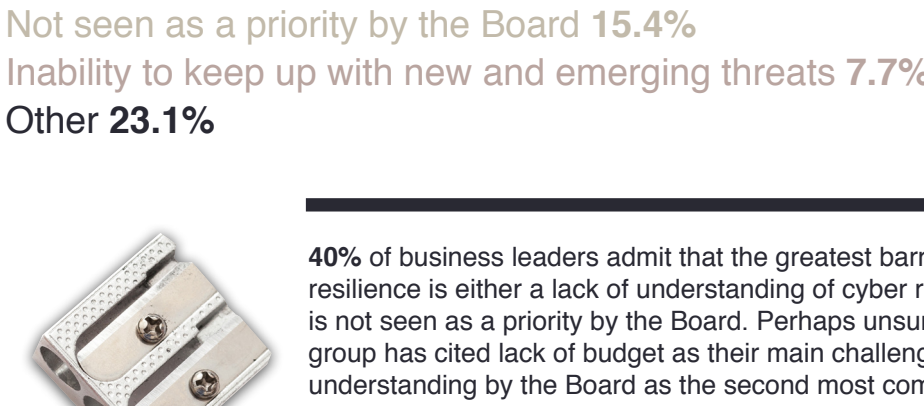
**Technical personas**  
 Yes 57.7%  
 No 38.5%  
 Don't know 3.8%

According to business leader respondents, one in four of their organisations either do not have a plan to respond in the event of a cyber incident - or they don't know if they do. This number rises worryingly to over 40% amongst technical respondents.

#### 4. What do you think the greatest barrier to building cyber resilience is for UK organisations?



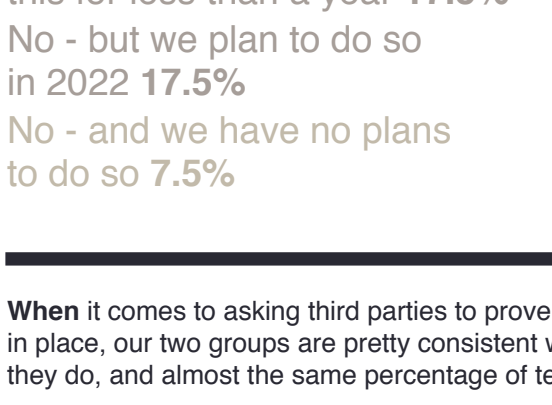
**Business personas**  
 Lack of budget 10%  
 Lack of cyber security expertise within technology teams 20%  
 Lack of understanding of cyber risk at the Board level 22.5%  
 Not seen as a priority by the Board 17.5%  
 Inability to keep up with new and emerging threats 22.5%  
 Other 7.5%



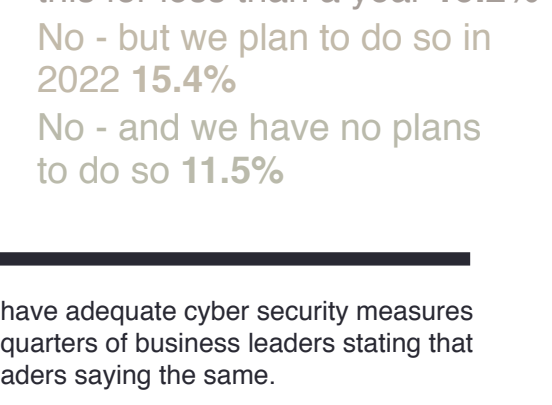
**Technical personas**  
 Lack of budget 23.1%  
 Lack of cyber security expertise within technology teams 11.5%  
 Lack of understanding of cyber risk at the Board level 19.2%  
 Not seen as a priority by the Board 15.4%  
 Inability to keep up with new and emerging threats 7.7%  
 Other 23.1%

40% of business leaders admit that the greatest barrier to building cyber resilience is either a lack of understanding of cyber risk, or the fact that it is not seen as a priority by the Board. Perhaps unsurprisingly, our technical group has cited lack of budget as their main challenge, with a lack of understanding by the Board as the second most common barrier.

#### 5. Do you currently ask third party partners and providers to prove that they have adequate cyber security controls in place?



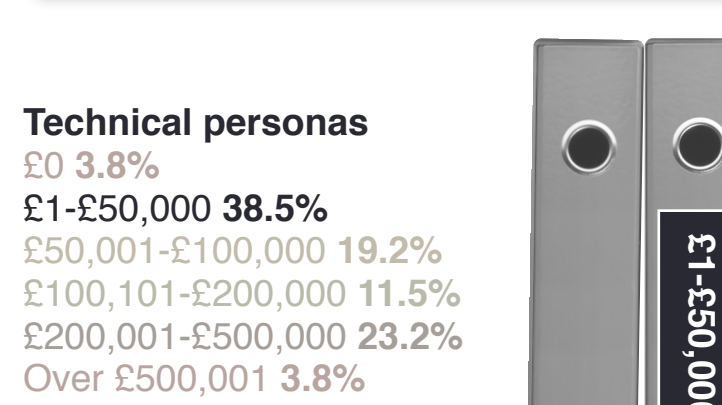
**Business personas**  
 Yes - we have been doing this for over a year 57.5%  
 Yes - we have been doing this for less than a year 17.5%  
 No - but we plan to do so in 2022 17.5%  
 No - and we have no plans to do so 7.5%



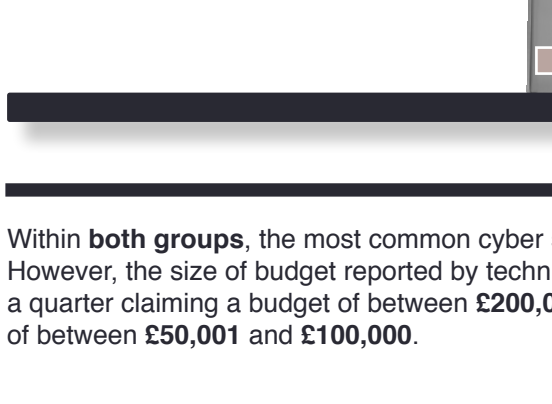
**Technical personas**  
 Yes - we have been doing this for over a year 53.9%  
 Yes - we have been doing this for less than a year 19.2%  
 No - but we plan to do so in 2022 15.4%  
 No - and we have no plans to do so 11.5%

When it comes to asking third parties to prove that they have adequate cyber security measures in place, our two groups are pretty consistent with three quarters of business leaders stating that they do, and almost the same percentage of technical leaders saying the same.

#### 6. What is your current budget for cyber security per annum?



**Business personas**  
 £0 5%  
 £1-£50,000 60%  
 £50,001-£100,000 22.5%  
 £100,101-£200,000 7.5%  
 £200,001-£500,000 5%  
 Over £500,001 0%



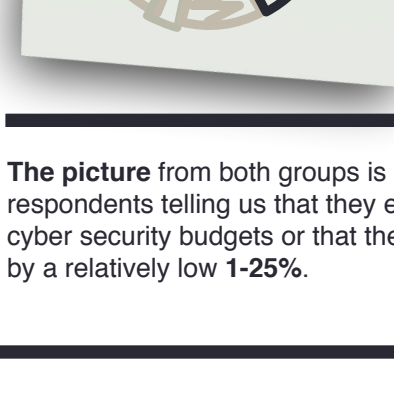
**Technical personas**  
 £0 3.8%  
 £1-£50,000 38.5%  
 £50,001-£100,000 19.2%  
 £100,101-£200,000 11.5%  
 £200,001-£500,000 23.2%  
 Over £500,001 3.8%

Within both groups, the most common cyber security budget was between £1 and £50,000. However, the size of budget reported by technical leaders was much more variable, with almost a quarter claiming a budget of between £200,001 and £500,000 and almost a fifth with a budget of between £50,001 and £100,000.

#### 7. By how much are you planning to increase your investment in cyber security in 2022?



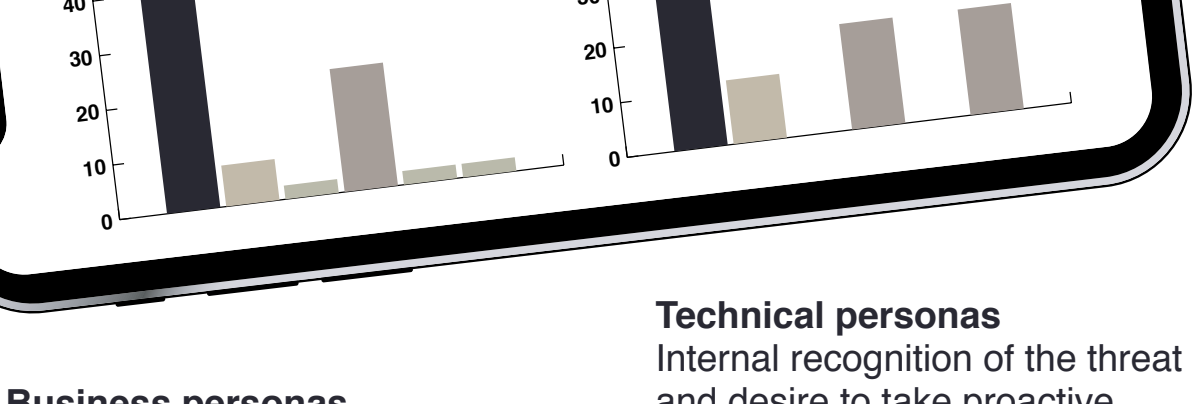
**Business personas**  
 By 1-25% 37.5%  
 By 25-50% 17.5%  
 By 50-75% 2.5%  
 By 75-100% 0%  
 We're not planning to increase it 40%  
 We're planning to decrease our investment in cyber security 2.5%



**Technical personas**  
 By 1-25% 42.4%  
 By 25-50% 11.5%  
 By 50-75% 3.8%  
 By 75-100% 11.5%  
 We're not planning to increase it 30.8%  
 We're planning to decrease our investment in cyber security 0%

The picture from both groups is relatively consistent with most respondents telling us that they either have no plans to increase cyber security budgets or that they only plan to increase them by a relatively low 1-25%.

#### 8. What will be the primary driver of your cyber security strategy in 2022?

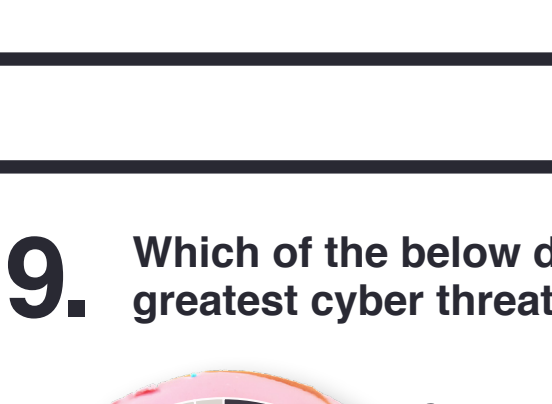


**Business personas**  
 Internal recognition of the threat and desire to take proactive action 62.5%  
 Increasing regulation concerning cyber security 7.5%  
 Requirements from our investors /shareholders 2.5%  
 Requirements from our customers /trading partners 22.5%  
 Whether or not we suffer a cyber incident/breach 2.5%  
 Other 2.5%

**Technical personas**  
 Internal recognition of the threat and desire to take proactive action 50%  
 Increasing regulation concerning cyber security 11.6%  
 Requirements from our investors /shareholders 0%  
 Requirements from our customers /trading partners 19.2%  
 Whether or not we suffer a cyber incident/breach 0%  
 Other 19.2%

Encouragingly, the majority of respondents in both groups told us that the primary driver behind their 2022 cyber security strategy will be internal recognition of the threat. In second place - also for both groups - was requirements from customers and trading partners.

#### 9. Which of the below do you think will pose the greatest cyber threat to UK businesses in 2022?



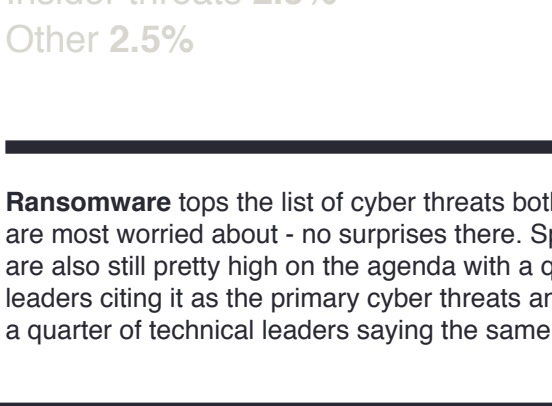
**Business personas**  
 Ransomware 37.5%  
 Other malware 12.5% (viruses, worms, Trojans, etc.)  
 Spam and phishing 25%  
 DDOS attacks 7.5%  
 Supply chain weaknesses 7.5%  
 Cloud computing weaknesses 5%  
 Insider threats 2.5%  
 Other 2.5%



**Technical personas**  
 Ransomware 46.2%  
 Other malware 3.8% (viruses, worms, Trojans, etc.)  
 Spam and phishing 23.2%  
 DDOS attacks 0%  
 Supply chain weaknesses 11.5%  
 Cloud computing weaknesses 7.7%  
 Insider threats 3.8%  
 Other 3.8%

Ransomware tops the list of cyber threats both of our groups are most worried about - no surprises there. Spam and phishing are also still pretty high on the agenda with a quarter of business leaders citing it as the primary cyber threats and just less than a quarter of technical leaders saying the same.

#### 10. Overall, do you think that UK organisations are better equipped to mitigate cyber risk now than they were 12 months ago?



**Business personas**  
 Yes 65%  
 No 10%  
 They're no better or worse equipped than they were 12 months ago 25%



**Technical personas**  
 Yes 61.6%  
 No 26.9%  
 They're no better or worse equipped than they were 12 months ago 11.5%

The good news is that for both groups almost two thirds believe that UK organisations are better equipped to mitigate cyber risk now than last year. The flipside of this is that over a third of all respondents believe that organisations are either worse equipped or haven't improved at all.

**RESULTS\***

To learn more about how to achieve complete visibility and control over your level of cyber risk, [click here](#)

**norm.**<sup>TM</sup>

\* Survey conducted in December 2021 by NormCyber Limited. Copyright © NormCyber Limited. All Rights Reserved.