National Cyber Security Centre
a part of GCHQ

The state of cyber security in the UK charity sector

CHARITY DIGITAL

Introduction

When we decided to undertake this survey with the National Cyber Security Centre – a part of GCHQ, we wanted to understand what charities thought about cyber security and how they were approaching it, particularly during the tumultuous changes brought about by COVID-19

In March 2021, when lockdown was introduced in the UK to curb the spread of COVID-19, charities had to adapt to new challenges, delivering their services to beneficiaries remotely and, significantly, moving their work from the office to home.

As you might expect, this had quite the impact on cyber security. Research from the Department for Digital Culture, Media, and Sport shows that 26% of charities suffered a cyber breach in 2020 and that, unlike in the business sector, this frequency has remained consistent in 2021.

This may not be directly linked to the pandemic, but there is reason to be cautious nonetheless. Working from home, charity workers are more likely to be using personal devices on their own networks. Without the on-hand guidance from dedicated IT teams, charities can no longer be as confident that they are not unwittingly opening vulnerabilities that cyber criminals can exploit – and that's if they had that guidance in the first place.

Charities have always been at particular risk from cyber threats because of the wealth of data they hold and the limited resources they have available to protect it. It is also not a priority for many charities – in this survey, cyber security was most often ranked third in importance for organisations, after service delivery and fundraising. Chief Executives prioritised it even less.

It seems that part of the problem is a failure to see how a cyber breach could affect those areas that charities deem more pressing. A well-reported cyber breach can undermine a charity's reputation and impact how much they are supported by fundraisers, while malware and viruses can disrupt their ability to deliver services and put beneficiaries at risk. So, it is vital that cyber security is not treated as an afterthought, but rather like an MOT. Monitoring it regularly, and making changes when you find problems, keeps the show on the road.

We know that this may seem complex and that charities differ in terms of how they approach cyber security. Our survey showed a clear disparity in the resources and techniques employed by smaller and larger charities in staying cyber secure. The larger the charity, the more likely they are to have someone dedicated to looking after it too – just a quarter of micro-charities (with an income of less than £10,000) said the same.

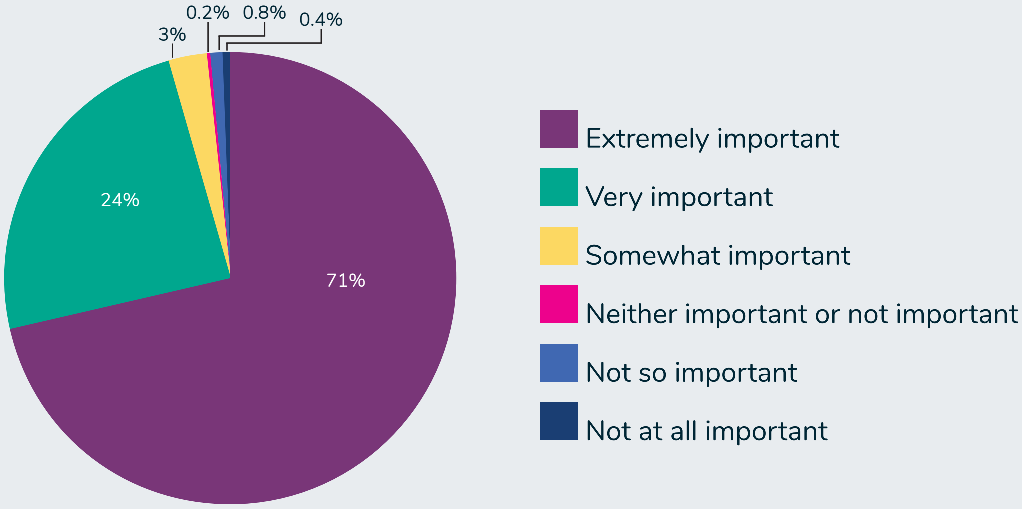
This trend is evident throughout much of the report. It shows us that, while smaller charities need to realise that cyber security does affect them, the charity sector as a whole needs to do better at standardising our cyber security approaches so that everyone – no matter what their income – is up to speed.

However, the most encouraging finding from the survey revealed how seriously charities are taking cyber security. Nearly all (98%) of charities told us that cyber security was either important or very important to them, showing that, contrary to popular belief, charities very much do care about cyber security.

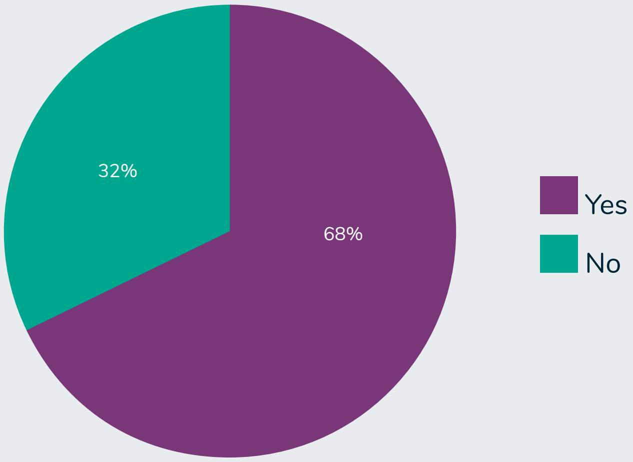
The issue is: **what next?**

The state of the sector

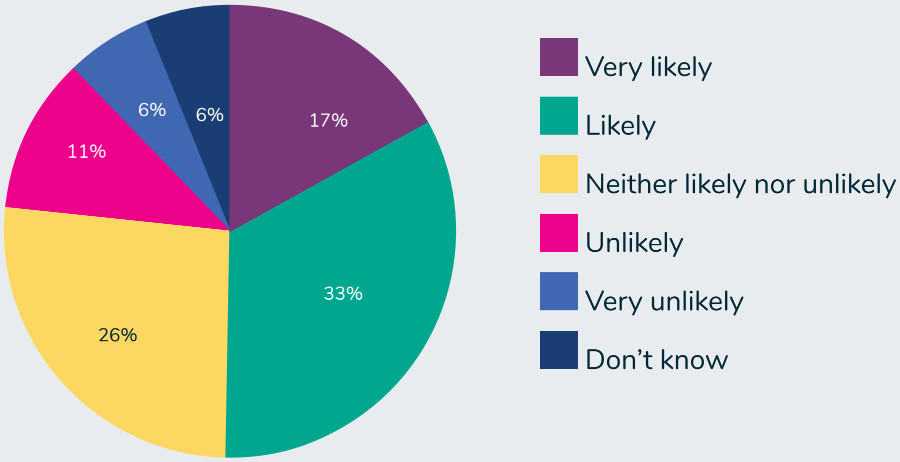
How many charities think cyber security is important



How many charities say they deal with sensitive user data



How many charities believe they are likely to suffer a cyber attack



What can you expect from the report?

In this report, we will outline five key themes from the survey and discuss what this means for the charity sector as we enter 2022.

The five themes are:

1. **We know cyber security is important – why don't we have strong approaches?**
2. **What has driven the positive shift in attitude?**
3. **Are we doing enough training?**
4. **Can leaders do more?**
5. **We're great with antivirus – what about other tech?**

By examining these themes, the report will highlight areas where the charity sector has got things right with cyber security and direct us to the key areas where we can improve. It is a timely project – with cyber attacks costing the UK economy upwards of £87 billion since 2015, making our charities safe and secure from cyber threats now is essential.

So without further ado, let's dive in, shall we?

Methodology:

This survey was conducted between July and August 2021, with 506 people from the charity sector taking part. Respondents worked in charitable organisations across a wide-range of fields – including arts and culture, community, and health – and represented a variety of roles, from volunteers to CEOs and trustees.

Charity size defined:

Micro	Small	Medium	Large	Major	Super-major
Less than £10k	£10k to £100k	£100k to £1m	£1m to £10m	£10m to £100m	More than £100m

National Cyber Security Centre
a part of GCHQ

We know cyber security is important – why don't we have strong approaches?

CHARITY DIGITAL

We know cyber security is important – why don't we have strong approaches?

Charities rate the importance of cyber security highly but do not rate their capabilities at the same level, due to uncertainty, lack of strategy, and, in smaller charities, a lack of confidence in their approach

So we know cyber security is important. Fewer than half a percent of respondents told our survey that cyber security wasn't at all important to their organisation. More than seven in ten (71%) said the exact opposite, reporting that cyber security was extremely important to them.

Yet when asked to rate how good they thought their organisation's approach to cyber security was, the average came out as six out of ten. This suggests that although the charity sector understands that cyber security matters, they remain frustrated in how they deal with it.

The contrast between how charities value cyber security and how they rate it may form a complicated picture, but the matter becomes clearer when the size of a charity is considered.

Micro organisations were less likely to say they dealt with sensitive user data and as a result, do not rank cyber security high in importance. While cyber security was ranked as the third biggest priority for charities overall (see Fig. 2), for micro charities, it was rated sixth, behind service delivery, fundraising, governance, IT, and finance.

Fig. 2 Rank these business operations in order of importance within your organisation

	1	2	3	4	5	6	7	8	9	10
Service delivery	■									
Fundraising		■								
Cyber security			■							
Governance				■						
Strategy					■					
IT						■				
Finance							■			
Culture								■		
Marketing									■	
HR										■

Fig. 3 Does your organisation have a plan in place in the event of a cyber breach?

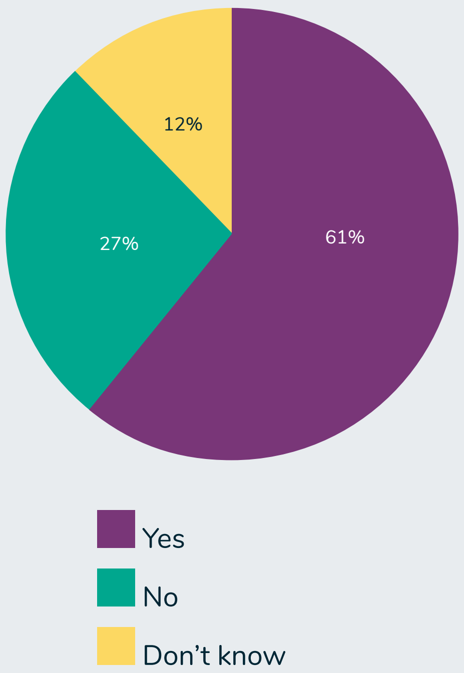
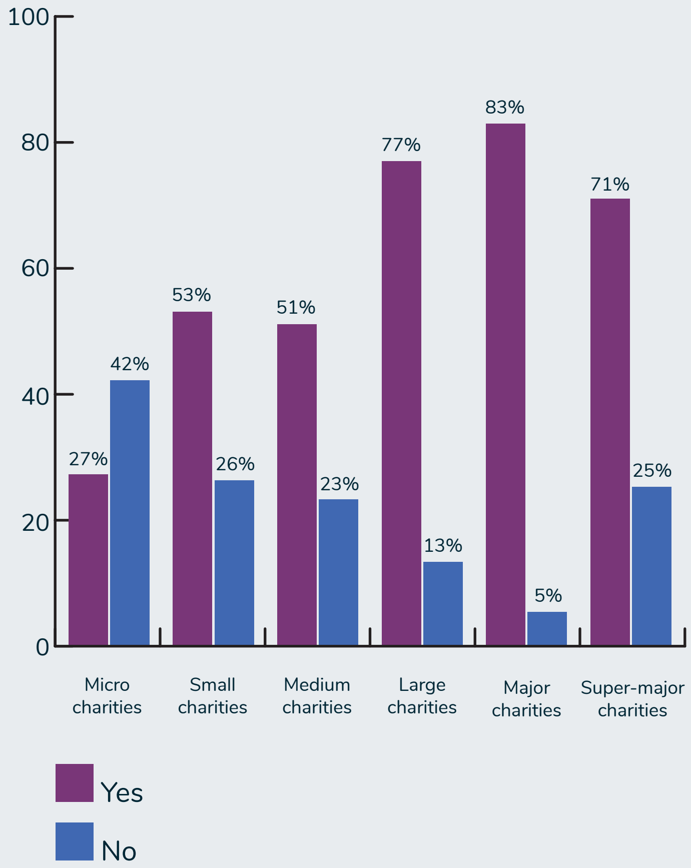


Fig. 4 Does your organisation have a plan in place in the event of a cyber breach? - by organisation size



Nearly three in ten (27%) respondents say their organisation does not have a plan in place in the event of a cyber breach. The larger the charity is, the more likely they were to say they had one. More than two in five micro charities (42%) said they didn’t have a plan in place to deal with a cyber breach (Fig. 4). Again, this is perhaps unsurprising, given that smaller charities don’t view themselves as housing sensitive user data and therefore feel less need to protect it.

This, in turn, has an impact on confidence. Overall, 83% of charities are confident in their response to a cyber breach, but as with the likelihood of having a plan in place, this confidence grows as organisation size grows. Only 72% of micro charities say they are confident, compared to 94% of major organisations.

When it came to a cyber security or cyber resilience strategy, 53% of organisations say that their organisation has a cyber security or resilience strategy. As with plans in the event of a cyber breach, the larger the organisation, the more likely they were to say that, yes, they did have a resilience strategy. Almost nine in ten major charities said they had one, in contrast with just 17% of micro charities.

The survey also revealed a lot of uncertainty around cyber security in the charity sector. The same proportion of charities (6%) say they are either very unlikely to suffer a cyber attack or don’t know. Similarly, when asked if their organisation had a plan in place in the event of a cyber breach, more than one in ten (12%) said they did not know (see Fig. 3).

Despite this mixed picture, however, most respondents did say their attitude towards cyber security had changed for the better. And of those who said it hadn’t changed, more than two thirds (68%) said it was because they already took cyber security seriously.

So, the problem is being understood for the most part – charities simply need to work on pulling together the solution.

National Cyber Security Centre
a part of GCHQ

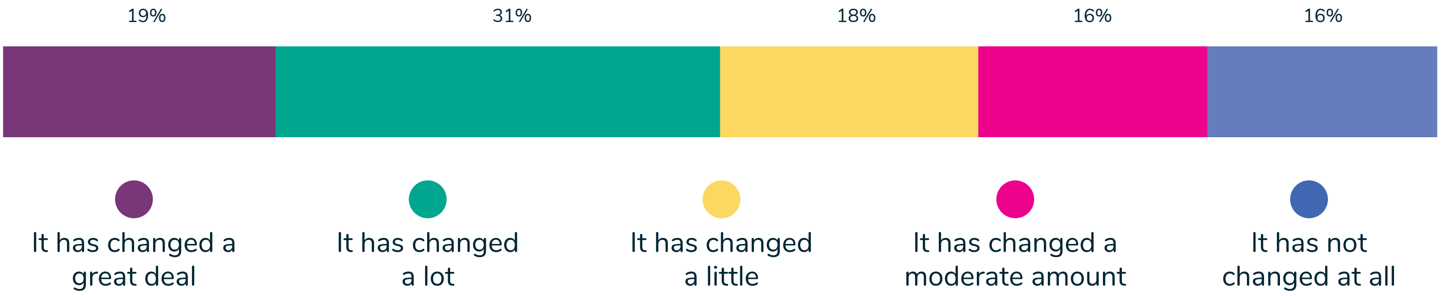
What has driven the positive shift in attitude?

CHARITY DIGITAL

What has driven the positive shift in attitude?

Our survey shows that attitudes towards cyber security have changed for the better since COVID-19, as a result of noticeable increases in cyber attacks in the sector, some of which our respondents suffered themselves

Fig. 5 Has your organisation's attitude or behaviour toward cyber security changed since the pandemic?

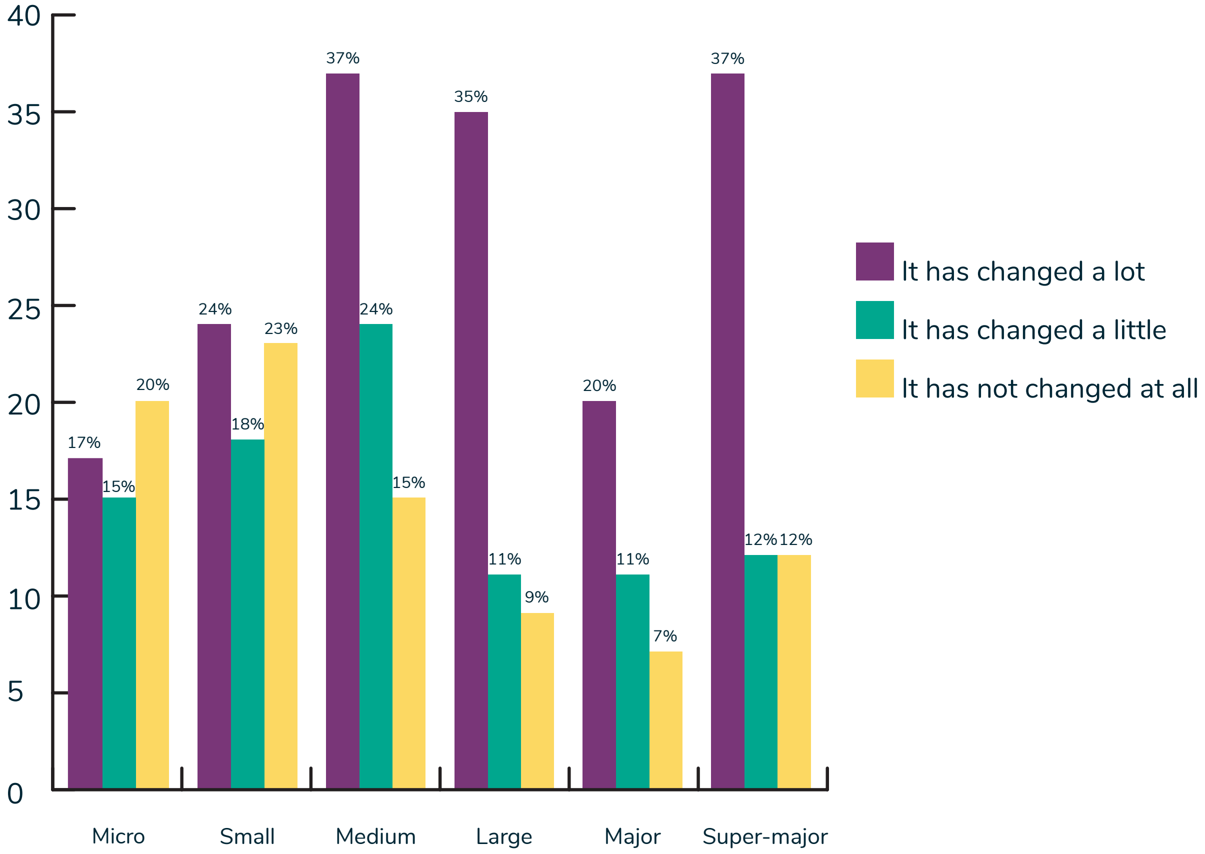


Fortunately, it is not only the amount of cyber threats that increased during the pandemic – our attitudes towards cyber security changed too.

Once again, charity size had an impact on how much change was experienced within organisations in terms of cyber security. More than a quarter of micro organisations (27%) said their attitude had changed a moderate amount (11 percentage points more than the sector overall), while one in five said it had not changed at all.

Compare this to medium and large charities – more than a third of medium and large charities said their attitudes towards cyber security had changed a lot (37% and 35% respectively), while just 15% of medium charities said it had not changed at all. This percentage lowered to 9% for their larger counterparts, and continued to lower for major and super-major organisations (see Fig. 6).

Fig. 6 Has your organisation's attitude or behaviour toward cyber security changed since the pandemic? - by organisation size



Job role also had an impact on how our respondents perceived change towards cyber security. The most people who said that attitudes or behaviours had changed a lot were in managerial positions. Trustees, on the other hand, were much more likely to say that attitudes and behaviours had not changed at all, with 43% choosing that option. Yet only 16% of respondents said this when considered as a whole, suggesting a disconnect between trustees and the cyber security approaches of their organisations.

But, regardless of what level of change people have experienced, what has driven it in the first place? The pandemic is not a factor alone in itself, though it did provide organisations with an opportunity to re-evaluate how they operate and give them new challenges to address, like how to protect themselves as they began to work predominantly in the Cloud.

There were many reasons for this post-pandemic attitude change highlighted in our survey, including an increase in training and heightened awareness of cyber breaches occurring in the sector (see Fig. 7). Of the organisations that changed their attitudes towards cyber security, two in five said it was due to the noticeable increase in cyber breaches in the sector, while 44% said it was due to more awareness from their peers. Soberingly, more than a quarter (26%) said it was because they suffered a cyber breach themselves.

The overwhelming majority of those who said their attitude towards cyber security hadn't changed since COVID-19 cited already taking cyber security seriously as the reason.

Fortunately, the report also found that cost no longer appears to be a prevalent barrier to cyber security in the charity sector. Of the organisations who hadn't changed their attitudes towards cyber security after the pandemic, the cost of implementing cyber security policies and procedures was only cited by 1% of respondents (see Fig. 8).

More than one in ten said it was because they had more important areas of focus, while 7% said they lacked the required training and skills needed.

As before, though charities say cyber security is important to them, this demonstrates that they are failing to understand that a cyber breach can affect every aspect of their operations, including those areas they prioritise more highly than cyber security – notably fundraising and service delivery.

Fig. 7 What, if anything, has caused the positive change in attitude or behaviour towards cyber security?

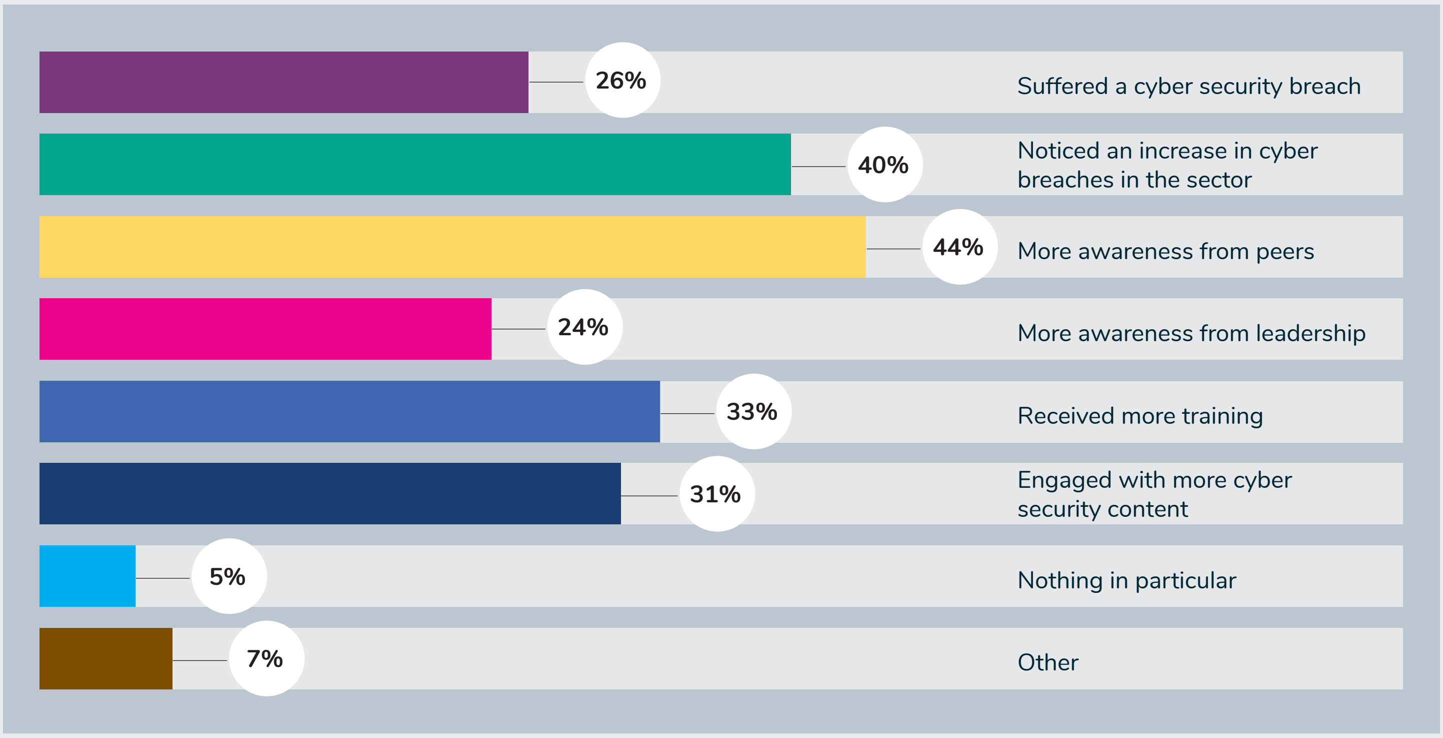
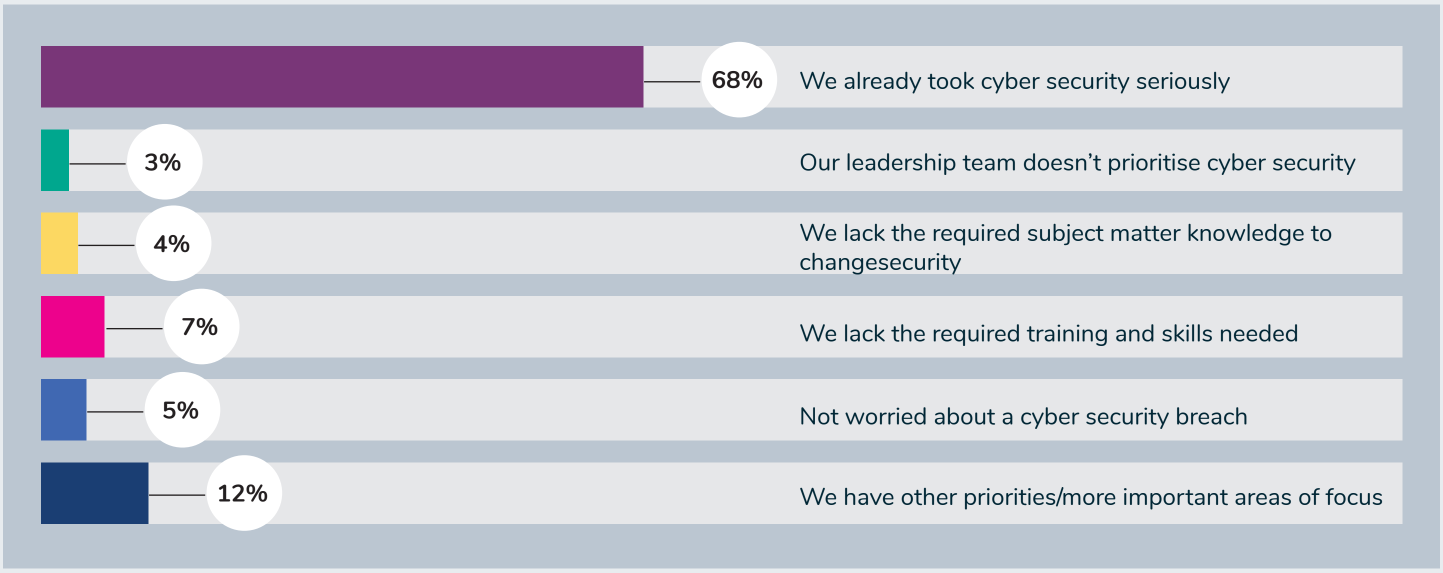


Fig. 8 Why hasn't your attitude towards cyber security changed since the pandemic?



Are we doing enough training?

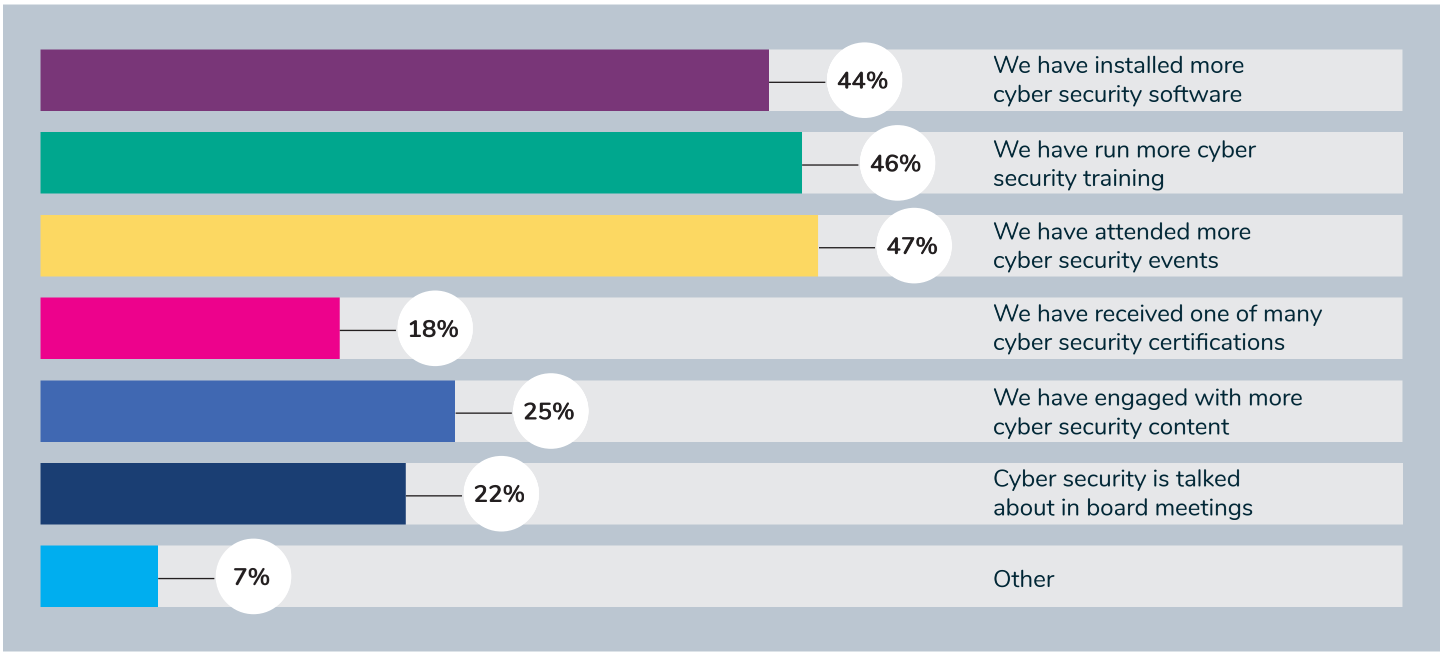
Are we doing enough training?

In the previous section, we learnt that 7% of charities felt they lacked the skills and training to positively change their attitudes towards cyber security. What training do charities currently have and how confident do they feel in their qualifications?

For the charities whose attitudes had changed towards cyber security since the pandemic, their behaviours changed too, and in many different ways (see Fig. 9).

Nearly half (46%) say they have run more cyber security training since the pandemic, with similar proportions saying they had attended more cyber security events (47%) and installed more software (44%).

Fig. 9 How has your organisation's attitude or behaviour changed?



When it comes to training in particular, more than three in five respondents (62%) said they had received at least some training or qualifications in cyber security, including 100% of those from super-major organisations.

Once again, the situation differed for small and micro charities, and the larger the organisation, the more likely they were to have received training. For example, 65% of micro charities said they hadn't received training, compared to just 8% of major organisations.

Micro charities also had the largest proportion of respondents saying they didn't know if they had received cyber security training or not – surely suggesting not or, at the very least, that it did not make a lasting impression.

Fig. 10 Have you undertaken any cyber security training or qualifications to improve your skills?

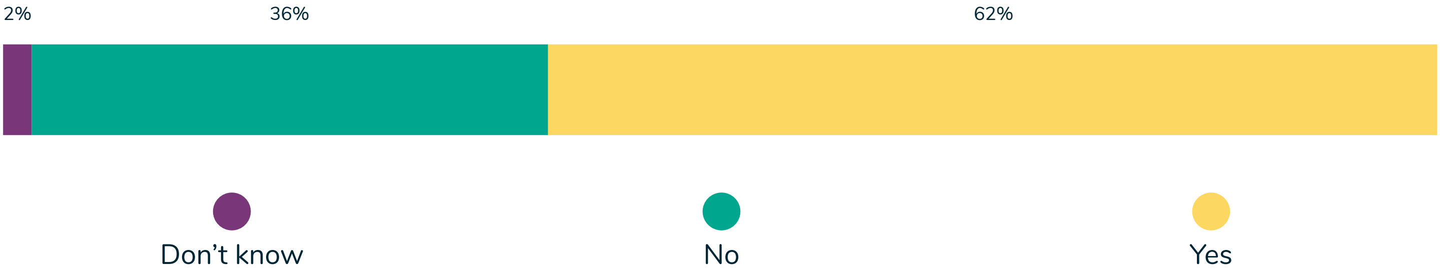
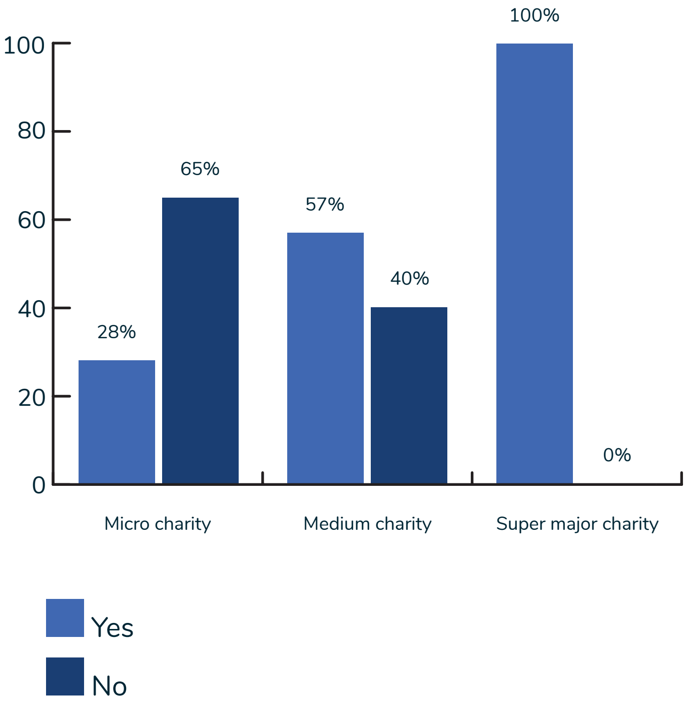


Fig. 11 Have you undertaken any cyber security training or qualifications to improve your skills? - by organisation size

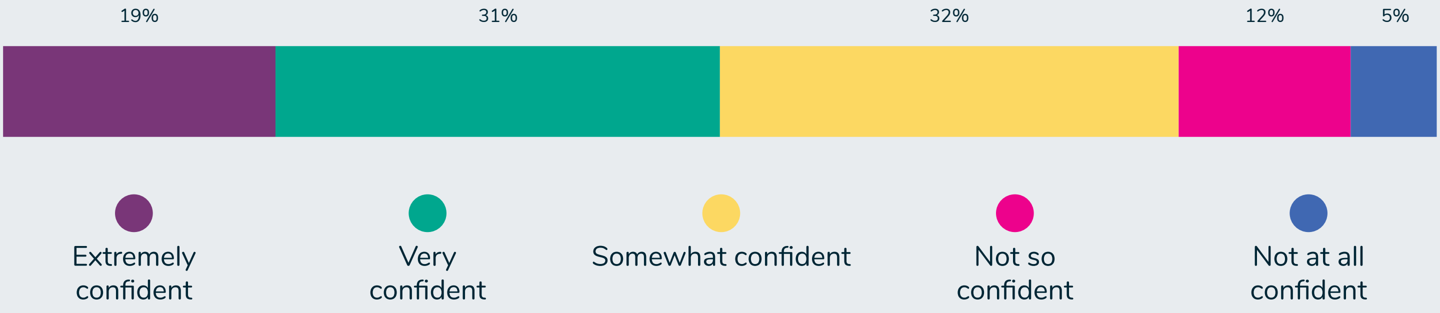


Volunteers were also less likely to say they had received any cyber security training, implying that they have been overlooked by organisations when considering their cyber protection. Two thirds (66%) of volunteers said they hadn't received training, compared to just one in five (22%) who said they had and 12% who didn't know either way.

It is critical that everyone who works at an organisation in any capacity is aware of the risks of cyber threats. It only takes one phishing email to get through the net to cause a breach and charities must recognise that volunteers are working on their networks too.

Despite the differences in cyber security training within the sector, fortunately, the majority of respondents to the survey (82%) were at least somewhat confident in their cyber security knowledge and practical expertise (see Fig. 12). Understandably, those in managerial roles were more likely to be confident than volunteers – 96% of assistant managers said so, as opposed to 66% of volunteers.

Fig. 12 How confident are you in your knowledge and practical expertise of basic cyber security?

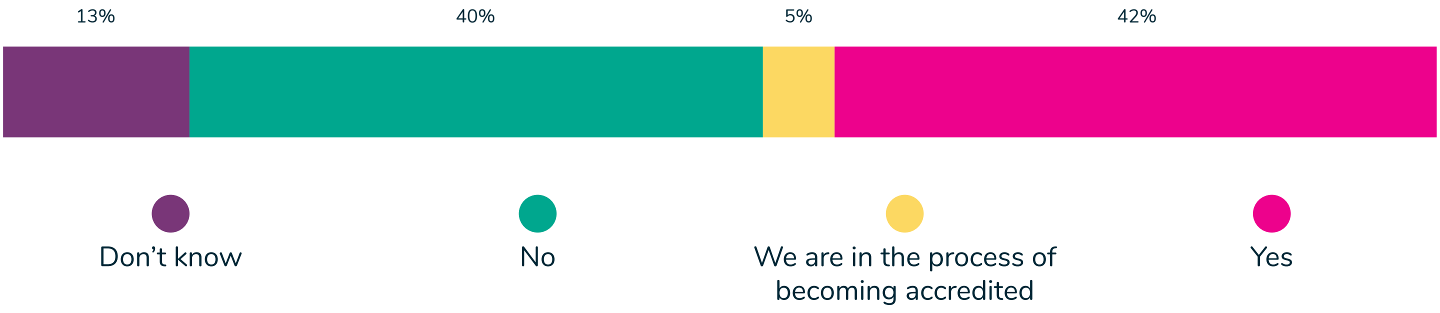


What is interesting here, however, is the gap between confidence in knowledge and how much training has been received, particularly in leadership teams. As evidenced by the previous section, a third (33%) of those whose attitudes towards cyber security had changed said this happened because they had more training – so we can see that training is having an impact on our behaviours.

However, four in five members of the C-Suite said they felt confident in their knowledge, despite 60% saying they hadn't received any training in cyber security at all. Similarly, three quarters of trustees said they felt confident, yet only 36% had taken any training. This begs the question, are charity leaders truly on top of their cyber security or is their confidence misplaced?

When it comes to holding cyber security certifications or accreditations, like Cyber Essentials, most respondents (47%) said they held one or were in the process of becoming accredited. This was, again, truer for larger organisations. Almost nine in ten super-major charities (86%) had an accreditation, compared to just 3% of micro organisations.

Fig. 13 Does your charity have any cyber security certifications or accreditations?

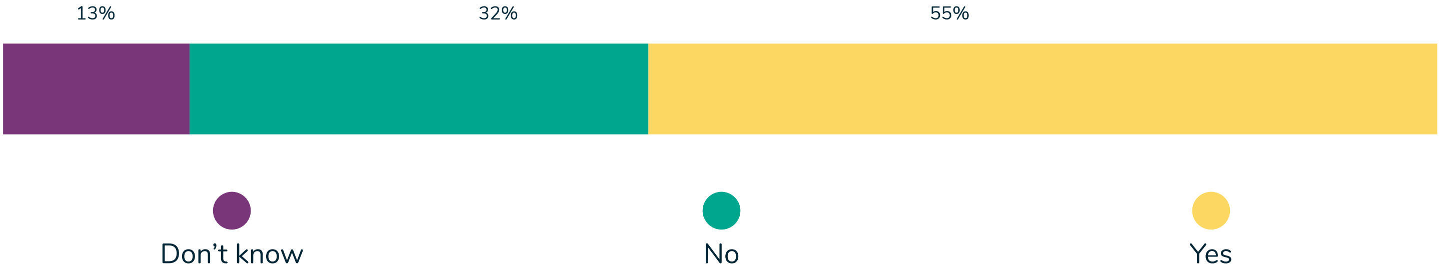


There was also some uncertainty regarding the qualifications and credentials of those who were considered responsible for cyber security in their organisation (See Fig. 14). More than half of respondents (55%) said the person in their organisation had official qualifications and accreditations, but 32% said no and 13% did not know either way.

Once again, the survey also found a disparity between the qualifications and credentials of those working in larger charities and those working in smaller organisations. Nearly two thirds (65%) of larger organisations (with an income of more than £1 million) said the person in charge of their cyber security had cyber security qualifications, compared to 15% of smaller charities.

Every respondent from a super-major charity said the person responsible for cyber security in their organisation had a qualification – this number decreased significantly alongside organisation size.

Fig. 14 Does the person responsible for cyber security in your organisation have any official qualifications or credentials?



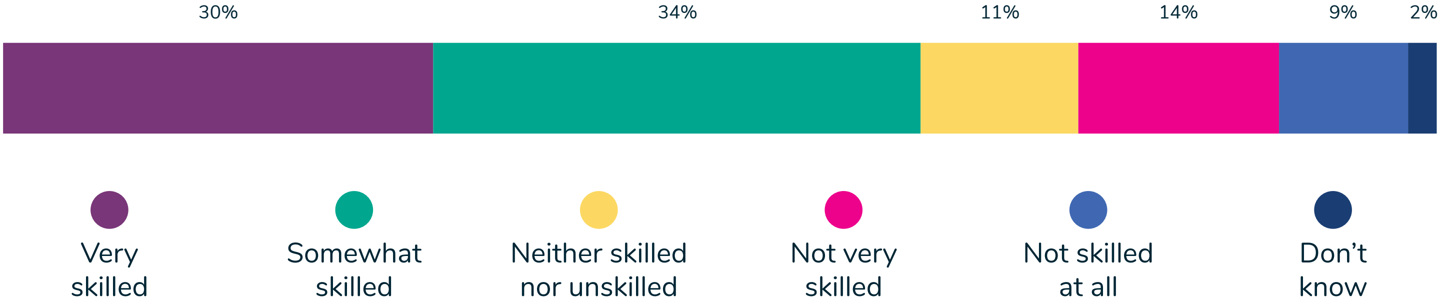
Moreover, this question produced more unease over charity leadership's knowledge of cyber security in their organisation. More than three in five (63%) trustees said the person responsible for their cyber security did not hold any qualifications or accreditations, with a similar proportion of directors and senior executives saying the same (64%). Yet, across all job roles, the percentage of people saying this was only 32%.

This could suggest that leadership has little faith in their cyber security people, or that they are out-of-touch with them. Either way, the high percentage of negative responses to this question from leadership should cause disquiet.

Indeed, the outlook was more worrisome on the whole for charity leaders. While three in five (60%) of those in C-Suite positions said that they have not received training or qualifications in cyber security, this was true, too, of more than half (54%) of those in director or senior executive roles.

Yet, as we'll see in the next section, organisations look to their leadership for guidance on their cyber security. Overall, nearly two thirds (64%) of organisations believed their leadership team to be skilled in such matters (See Fig. 15).

Fig. 15 Would you consider your organisation's leadership team to be skilled or proficient when it comes to matters of cyber security?



National Cyber Security Centre
a part of GCHQ

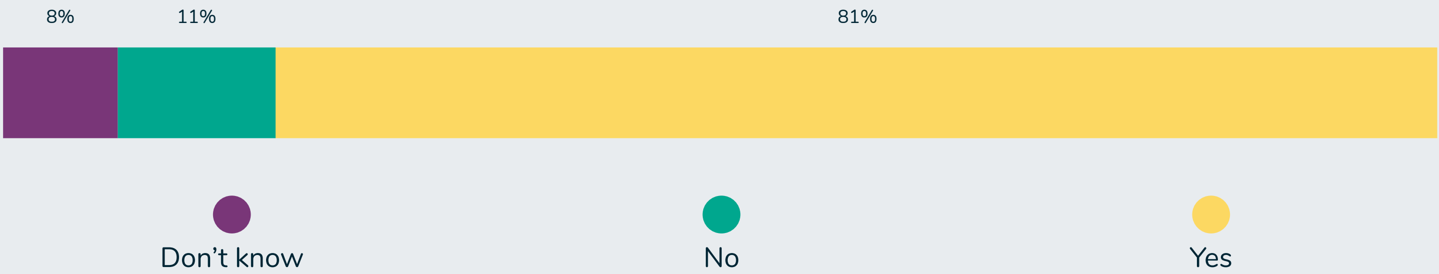
Can leaders do more?

CHARITY DIGITAL

Can leaders do more?

Our survey shows that there is a clear role for leadership to play when it comes embedding cyber security throughout an organisation. But currently our leaders are not doing enough and there appears to be a disconnect between their knowledge and that of the managers they support

Fig. 16 Do you feel your leadership team values cyber security?



Four in five respondents (81%) told the survey that they thought their leadership valued cyber security. Of those charities who said their attitudes towards cyber security had changed, 24% reported it was because there was more awareness from their leadership.

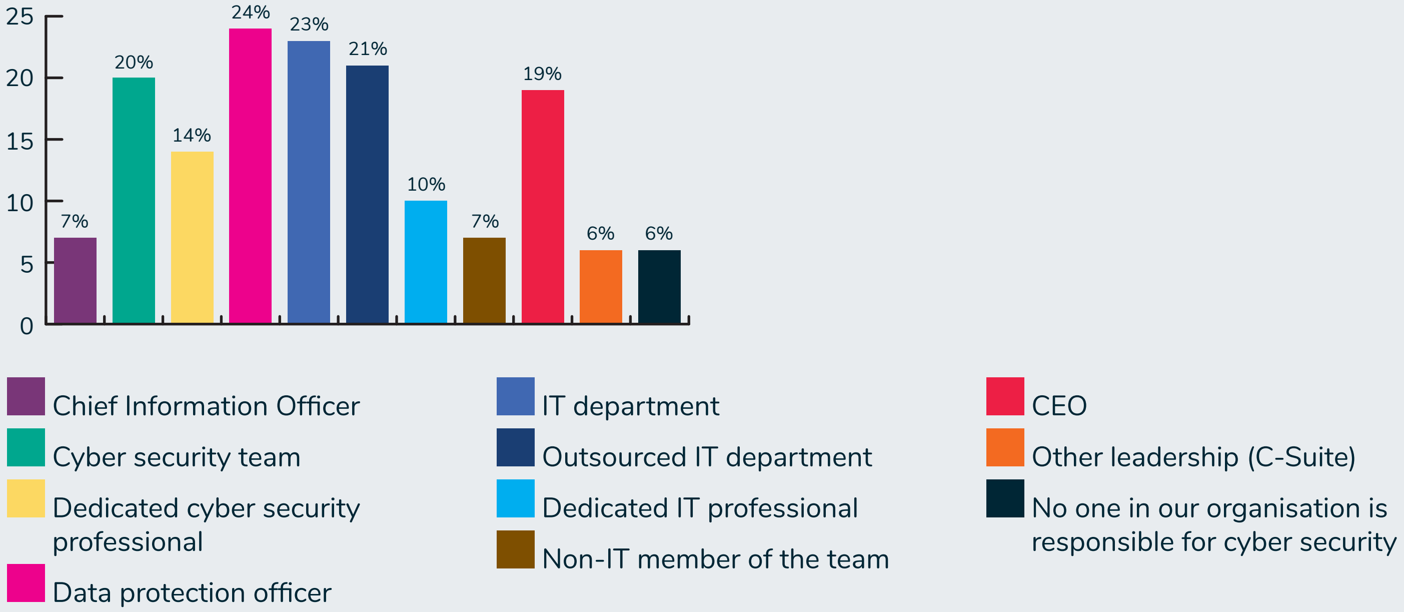
However, the survey also revealed that leadership is not as clued into their organisation’s cyber security as one might expect. Only 54% of CEOs said that their organisation deals with sensitive user data, compared to 95% of cyber security professionals.

CEOs also placed more importance on service delivery, governance, fundraising, finance, and strategy than cyber security. To recall what we revealed in the first part of this survey, cyber security was cited as the third biggest priority for charities overall.

Fig. 17 Rank these business operations in order of importance within your organisation – CEOs only

	1	2	3	4	5	6	7	8	9	10
Service delivery	■									
Fundraising			■							
Cyber security							■			
Governance		■								
Strategy					■					
IT						■				
Finance				■						
Culture								■		
Marketing									■	
HR										■

Fig. 18 Who is responsible for cyber security in your organisation?



Another worrying finding arose when we asked charities who was responsible for cyber security in their organisation. Though CEOs are clearly not prioritising cyber security, a considerable number of respondents think they are responsible for it (19%). This was only slightly less than the number of respondents who said the IT department held responsibility for their cyber security (23%).

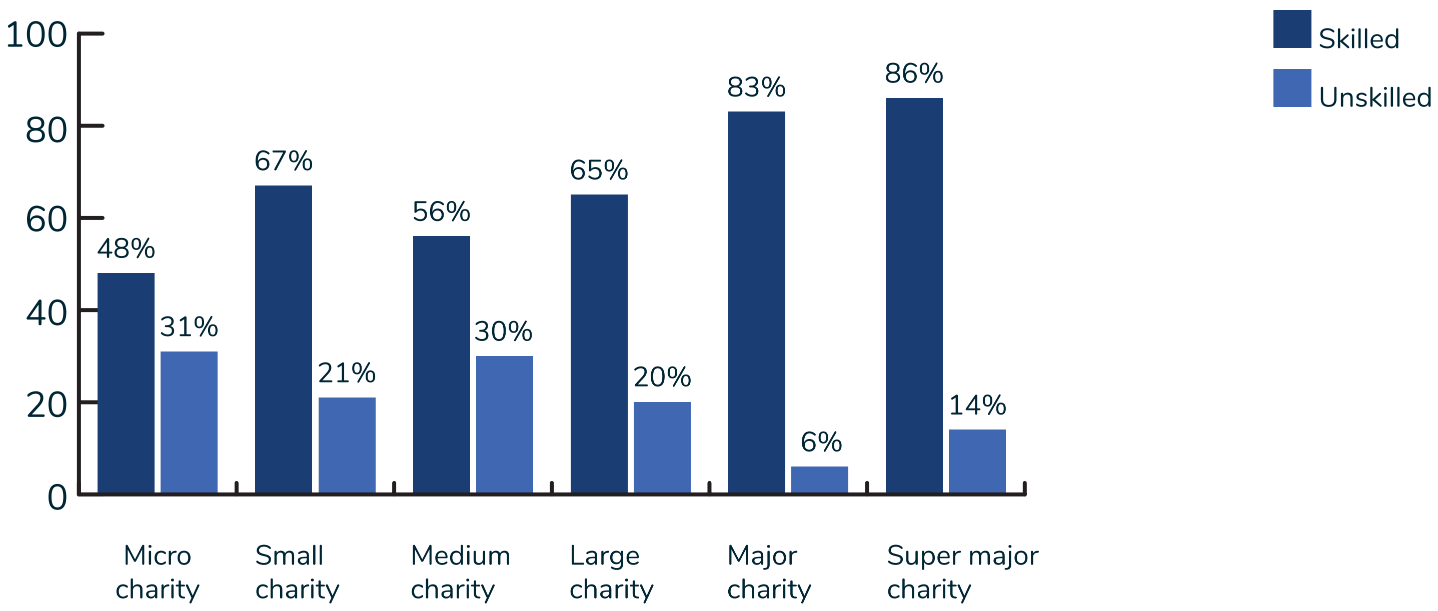
Yet, despite this belief, nearly half (44%) of respondents from the C-Suite said they were not aware that their organisation had a cyber security resilience strategy at all. More than three quarters of trustees (78%) reported the same, despite 58% of managers saying they did have one.

In fact, directors and trustees were more likely to say their charity didn't have a cyber resilience strategy than any other job role, except volunteers. This suggests that leadership teams are perhaps ignorant of the cyber resilience strategy in their organisation or that they have yet to implement one. Leaders need to recognise that they have a role to play in this and that their organisations are looking to them for such guidance.

Broadly, organisations of all sizes thought their leaders were skilled (64%), but there were still areas of concern (see Fig. 19). Almost a third of both medium-sized and micro charities did not think their leadership team was skilled, while smaller organisations were also more likely to give an indifferent answer ('neither skilled or unskilled'), suggesting that they are unsure about the skill level of the leaders. Skill perception also rose with charity size – fewer than half of micro organisations (48%) thought their leaders were skilled, compared to 86% of super-majors.

From this, we can see that leaders in smaller charities have a bigger role to play when it comes to promoting good cyber security and engendering confidence in their employees. But they also need to work on engendering confidence in trustees, too. Two in five trustees said the leadership were not skilled when it came to cyber security – more than any other position in the charity sector.

Fig. 19 Do you consider your organisation's leadership team to be skilled? - by organisation size



Lack of leadership was also cited as a reason for respondents lacking confidence in their knowledge and practical expertise of basic cyber security. Nearly a fifth of respondents (17%) who said they did not feel confident in their knowledge said that they lacked encouragement to expand their knowledge from leadership.

Similarly, more than one in ten (12%) said they had been given a lack of training options by their leadership, while 43% said they did not know where to find more information on cyber security (spoiler alert: our conclusion has plenty). It is not leadership's sole responsibility to point their teams to cyber security resources but making them readily available will certainly help in demonstrating that cyber security is on your organisation's radar.

On the whole, in terms of leadership, our survey shows continually that confidence is high for leaders and that organisations have faith in their influence on matters of cyber security. However, it is evident that skill levels need to catch up with that faith, else leadership risks taking their cyber security for granted.

It is crucial that they have knowledge of their cyber security strategy and take control of promoting its importance throughout their organisation. Currently, the lack of clarity on who is responsible for cyber security, and who should be prioritising it, is holding charities back from addressing the problem head on.

National Cyber Security Centre
a part of GCHQ

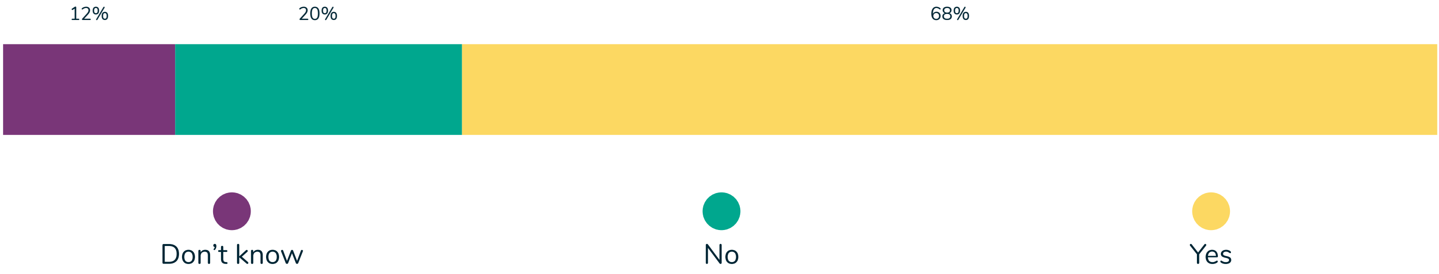
We’re great with Antivirus – but what about other tech?

CHARITY DIGITAL

We're great with Antivirus – but what about other tech?

What does good cyber security actually look like? Our survey found that charities are familiar with antivirus software – but is that enough to protect against the cyber threats the sector faces?

Fig. 20 Has your organisation implemented any cyber security software in the last 18 months?



So far, we have established that cyber security is important, that charity leaders could take a stronger role in cyber security, and that our perception of confidence in cyber security outweighs our skills. At worst, the latter is remarkable hubris, but more likely, given how highly the sector views cyber security, its lack of skills is a result of not knowing what good cyber security actually looks like.

Our survey revealed that, once again, the picture across the sector varies. More than two thirds of organisations told us they had implemented cyber security software in the last 18 months (see Fig. 20) but, as has been the trend throughout this report, smaller organisations were more likely to say that they had not.

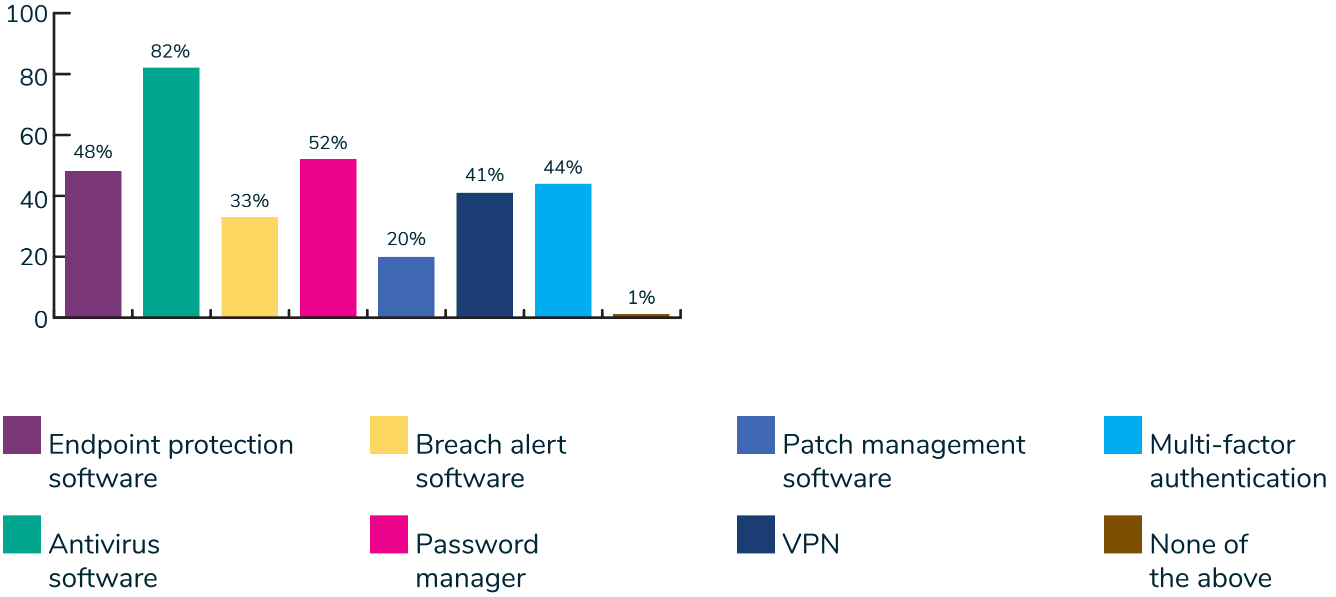
Almost half of micro charities (46%) said they had not implemented software in the last 18 months, alongside 33% of small organisations. Seven in ten (71%) of super-major organisations reported the opposite, with more than four in five major and large charities (83% and 85% respectively) also saying they had implemented cyber software.

But there was also, again, uncertainty over whether organisations had implemented new cyber security software. Volunteers and interns were the most likely to say they hadn't or that they did not know – suggesting once more that charities need to improve how they bring everyone involved in their charity along with cyber security, regardless of role and seniority.

Trustees, too, seemed unclear as to what cyber security had been implemented, with 18% saying they did not know. Likewise, a quarter of those who said they did not know what cyber security software was being used were directors. This seems like an oversight and, again, highlights the importance of embedding cyber security throughout an organisation, from the very top to the bottom.

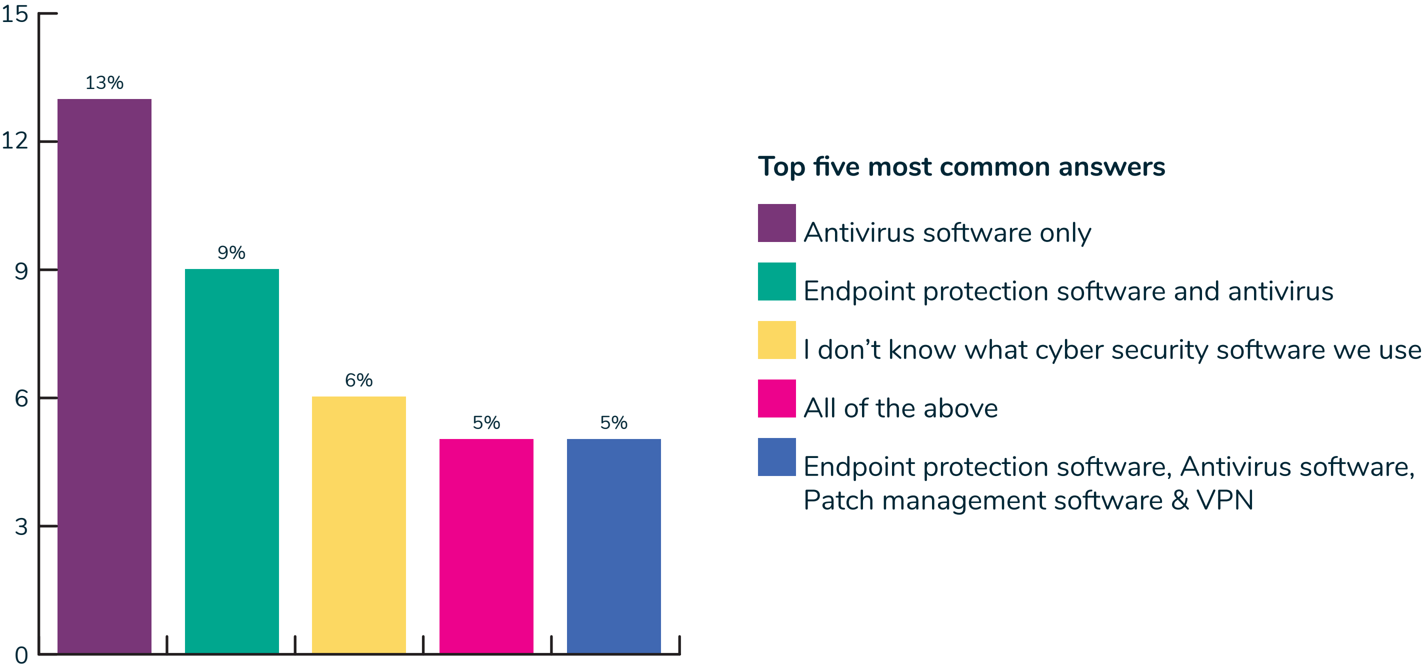
When it comes to what software charities have in place, antivirus was by far the cyber security tech charities were most familiar with. Four in five respondents (82%) said they were familiar with it, compared to just 20% who said the same about patch management. In fact, password managers were second in familiarity, with half saying they were familiar with it – a full 30 percentage points less than those who talked about antivirus (see Fig. 21).

Fig. 21 Which of the following cyber security software are you familiar with?



But in terms of what cyber security software charities actually use, only 5% said they were using what we at Charity Digital would describe as 'the works' (see Fig. 22). In fact, more people said they did not know what cyber security software they used than said they used 'All of the above' described in Fig. 21.

Fig. 22 Which of the following cyber security software does your charity use?



The most shocking statistic here is that 13% of charities are using antivirus software only. Our level of connectivity across multiple devices means that we have increased vulnerabilities that cyber criminals can exploit if our devices and networks are improperly protected. Viruses and malware are more advanced and don't only infect one computer – they can infect all of our devices connected to it too.

Using password managers (to decrease the risk of forgetting unique passwords for your accounts), VPN, patch management, and endpoint protection software – or, indeed, 'the works' – charities can ensure that they are as protected as possible from cyber threats, wherever they come from.

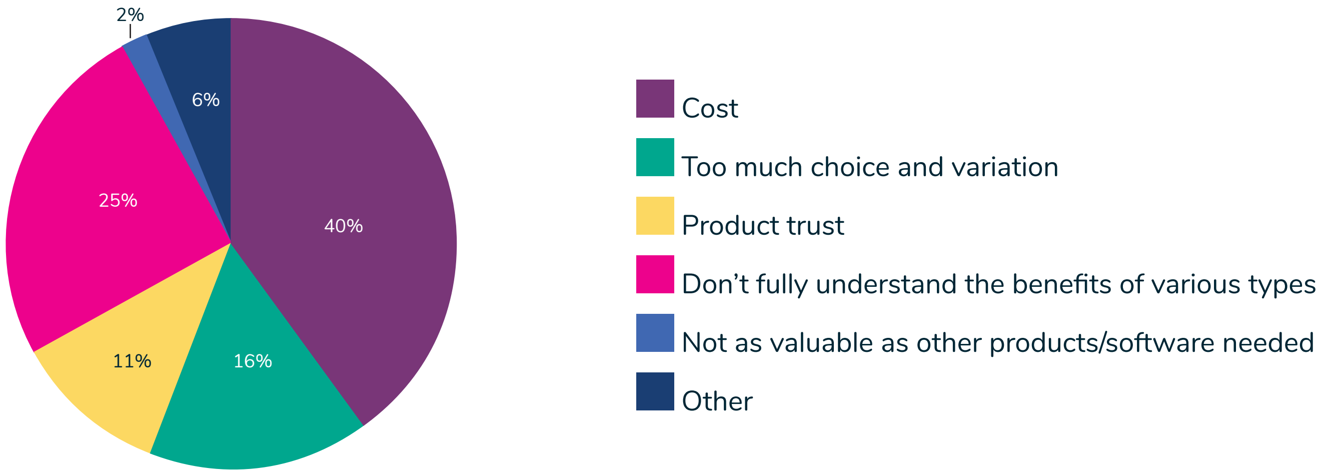
*This question received multiple answer combinations with respondents ticking all boxes that applied

While we noted earlier that those organisations who hadn't changed their attitudes towards cyber security did not put this down to cost, the majority of respondents said that cost was a barrier towards equipping their charity with the complete cyber security package (see Fig. 23).

However, the combined number of respondents who cited too much choice and variation, trust in products, and not fully understanding the benefits of different software as a barrier outweighed the number who chose cost. More than half (52%) of charities said, in some form or another, that they lacked clarity on what good cyber security looked like and what products they actually needed.

This implies the need for cyber security companies to be clearer in what they are prescribing, but also demonstrates that charities are ready to take the steps required to become cyber secure – they simply remain unsure of what those next steps are.

Fig. 23 What do you see as the barriers to equipping your organisation with all the cyber security software mentioned previously?



Conclusion

The disparity between the cyber security capabilities and actions of small and large charities stood out throughout the survey, as did the lack of clear leadership from the C-Suite. What does this mean for charities moving forwards?

As we said at the start of this survey, we wanted to understand where the UK charity sector stood overall when it came to cyber security.

Our subsequent findings make for interesting, if often uneasy reading. That we rate our efforts at six out of ten is a concern, as is the fact that, on almost all counts, small and micro organisations are at a disadvantage when it comes to cyber security.

But what remains most troubling is that charities fail to see how a lack of cyber security can affect their operations (See Fig. 24). Only two thirds of charities thought it was likely or very likely that a cyber attack would prevent them from continuing operations, with organisation size once again proving contentious here. One third of micro organisations believed their organisation would be unaffected in the event of a cyber breach.

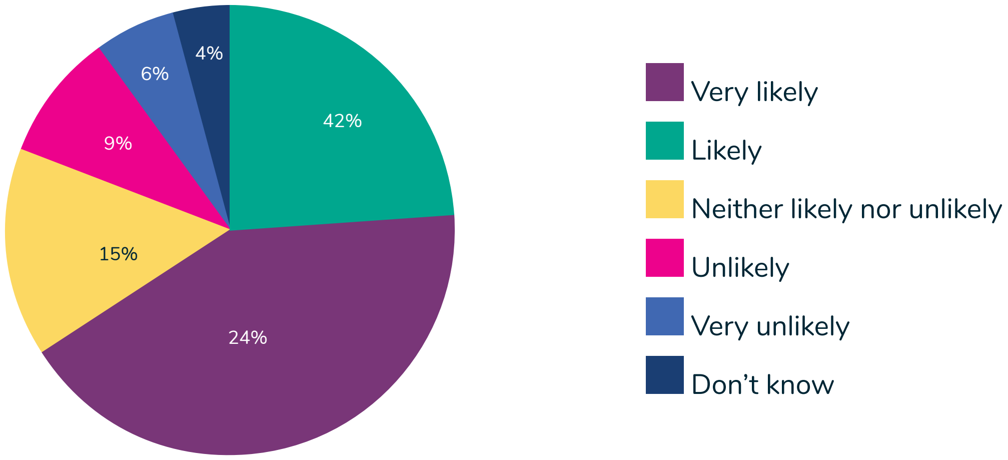
This compartmentalisation of cyber security is reflected, too, in the sector's priorities. Service delivery is an admirable priority and a rightful one – charities exist to serve their beneficiaries. However, service delivery can be easily compromised if our networks and technology are rendered unusable by viruses and malware, if our data is held to ransom, or our funds lost – all of which are consequences of incomplete cyber security.

With the increasing sophistication of cyber attacks, and with charities posing a particularly tantalising target for cyber criminals, charities need to act now to improve their security online and on their devices.

The need to be cyber secure will not become less urgent as time goes on – in fact, quite the opposite. The shift to hybrid working – and the Bring Your Own Device policies that have come with it – means that endpoint protection needs to be ensured to protect against infiltration by cyber criminals on our networks. Charity employees and volunteers need to ensure that they update their apps and software regularly to patch any vulnerabilities, and to keep up to date with what a phishing email looks like.

Charities also need to be honest with each other. Sharing knowledge and experience of cyber breaches can help protect against the next one, as we become more attune to the methods of cyber criminals. Admitting to a cyber breach remains taboo for most organisations in the charity sector, but we can only keep learning.

Fig. 24 How likely would a cyber attack affect your organisation's ability to continue operations?



This requires leadership, both within and without our charities. Sharing our cyber security lessons is the next step to standardising our efforts across the entire sector, ensuring the smallest micro charity is as cyber secure as the largest super-major. Everyone can be a target for cyber criminals and no one is immune.

There are plenty of free resources available to charities looking to improve their cyber security. The National Cyber Security Centre has guidance for small charities that can also be of use for some larger non-profits. Micro charities, especially, can also benefit from the NCSC's CyberAware Action Plans, where answering just a few questions about your organisation will get you access to a free personalised list of actions to help improve your cyber security.

Charities looking for a place to begin can find many useful tools on the NCSC website, including Web Check, which helps organisations identify and fix common security issues in your website, and Mail Check, which does the same for emails. There's also Exercise in a Box, where organisations can test their resilience against a cyber attack and practice their response in a safe environment.

For charity leadership and board members – who, we've identified, have a clear role to play in improving their cyber security – they can find guidance from the NCSC's Board Toolkit, which lays out recommendations for individual board members on cyber security but also points out the questions that they should ask about the whole organisation.

The IASME Consortium, the certification body that works with the NCSC to deliver the Cyber Essentials accreditation, also provides a batch of articles on the five core controls that charities need to protect against a cyber breach. Charities can also find its readiness tool on its website and use it to gauge where they are on their cyber security journey.

The Charity Digital website is also home to articles, podcasts, webinars, and much more, on the topic of cyber security, and offers guidance to charities no matter what their technical capabilities, size, or income. Charities looking to improve their cyber security protection software can also look on the Charity Digital Exchange for discounted options – don't just leave it to the anti-virus anymore!

In the introduction to this survey, we described looking after our cyber security as an MOT for your organisation. We're not wrong. But it is not just the checks that are comparable – it's the regularity, keeping an eye out for what might go wrong between checks, and fixing anything that needs attention.

This survey shows the picture for charities in 2021. The outlook may be vastly different in 2022 – hopefully that six out of ten rating will be a thing of the past. The first action we can take is to start.

Resources

The National Cyber Security Centre:
www.ncsc.gov.uk/collection/charity/

Exercise in a Box:
www.ncsc.gov.uk/information/exercise-in-a-box

Web check:
www.ncsc.gov.uk/information/web-check

Mail check:
www.ncsc.gov.uk/information/mailcheck

Board toolkit:
www.ncsc.gov.uk/collection/board-toolkit

Charity Digital Cyber Security hub:
www.charitydigital.org.uk/cyber-security

About us

CHARITY
DIGITAL

Charity Digital

Charity Digital partners with leading technology providers to deliver the UK's only software donation platform, Charity Digital Exchange. The charity aims to improve digital awareness and access, connect charities to the digital expertise and talent they need, and raise the bar for digital skills and understanding for non-profit organisations of all kinds.

Since 2001, Charity Digital has helped more than 400,000 charity professionals learn about digital transformation through our media platform and enabled more than 68,000 to save in excess of £260 million on technology investments.

National Cyber
Security Centre
a part of GCHQ

The National Cyber Security Centre

The National Cyber Security Centre (NCSC) – a part of GCHQ – is the UK's lead technical authority on cyber security. Launched in October 2016, the NCSC is committed to making the UK the safest place to live and work online.

It offers unrivalled real-time threat analysis, defence against national cyber attacks, and tailored advice and guidance for the public sector, critical UK infrastructure, organisations of all sizes, and citizens.

National Cyber Security Centre
a part of GCHQ

To find out more about cyber security in the charity sector, visit the NCSC website (www.ncsc.gov.uk) or check out helpful tips and guides on how to stay secure online, and much more, from Charity Digital (www.charitydigital.org.uk).

CHARITY DIGITAL