QMS INTERNATIONAL

CYBER SECURITY SURVEY REPORT

STAYING SECURE: SMEs AND CYBER SECURITY

As the digital transformation of business and industry has progressed, more and more businesses have found themselves becoming the target of opportunistic cyber criminals, causing widespread business disruption, financial loss and damaged reputations.

And while larger businesses certainly offer criminals greater financial gain, small-to-medium-sized enterprises are far from being safe from opportunists. Indeed, the Federation of Small Businesses found that in the two years to 2019, SMEs were experiencing almost 10,000 cyber-attacks a day, costing them a total of around £4.5 billion [1].

The frequency of cyber-attacks has also been escalating over the last few years. According to the government's 2020 cyber security breaches survey, of the 46% of businesses that had identified a cyber breach or attack, 32% were experiencing these issues at least once a week.

The outbreak of COVID-19 and the rapid and unprecedented shift to mass remote working has triggered an even greater spate of cyber threats with many hacking and phishing scams being redirected to capitalise on the uncertainty and vulnerability of home workers.

For instance, data provided by cybersecurity company Darktrace in spring 2020 revealed that 60% of all advanced spear-phishing attacks blocked by one of their cyber security products were linked either to COVID-19 or were aimed to trick people by mentioning remote working. The company also revealed that the proportion of attacks targeting home workers rose from 12% of malicious email traffic before the first national lockdown in March to more than 60% six weeks later.

The unexpected shift to remote working for many businesses has also meant that many were unprepared for this assault on their cyber security. In June 2020, a survey by Centrify revealed that 48% of their respondents admitted that their cyber security policies were not fit for purpose in the world of mass remote working.

With this background of growing cyber security risks and accelerated digital transformation, we wanted to find out more about the awareness of cyber security risks among SMEs and what measures they currently have in place to protect their business information. We therefore constructed a survey and sent it out to our SME contacts.

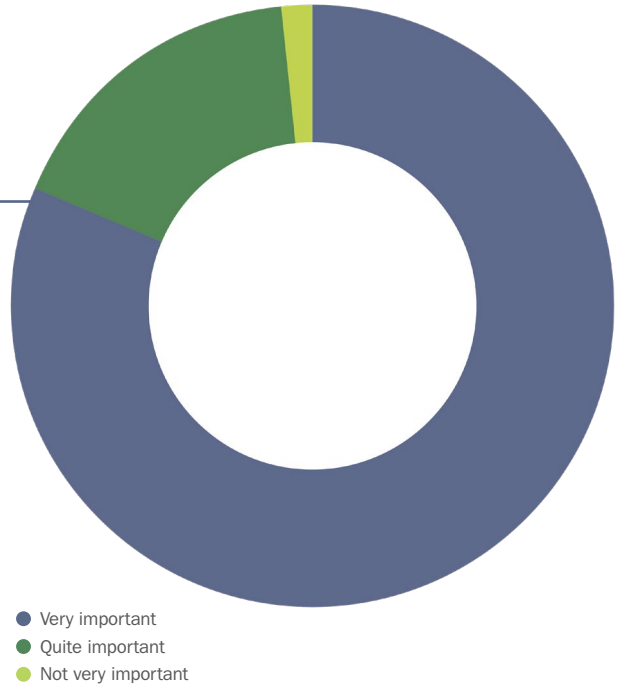
What follows is an in-depth analysis of what we discovered.

[1] Federation of Small Businesses 2019. https://www.fsb.org.uk/resources-page/small-firms-suffer-close-to-10-000-cyber-attacks-daily.html

1 CYBER SECURITY AWARENESS

How important is data security to your business?

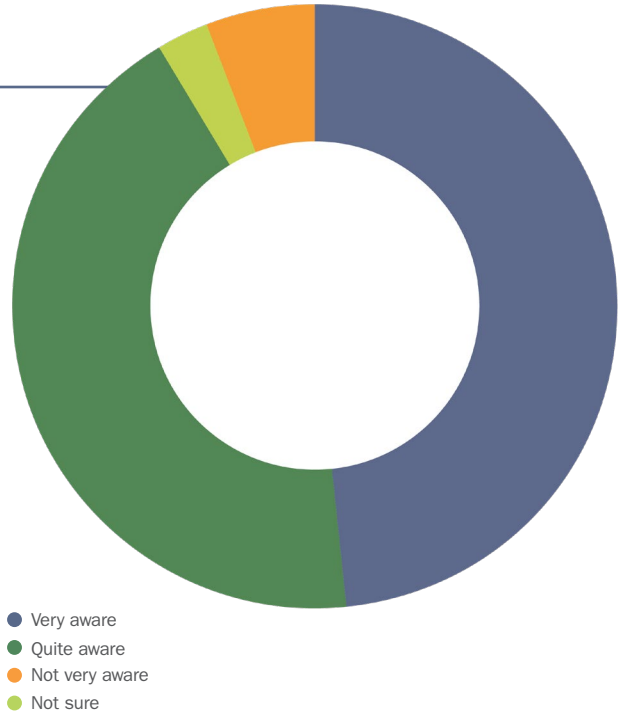
The vast majority of our respondents recognised the importance of cyber security for the success and reputation of their businesses, with 81.4% classing it as ‘very important’ and another 17.1% labelling it as ‘quite important’. This reflects the growing reliance on IT systems within businesses of all sectors, which can seriously affect a business’ ability to operate if compromised.



QUESTION OPTIONS	PERCENT
Very important	81.4%
Quite important	17.1%
Not very important	1.4%
Neither important nor unimportant	0%
Not important at all	0%

How would you describe the level of data security awareness within your business?

Awareness was also generally good, with 48.6% of respondents declaring that they were ‘very aware’ of the risks and another 42.9% saying that they were ‘quite aware’.

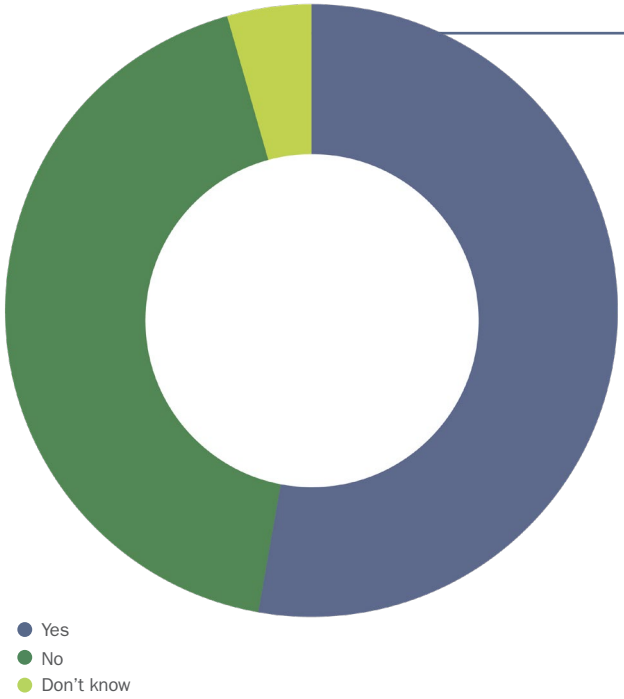


QUESTION OPTIONS	PERCENT
Very aware	48.6%
Quite aware	42.9%
Not very aware	5.7%
Not sure	2.9%
Not aware at all	0%

Would you say that data security was higher priority in 2020?

However, this does not necessarily mean that businesses recognise cyber security as a growing priority, even in the aftermath of the cyber security issues brought by the COVID-19 pandemic.

When asked if data security had been made a higher priority in 2020, just over half of our survey participants (52.9%) said yes, but this leaves a significant 42.9% of respondents who reported that it hadn’t been bumped up the priority list.



QUESTION OPTIONS	PERCENT
Yes	52.9%
No	42.9%
Don’t know	4.3%

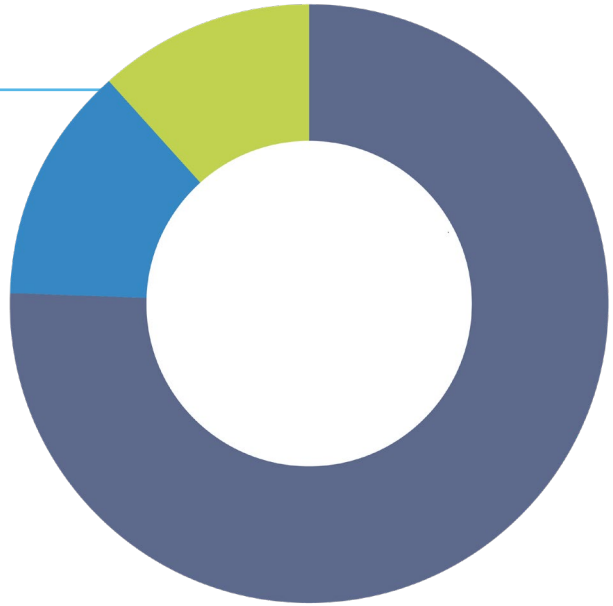
2 INCREASING VULNERABILITY

When it comes to vulnerability, it is evident that the changes wrought by the pandemic in 2020 have affected the confidence of SMEs, leaving them feeling more open to attack.

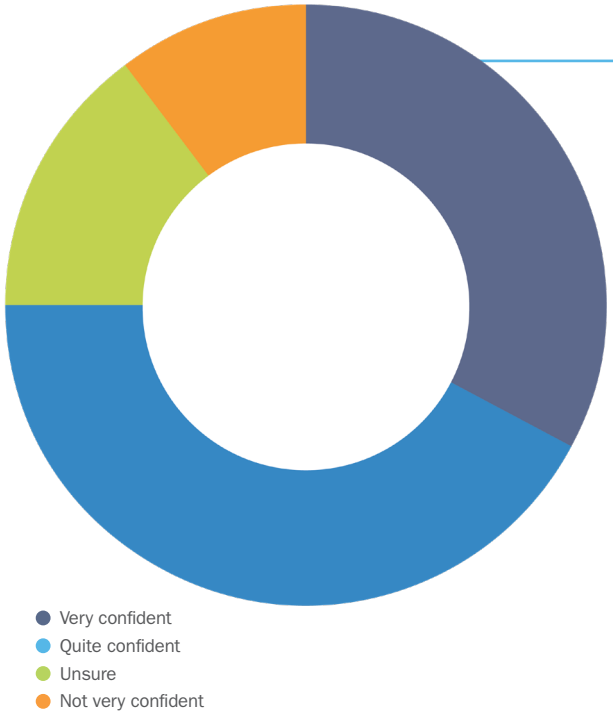
Do you think the pandemic has made businesses more vulnerable to cyber attacks?

A significant 75.7% of respondents admitted that they felt that their business was now more at risk, with one participant pointing the finger at home working: “Home working has definitely increased our exposure to risk,” they explained, “as many people are remotely accessing their office PCs using personal laptops.”

Others reported an increased frequency in attacks, particularly phishing attempts. In light of this, it is surprising that more businesses have not decided to reprioritise their cyber security.



QUESTION OPTIONS	PERCENT
Yes	75.7%
No	12.9%
Don’t know	11.4%



How confident are you that your company could quickly identify and secure a cyber security breach?

Despite feeling more vulnerable, our participants were generally confident about their ability to detect and secure a cyber breach.

Just over a third (34.3%) claimed that they were very confident, but 41.4% were a little more uncertain, saying that they were ‘quite confident’, while another 14.3% were ambivalent, saying that they were ‘unsure’. A notable 10% were left feeling even more vulnerable and reported that they weren’t at all confident about their business’ ability to spot and sort a cyber breach, which suggests that there may be significant gaps in their knowledge of current cyber risks and their defence strategies.

QUESTION OPTIONS	PERCENT
Quite confident	41.4%
Very confident	34.3%
Unsure	14.3%
Not very confident	10%
Not confident at all	0%

3 EXPERIENCES OF A CYBER ATTACK

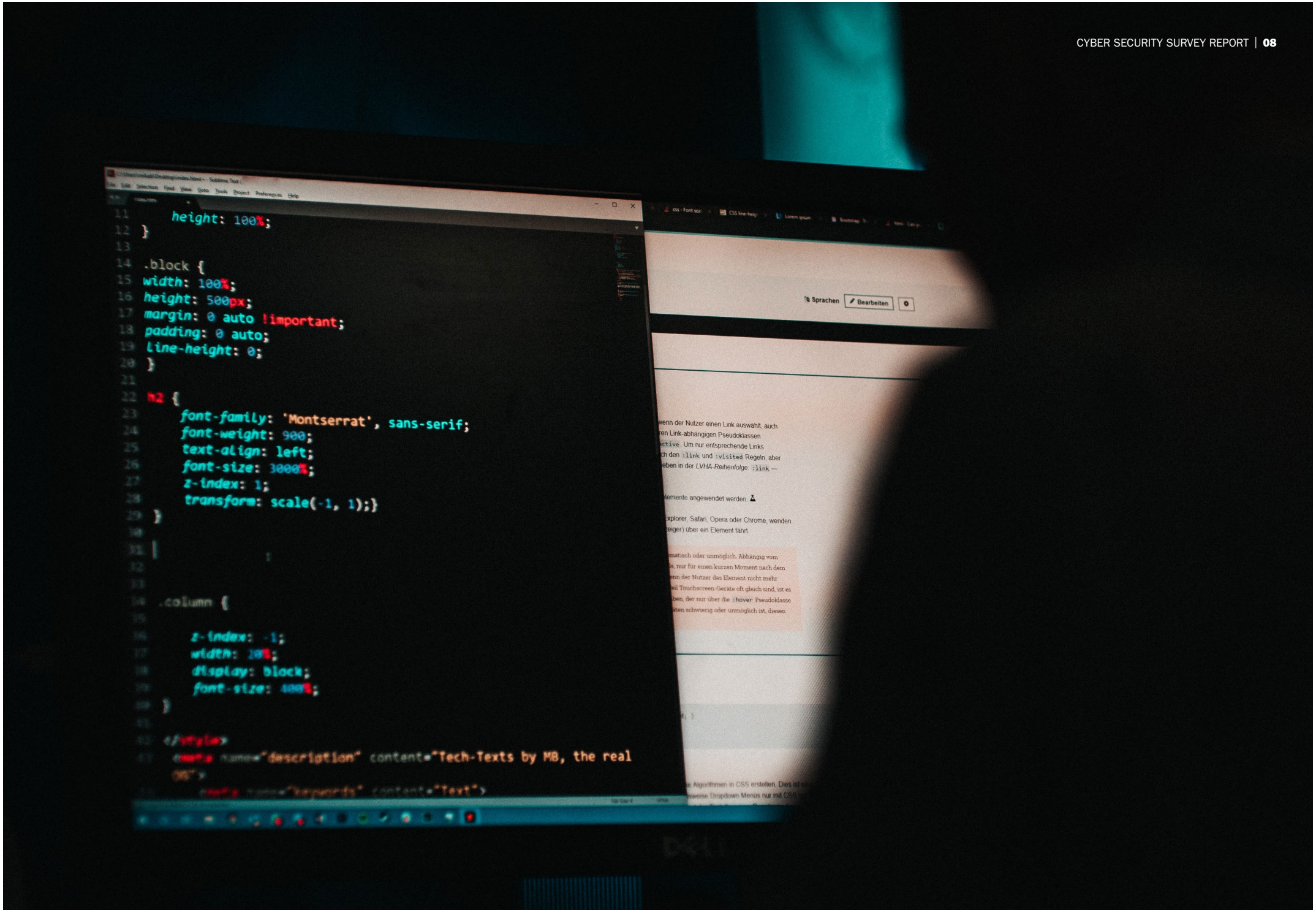
Has your business ever experienced a cyber attack?

For some of our respondents, cyber-attack is not just a theoretical possibility. Of those we questioned, 21.4% have had already had experience of one. These attacks demonstrate the many ways in which a cyber criminal can injure a business.

QUESTION OPTIONS	PERCENT
No	61.4%
Yes	21.4%
Don't know	17.1%

The majority of attacks appear to come in the form of **phishing attempts**, in which a cyber criminal uses the internet, email or a message platform to imitate a reputable company or person and encourage the recipient to click on a malicious link or attachment. In one case, **bank details were stolen**, and the company lost funds as a result.

Another recipient reported a **breach of security via a laptop**, which resulted in compromised information and the demand for a ransom. In a different case, **a hacker took control of a business' information system and encrypted it**, resulting in paralysis of the business for a week. Hacking of emails, mobile devices and social media accounts were also reported.

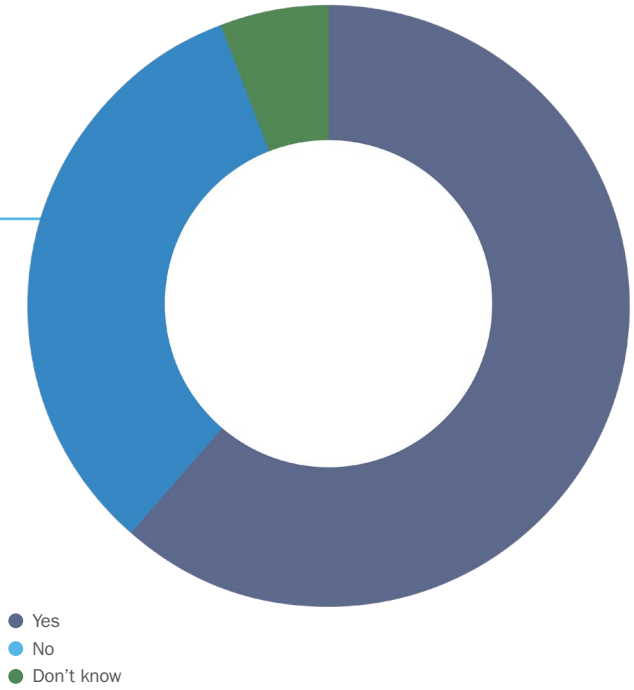

height: 100%;
}
.block {
width: 100%;
height: 500px;
margin: 0 auto !important;
padding: 0 auto;
line-height: 0;
}
h2 {
font-family: 'Montserrat', sans-serif;
font-weight: 900;
text-align: left;
font-size: 3000%;
z-index: 1;
transform: scale(-1, 1);}
}
.column {
z-index: -1;
width: 20%;
display: block;
font-size: 400%;
}
Sprachen
Bearbeiten

4 PROTECTION POLICIES

Setting down detailed processes and procedures is a great way for a company to begin to cultivate a culture of security within the organisation.

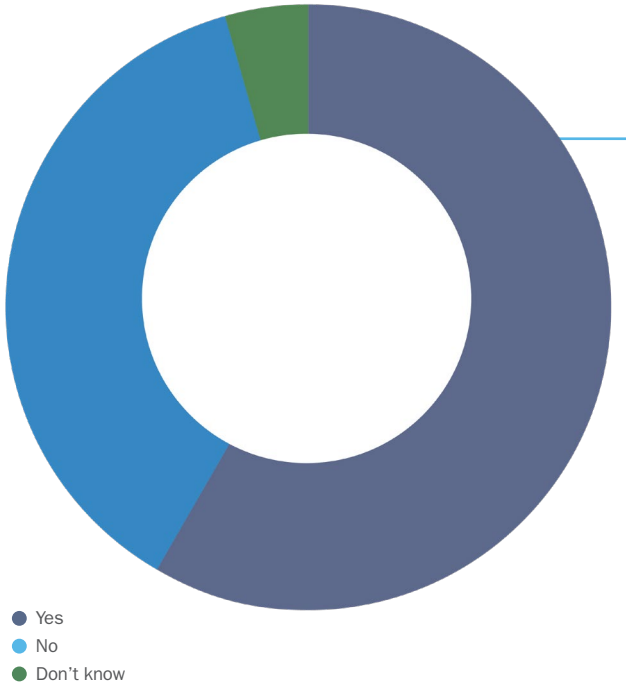
Does your company have a published information security policy?

It is reassuring to see that 61.4% of our respondents have such a policy in place, although this number could be higher given the fundamental security principles these policies cover.



QUESTION OPTIONS	PERCENT
Yes	61.4%
No	32.9%
Don't know	5.7%

Policies work to set out objectives, authorisations, access control, data support and training, among other essential security considerations, to help a business control the confidentiality, integrity and availability of data.



QUESTION OPTIONS	PERCENT
Yes	58.6%
No	37.1%
Don't know	4.3%

Do you have a remote working policy?

There is, however, the possibility that these policies need to be adapted or updated in light of the rapid digital transformation triggered by the COVID-19 pandemic. More specifically, organisations need to ensure that they develop a bespoke remote working policy that can help its employees to keep information safe, no matter where they are.

In June 2020, research carried out by Centrify revealed that 48% of survey participants thought that their cyber security policies were not fit for purpose in the world of mass remote working[2], but our research suggests that some organisations still do not have any policies in place to govern this. Indeed, of our survey participants, only 58.6% currently have a targeted remote working policy in place.

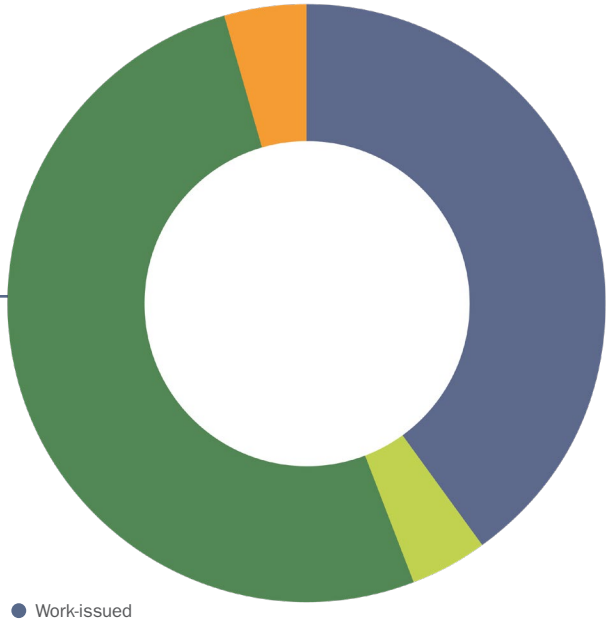
[2] Centrify, 2020. https://www.centrify.com/about-us/news/press-releases/2020/nearly-half-uk-businesses-admit-current-cyber-security-policies/

5 PROTECTION OF MOBILE DEVICES

Do your employees use work-issued or personal mobile devices?

The advent of widespread remote working, or more flexible working, has led to more workers using mobile devices such as laptops, mobile phones and tablets in order to do their job.

This is reflected in our results, with only 4.3% of respondents saying that no mobile devices were being used. Work-issued devices are by far the most common, with 40% of respondents reporting that devices provided by their organisation were being used. A far smaller percentage (4.9%) were using personal devices.

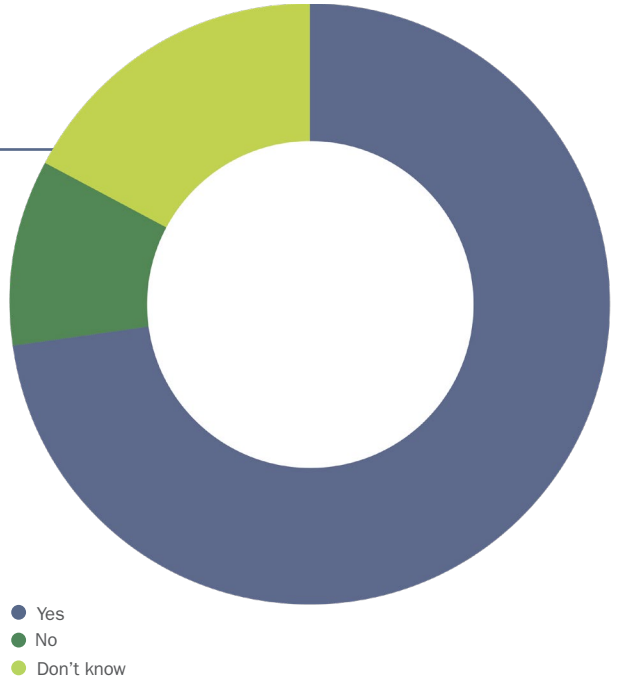


QUESTION OPTIONS	PERCENT
Both	51.4%
Work-issued	40%
Personal	4.3%
Neither	4.3%

The use of mobile devices, whether personal or work-issued, can add another layer of complexity into the protection of business information as it adds to the burden of maintaining malware and virus protection.

If employees do use mobile devices, are these devices protected in any way?

It is reassuring that in our survey, 72.9% of respondents said that these mobile devices were protected, but there is still a worrying 10% who responded that these devices were not protected at all, leaving the business wide open to criminal opportunists. One respondent admitted that remote working and the use of these devices had increased their organisation's risk.



QUESTION OPTIONS	PERCENT
Yes	72.9%
No	10%
Don't know	17.1%

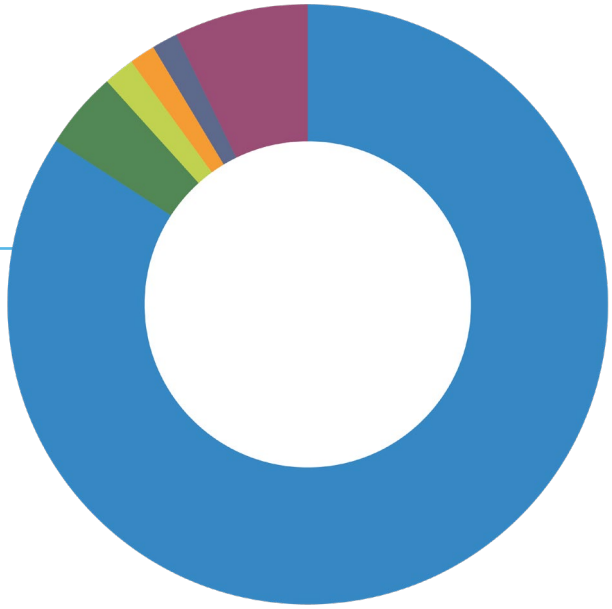
"Homeworking has definitely increased our exposure to risk as many people are remotely accessing their office PCs using personal laptops. We are reviewing our policies and contracts in light of this."

6

VIRUS AND MALWARE PROTECTION

How often is your company's virus/malware updated?

When it comes to providing protection more generally, it is positive to see that the vast majority of businesses (84.3%) take great care to update their virus/malware protection as soon as updates become available – the surest way to maintaining strong defences. However, it is still surprising that there were 4.3% of respondents who do this only on a monthly basis, and that there were also answers that corresponded to updates on a six-monthly, yearly or 'rarely' basis. This suggests that there are a small proportion of organisations that need to get on top of their information protection by prioritising the installation of updates.



QUESTION OPTIONS	PERCENT
As soon as updates become available	84.3%
Don't know	7.2%
Monthly	4.3%
Every 6 months	1.4%
Yearly	1.4%
Rarely	1.4%
Every 2 or 3 months	0%
Never	0%

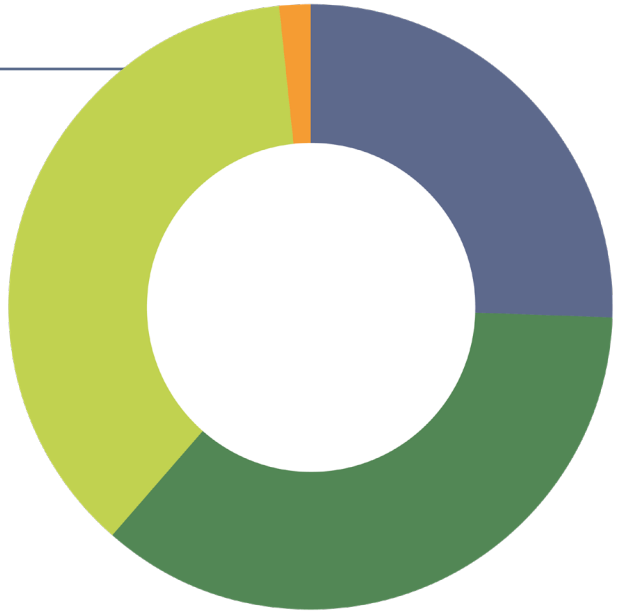
7 DATA STORAGE

The changes to the workplace caused by the coronavirus pandemic have certainly increased many organisations' reliance on digital solutions. This includes a movement towards cloud-based servers.

Where is your company's data stored?

Our survey results show that while 25.7% of respondents still use physical servers, there is a larger proportion who are moving towards both (37.2%). A notable 35.7% are also entirely cloud based.

This introduces new security considerations. Cloud servers do not require the robust back-up procedures of physical servers, and do not need processes in place in case the physical workplace is damaged or inaccessible. However, the choice of cloud provider needs to be considered carefully, and how confidential information is stored, and where in the world it is stored, needs to be investigated and clarified. Disruption protocols also need to be established in case there is an issue with the cloud host.



QUESTION OPTIONS	PERCENT
Both	37.2%
Cloud platforms	35.7%
Physical servers	25.7%
Don't know	1.4%

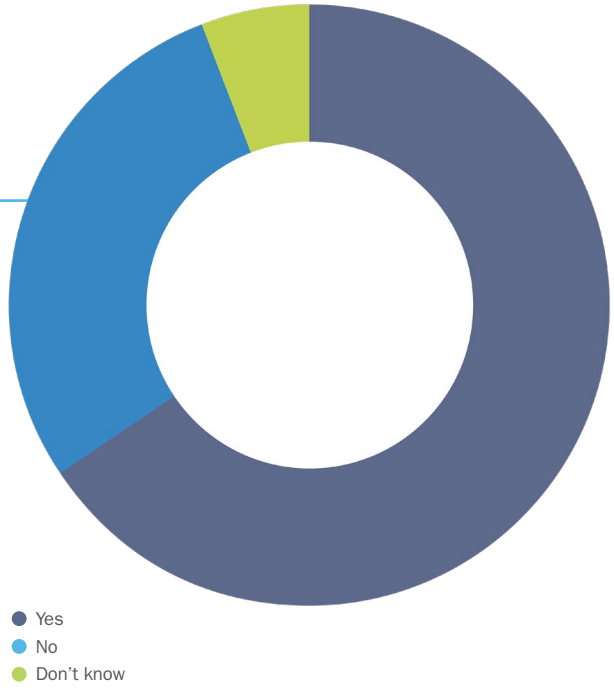
8

PASSWORD PROTECTION

Weak passwords can often be a business' Achilles heel when it comes to keeping information safe and have been identified as one of the top 10 vulnerabilities by techUK and the Cyber Crime Reduction Partnership.

Do you have a password policy?

Given the very evident risks of weak passwords, it is reassuring that 65.7% of our survey participants reported that they have a password policy in place, although this still leaves 28.6% without one and another 5.7% being unsure about one being in place.

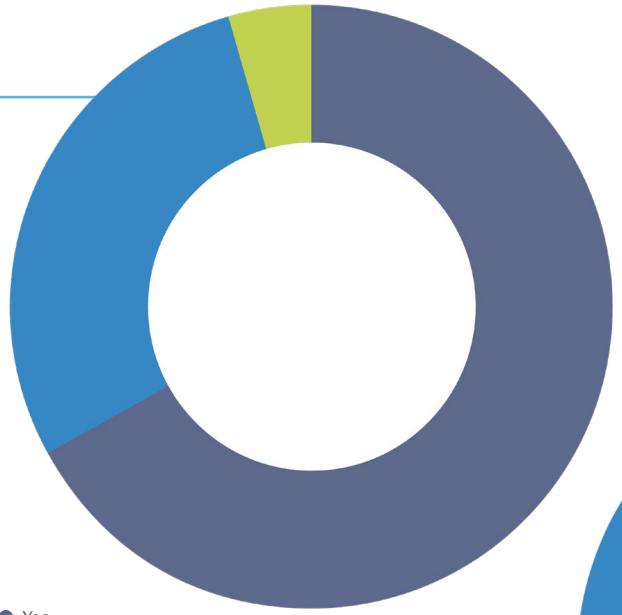


QUESTION OPTIONS	PERCENT
Yes	65.7%
No	28.6%
Don't know	5.7%

Does your organisation enforce password structures and complexity?

Similar figures can be seen in answer to the question about having password complexity enforced, with 67.1% saying ‘yes’ and 28.6% saying ‘no’.

As a simple method of adding a layer of security, implementing a policy that governs the complexity of passwords and how employees remember and save them should be encouraged and we would expect to have a higher positive response in this area.



QUESTION OPTIONS	PERCENT
Yes	67.1%
No	28.6%
Not sure	4.3%

QUESTION OPTIONS	PERCENT
Yes	55.1%
No	33.3%
Don’t know	11.6%

Does your organisation implement two-factor authentication for accessing key information?

Two-factor authentication is also not as widespread as expected, with just 55.1% of respondents saying that they use this method to add security to confidential data.

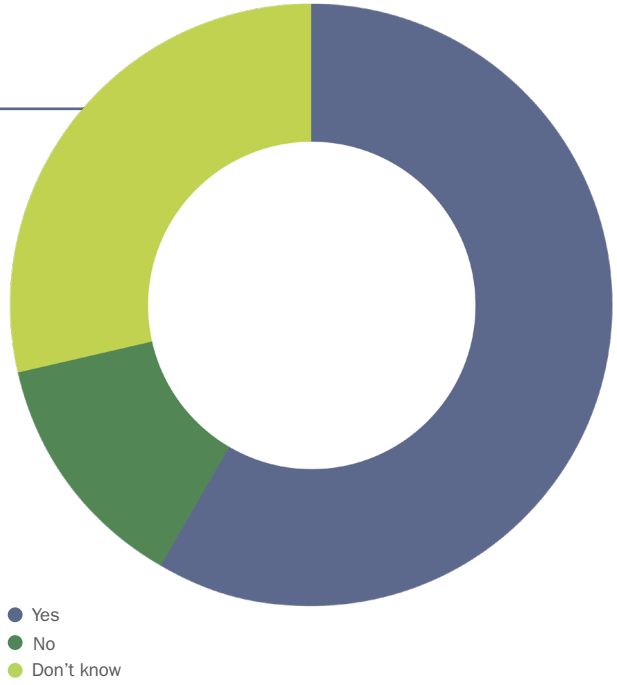
Two-factor authentication is when a PIN or code is needed in addition to a password in order to make it harder for hackers to cheat the system. This PIN can be sent via a SMS, app or security key. By adding a second step to the log-in process and making that step involve something that has to be personally with you, businesses can help to deter more hacking attempts.

9 ACCESS CONTROL

Access control is a security technique that can help to limit who can view or use specific computing resources, thereby restricting access to the most confidential information and minimising risk.

Is logical access control implemented across your business?

In our survey, 58.6% of respondents have implemented this technique in order to protect their information. A surprisingly high percentage (28.6%) reported that they didn't know if this was in place or not, although this may be because access control is only encountered by those who need to use it in order to do their jobs.



QUESTION OPTIONS	PERCENT
Yes	58.6%
Don't know	28.6%
No	12.8%

10 ASSESSING THE RISK

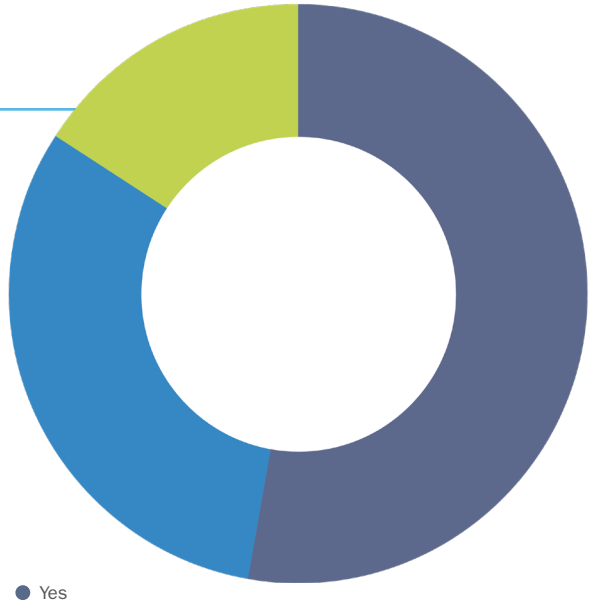
Risk assessments can easily be relegated to the realm of health & safety, but risk can be assessed in every aspect of business, including cyber security.

By carrying out a data security risk assessment, businesses can identify potential threats and then plan ways to mitigate or remove these threats, such as by introducing stronger passwords, access control or staff training.

Has your business ever carried out a data security risk assessment?

Our survey revealed that 52.9% of those questioned have carried out a risk assessment of this kind, which will help them to react to and recover from a cyber threat. However, a not insignificant proportion (31.4%) have not carried out a risk assessment of this kind, while a further 15.7% are unsure.

There is evidently a need for better communication of the benefits of this kind of risk assessment, as well as training on what to include and how to carry one out. This will give more businesses the motivation to use data risk assessments to raise awareness of cyber risks and improve their confidence in reacting to threats.



QUESTION OPTIONS	PERCENT
Yes	52.9%
No	31.4%
Don't know	15.7%

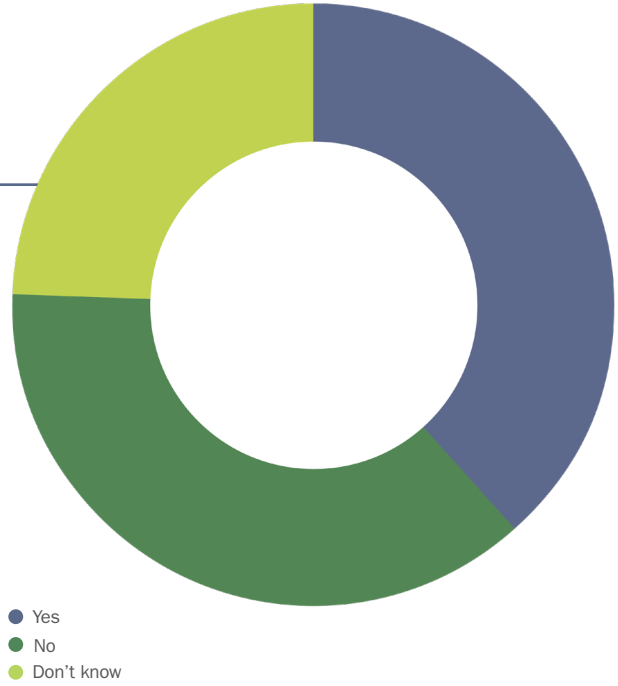

Login
****
Sign in

11 INSURANCE

Does your business have cyber insurance?

We also questioned our participants on whether or not they pay for cyber insurance, which can cover an organisation for the disruption during and after a cyber incident. It is possible that this kind of insurance may become more popular as more organisations recognise the potential financial and reputational losses of a cyber-attack.

Among our respondents, just over a third (38.6%) already have this kind of insurance, with 37.1% confirming that they don't. However, there is a significant percentage (24.3%) who didn't know, which makes it difficult to draw any further conclusions.



QUESTION OPTIONS	PERCENT
Yes	38.6%
Don't know	37.1%
No	24.3%

12

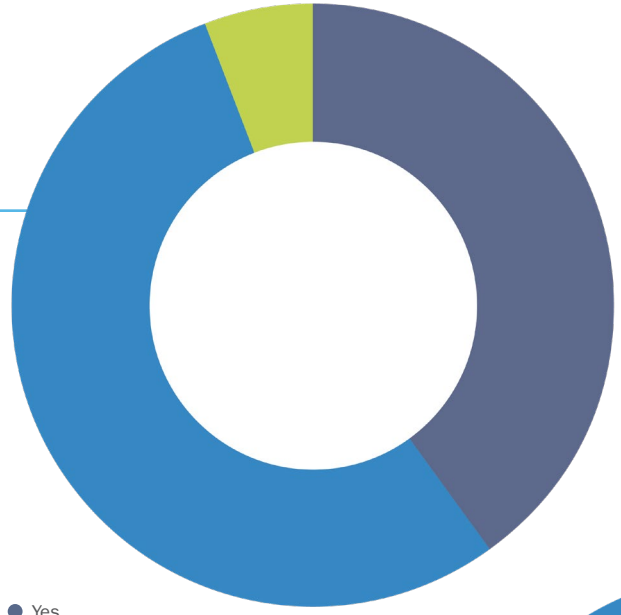
STAFF TRAINING

Employees sit on the frontline of cyber security, but can be overlooked, which makes them the weak point in an organisation's cyber strategy.

Training on how to spot a cyber threat, phishing email or suspicious activity, and knowing how to report it, are key to a swift response and can make it much more difficult for opportunists to gain access to a business' information.

Does your business offer staff training on data security and cyber security threats?

From our survey it appears that many organisations are not realising the value of teaching their staff about cyber-crime. Of those we questioned, just 40% currently provide training on this topic, with 54.3% not providing any training at all. This is a significant weakness, but one that can easily be resolved with certified eLearning training, which can be accessed whenever and wherever a staff member is.

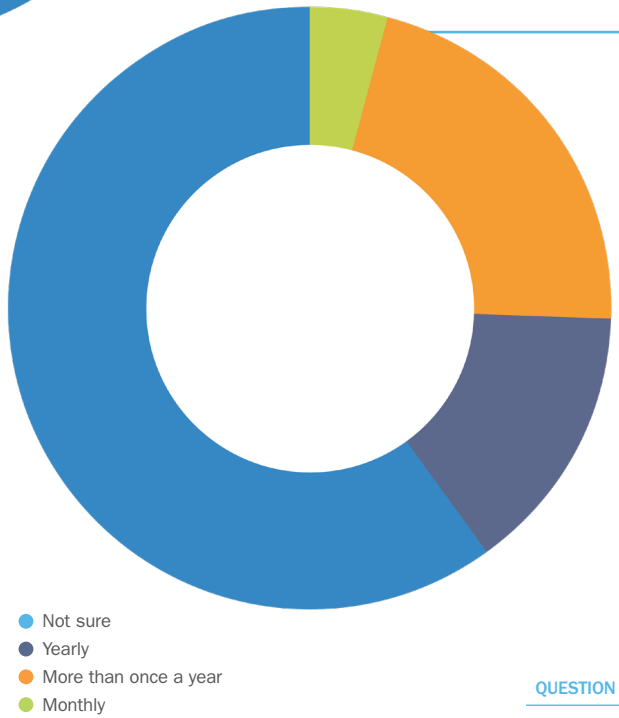


QUESTION OPTIONS	PERCENT
No	54.3%
Yes	40%
Don't know	5.7%

If so, how often is the training provided?

This training should then ideally be refreshed regularly as new cyber threats emerge. As more workers are now working remotely, this is even more important as staff members cannot so easily check on the validity of emails or report anything suspicious. In our survey, the frequency of training provided was adequate, with the majority (21.5%) providing it more than once a year and 14.3% providing it yearly.

Businesses should, however, look to refresh this training if new cyber threats are identified in data risk assessments or if there is a significant change to the way the business works, such as switching to remote working.



QUESTION OPTIONS	PERCENT
Not sure	60%
More than once a year	21.4%
Yearly	14.3%
Monthly	4.3%

13

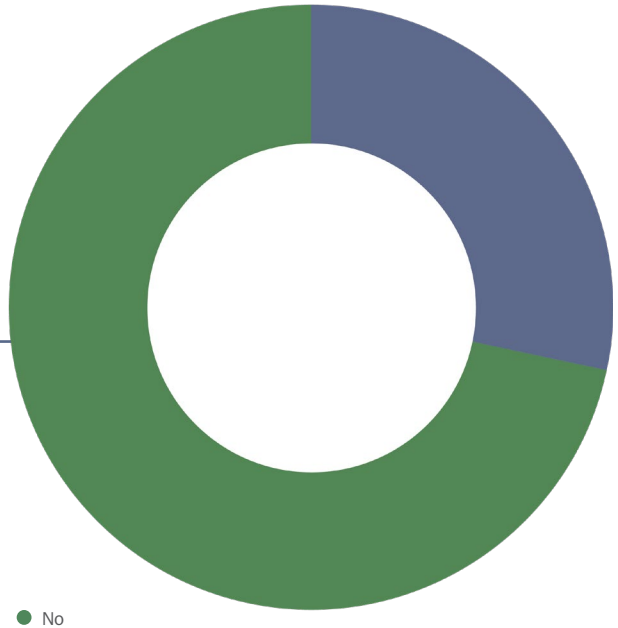
INFORMATION MANAGEMENT SYSTEMS

In our survey, 28.6% of respondents have placed great importance on cyber security by implementing ISO 27001, the international Standard for information security.

This Standard has been developed by the ISO (International Organisation for Standardisation), which calls upon information security experts from all across the world to develop its requirements. With 114 controls designed to help businesses manage their information security and keep their data confidential and in-line with the latest legislation, the Standard can help businesses to develop a real culture of security.

Is your organisation certified to ISO 27001?

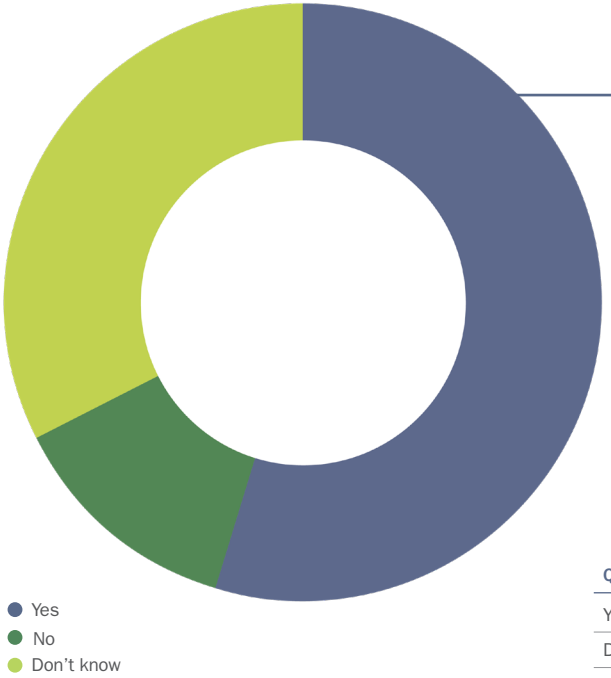
Of those we questioned, 28.6% have implemented this Standard, but it is likely to become more popular going forward. At QMS, we are expecting an increase of around 10% in sales of this particular Standard in 2021.



QUESTION OPTIONS	PERCENT
No	71.4%
Yes	28.6%

If yes, has ISO 27001 made you feel more confident about your cyber security?

A significant percentage of respondents with the Standard also reported that it has made them feel more confident about their cyber security, with 54.8% affirming this.



QUESTION OPTIONS	PERCENT
Yes	54.8%
Don't know	32.3%
No	12.9%

CONCLUSION

Organisations have experienced significant change over the last year and their reliance on digital information solutions has increased significantly. It is also clear that the risk of cyber-attack has risen alongside this greater reliance.

Our survey has revealed that the majority of organisations have a good understanding of the threat of cyber-attack and are aware of the risks to them. Most have also been proactive in creating information security policies and implementing controls such as additional password protection.

However, there is still much room for improvement. More businesses need to develop their remote working policies and should look to implement regular data risk assessments and staff training to ensure that their business is equipped to respond to potential threats. There are also other easy defence measures, such as enforced password complexity, which could be quickly introduced to add another layer of security.

With regularly updated policies, regular staff training and comprehensive data risk assessments, businesses can become more confident in their ability to spot, mitigate and respond to cyber threats, keeping their information and their reputations intact.

These can be implemented on the organisation's own initiative, or they can be enacted as part of a more comprehensive system of processes and controls, such as in an information management system.

This should be done as soon as possible to ensure that more SMEs do not become the victims of disruptive cyber-crime, which shows no sign of slowing down even as the threats of the COVID-19 pandemic recede.

QMS INTERNATIONAL

Get in touch

To learn more about our service, ISO 27001 or any other ISO certification, just contact us by phone or email. You can also visit our website to get a quote online or chat live with one of our friendly team.

0333 344 3646 **enquiries@qmsuk.com** **qmsuk.com**

QMS International, Muspole Court, Norwich NR3 1DJ.