April 2021

Northern Ireland Cyber Security Research

SMEs and Charities

Author
Fiona Rooney
and Karen Clarke

NI Cyber Security Centre

Ipsos MORI

Contents

List of Figures

List of Tables

1 Introduction and Methodology

Introduction

Ipsos MORI Northern Ireland were commissioned by the NI Cyber Security Centre (NICSC) part of the Department of Finance to conduct quantitative research among small and medium sized businesses (SMEs) and voluntary and community (V&C) sector organisations (charities) in Northern Ireland into current cyber security practices and barriers to implementing or, improving cyber security in these organisations.

The NICSC wanted to better understand the level of cyber awareness, activity and resilience that currently exists across Northern Ireland businesses and in the voluntary and community sector. By conducting the survey among SMEs and those in the V&C sector this provides valuable and important information to the NICSC on the cyber health, resilience and readiness of businesses. This in turn will help the NICSC to prioritise the necessary advice, guidance and support to assist in making businesses more cyber resilient and collectively making Northern Ireland cyber safe, secure and resilient to be working online.

The aim of this research is to help the NICSC to understand what guidance or additional interventions or support organisations may need for cyber security. The survey was open to all types of small businesses and charities - not just those who had experienced cyber security breaches. It was important to speak to organisations that do not have any cyber security issues, or that outsource their cyber security, as their views and experiences were important too.

The survey was set up so as not to include technical terminology as it was important to be able to garner the views of all types of business and V&C sector organisations, not just expert opinion on cyber security. The NICSC wanted to hear from all types of businesses regarding their level of cyber awareness, activity and resilience in order to understand how they can best provide advice, guidance and support to make organisations in Northern Ireland more cyber resilient

Key Research Questions

The specific objectives of this research are to provide a robust evidence base, to: -

1. Understand current levels of cyber health within the NI Business Sectors. This is determined by current knowledge of cyber threats, knowledge of protective actions that can be taken for businesses and staff, preparedness for recovery from a cyber event, and level of independent assurance sought on their business.

2. Understand current barriers and constraints to implementing good cyber security.

3. Provide recommendations on measures that can develop good cyber security practices and culture across NI Business Sector and charities.

In order to meet the above objectives, a quantitative study was commissioned and carried out using a Computer Assisted Telephone Interviewing (CATI) survey.

Sampling

Interviews were completed with 451 organisations: 304 SMEs and 147 organisations from the V&C sector. We identified businesses from the Dun and Bradstreet databases and from the NI Charity Commission database. SMEs are defined as businesses with less than 250 employees and a turnover of less than £41m. It was agreed that the SME sample would be drawn to be representative of SMEs in Northern Ireland using the Standard Industrial Classifications (SIC) codes which categorise business. Sole Traders were also included in the sample.

Questionnaire Development

Ipsos MORI in conjunction with the NICSC drafted the questionnaire which was used with both SMEs and V&C organisations. The Northern Ireland survey was based on the GB[1] questionnaire but also had questions specific to Northern Ireland. There are several advantages to this: firstly using some of the same questions allows for a comparative analysis across the UK and secondly it was an efficient use of time and resources by using a pre-existing survey that has already been successfully used with SMEs. We proposed a number of amendments/improvements to the UK survey to ensure that it was up to date and relevant to small businesses in Northern Ireland, including:

- In the introduction to the survey we requested to speak to the senior person at the organisation with the most responsibility when it comes to cyber or IT security;

- Ensuring that questions link to existing guidance for organisations, such as Cyber Essentials, the 10 Steps, and the NCSC guides for small businesses and charities;

[1] Department for Digital, Culture, Media and Sport. Cyber Security Breaches Survey. Ipsos MORI, 2021

- A review of the list of cyber attacks covered in the questionnaire and asking about understanding and experience of these types of attacks.

- The final questionnaire had an interview length limit of 15 minutes

Piloting

Prior to the commencement of the fieldwork Ipsos MORI conducted a pilot of the questionnaire among participants. The purpose of this was to test the questionnaire length, the script and the best ways to encourage participation. We conducted 10 pilot interviews (5 SMEs and 5 V&C sector organisations). As a result of the pilot it was evident that the questionnaire was too long at more than 25 minutes. However, no participants reported that they did not understand the questions and they offered that the questions were easy to understand and had a logical progression through the subject matter. The pilot also provided additional information about likelihood to complete the survey and the likelihood of contacting the correct person within the organisation. It was immediately obvious that many SMEs are still closed or, that individuals are working from home/ furloughed due to COVID 19 restrictions. Hence, SMEs were not answering their main switchboard phones. Once contact was made with an individual within an SME it took a number of calls back to the SME in order to find the appropriate individual. Ipsos MORI also sent out emails to clarify the nature and scope of the survey and to verify that we were conducting this on behalf of the NI Cyber Security Centre (NICSC), part of the Department of Finance.

Fieldwork Issues

Ipsos MORI commenced fieldwork on the 22nd February 2021 and interviewing was complete on the 31st March 2021 with 451 interviews completed. This was an unusually slow response rate for a business survey of this nature, and we would have expected to have completed all 450 interviews by 12th March 2021. However, as fieldwork progressed it was evident the effect that COVID 19 restrictions was having on businesses meant that finding businesses which were open or, who were answering their main switchboard number was very challenging. Added to that, finding the appropriate person to speak to involved multiple call backs. Additionally, given the subject matter and the number of warnings being issued by police and other bodies about scam phone calls and emails. Ipsos MORI also sent out many more confirmation emails than usual.

A total of 364 emails were sent to potential participants. Although given the nature of the survey this was an encouraging finding it did slow the process.

Fieldwork Processes

Fieldwork was conducted using Computer Assisted Telephone Interviews (CATI). The questionnaire for this survey was scripted for CATI using SPSS Dimensions software, a unified survey scripting, interviewing, and data processing package, provided by IBM Dimensions. This allows for all the functionality one would expect in a state-of-the-art survey software package. These include split-sampling; modularisation, randomisation, and rotation; logic-checks; dynamic text substitution; concurrent interviewing; links to look-up databases; interviewer comments; and synchronisation with secure servers to meet the most stringent of data security requirements.

Ensuring accuracy in the CATI instrument is critical to ensuring data quality since this is where most of the parameters of the data are set. The CATI programme defined the structure and content of the variables and these were linked with programmed routes and a number of hard checks, where the interviewer will be required to correct values that are definitely wrong and 'soft' checks, where potentially incorrect values are brought to the attention of the interviewer for confirmation or correction.

The CATI script contained 'hard' checks, for example:

- The acceptable range of responses at a question, for example, if the participant's company has more than 250 employees.
- The acceptable relationships between questions asked (the routing) – for example, if the participant reports no IT problems then they would not be asked qualifying questions about IT problems.
- The CATI programme also defined different types of 'soft' check, requiring interviewers to confirm or correct implausible but possible data, for example, if a company has a turnover of more than £50m etc.

A number of procedures and processes were built into the script for checking such as a dummy topline data run from the CATI script, which creates randomly generated data. From this, we were confident that the questionnaire was correctly scripted and that the data were in line with expectations (for example, single-coded responses only allowing a single answer).

We also created dummy datafiles. These provided all responses to the survey on a participant-level basis. By filtering the data, we could check routing protocols that are contingent upon multiple responses. By contrast, standard script checking procedures only allow routing to be checked where it is contingent upon a single response.

We adopted these processes to ensure that there were no errors in the interviewer script, or the data generated from the survey. As well as ensuring that we had a thorough process in place to check the survey programming, all members of the team had extensive experience of checking interviewer scripts.

1.1.1 Briefing

Prior to the launch, the Ipsos MORI team fully briefed the telephone interviewers on the aims and objectives of the research, and the content of the questionnaire. There was an opportunity for the interviewers to conduct several mock interviews. A set of interviewer instructions were also produced as a reference for the interviewers during the fieldwork period.

2

Summary of key findings

Cyber Security Controls

How confident are you that the following are securely configured?

87%

MOST CONFIDENT that anti-virus and malware software is on and up

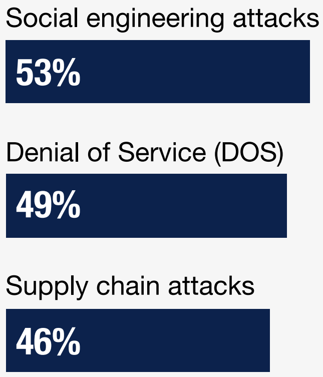
46%

LEAST CONFIDENT that services and functions not necessary are disabled from systems

Understanding of threats

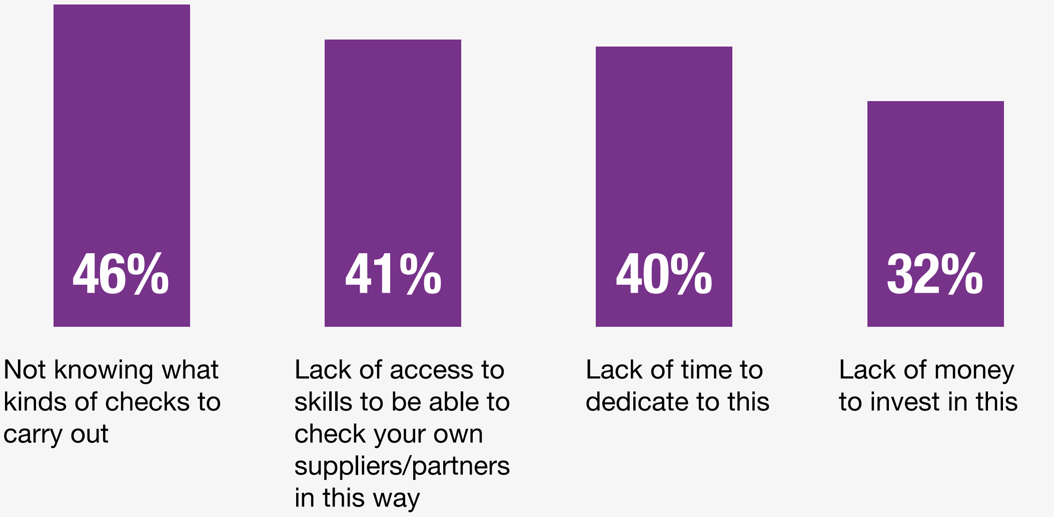
How well do you understand the following cyber threats?

NEVER HEARD OF:



Barriers to implementing good or better cyber security

Which of the following, if any, have made it difficult to manage any cyber security risks in your organisation or with your supply chain or partners?

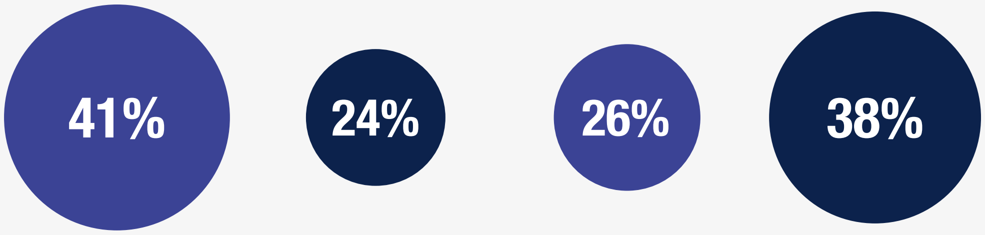


Value of services

What value would you put on each of these services to protect your organisation from a cyber attack?

LEAST INTERESTED/ LEAST LIKELY TO PAY FOR

MOST INTERESTED/ MOST LIKELY TO PAY FOR



Certification of your organisations security like council hygiene schemes

Staff training and awareness

■ No interest ■ Up to £500

Policy controls

And which of the following rules or controls, if any, do you have in place, do not have in place or plan to have in place in the next 6 months?

RULES AND CONTROLS MOST LIKELY TO HAVE

81% Up-to-date malware/ anti-virus protection

76% Restricting IT admin and access rights to specific users

74% A password policy that ensures users set strong passwords

RULES AND CONTROLS LEAST LIKELY TO HAVE

30% Separate WiFi networks for staff and for visitors

28% Any monitoring of user activity

26% A virtual private network, or VPN, for staff connecting remotely

3 Organisations Profiles

Introduction

This section details the demographics of the SMEs and charities who participated in the survey. At the outset of the survey quotas were set on business and charities, location, size of businesses according to number of employees and sector according to SIC codes. The table below provides an overview of the number of SME and charity respondents by location.

Table 3.1: Location quota

SME Business location		Charity location	
Antrim and Newtownabbey	21	Antrim and Newtownabbey	11
Ards and North Down	22	Ards and North Down	12
Armagh City, Banbridge and Craigavon	35	Armagh City, Banbridge and Craigavon	15
Belfast	39	Belfast	29
Causeway Coast and Glens	26	Causeway Coast and Glens	12
Derry City and Strabane	17	Derry City and Strabane	13
Fermanagh and Omagh	25	Fermanagh and Omagh	7
Lisburn and Castlereagh	26	Lisburn and Castlereagh	12
Mid and East Antrim	25	Mid and East Antrim	12
Mid Ulster	34	Mid Ulster	9
Newry, Mourne and Down	34	Newry, Mourne and Down	15

SMEs

Table 3.2: SME Size by Number of Employees

SME Size	Number	%
Sole Trader	58	19%
2 to 9	157	52%
10 to 49	73	24%
50 to 99	12	4%
100 to 249	3	1%

Table 3.3: SME by Sector

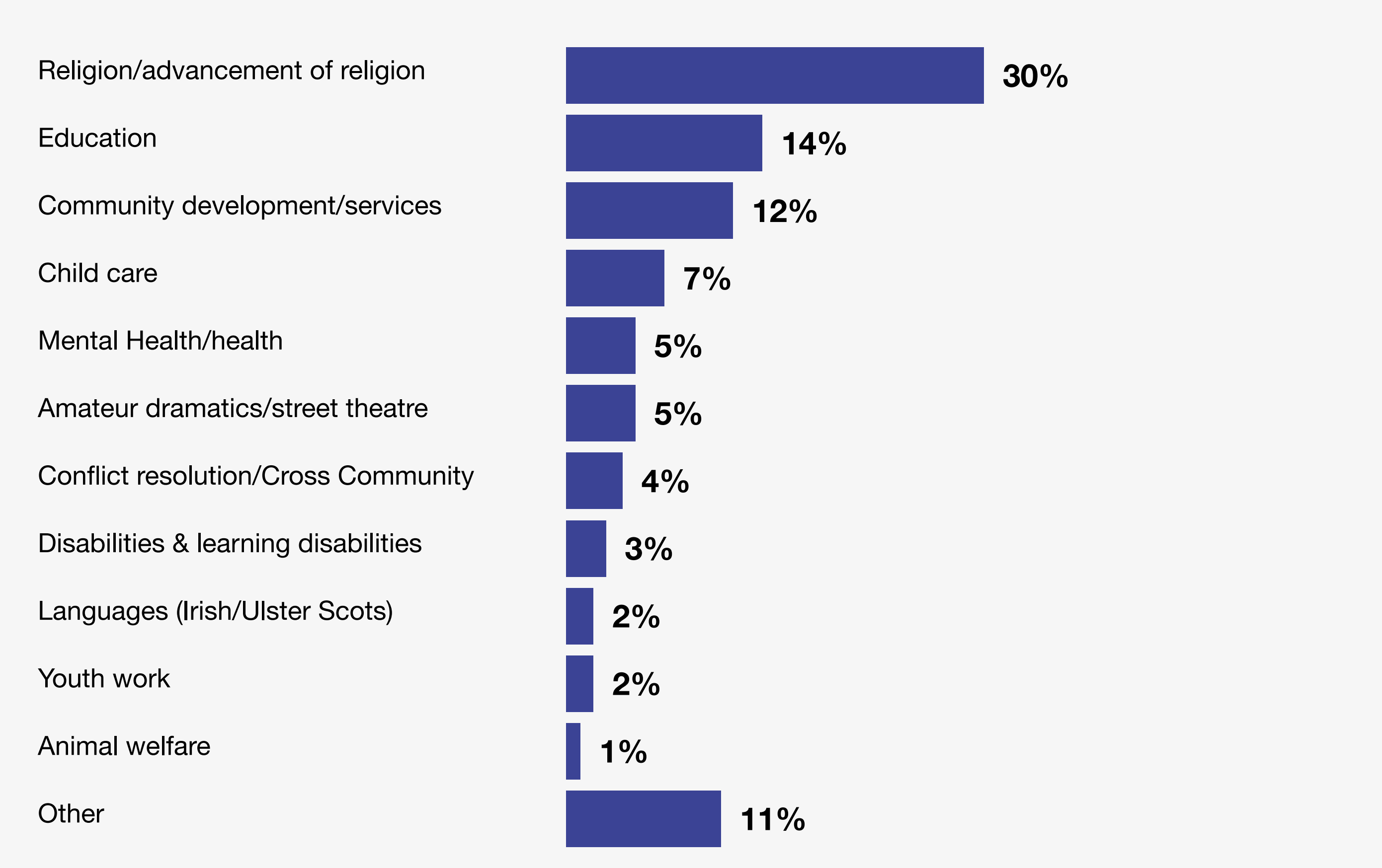
Sector	Number	%
Agriculture, Forestry & Fisheries	19	6%
Mining & Quarrying**/Electricity, gas, steam & air conditioning supply **/Water supply, sewerage, waste management and remediation activities**	10	3%
Manufacturing	25	8%
Construction	29	6%
Wholesale and retail trade; repair of motor vehicles and motorcycles	43	10%
Transportation and storage	7	10%
Accommodation and food service activities	10	3%
Information and communication	6	2%
Financial and insurance activities	19	6%
Real estate activities	8	3%
Professional, scientific and technical activities	12	4%
Administrative and support service activities	2	1%
Public administration and defence; compulsory social security	2	1%
Education	21	7%
Human health and social work activities	27	9%
Arts, entertainment and recreation	8	3%
Other service activities/Activities of households as employers; undifferentiated goods- and services-producing activities of households for own use/Activities of extraterritorial organisations and bodies	56	18%

No quotas were set for charities.

Charity Organisations

The majority of charities interviewed were religious organisations, community groups and educational organisations.

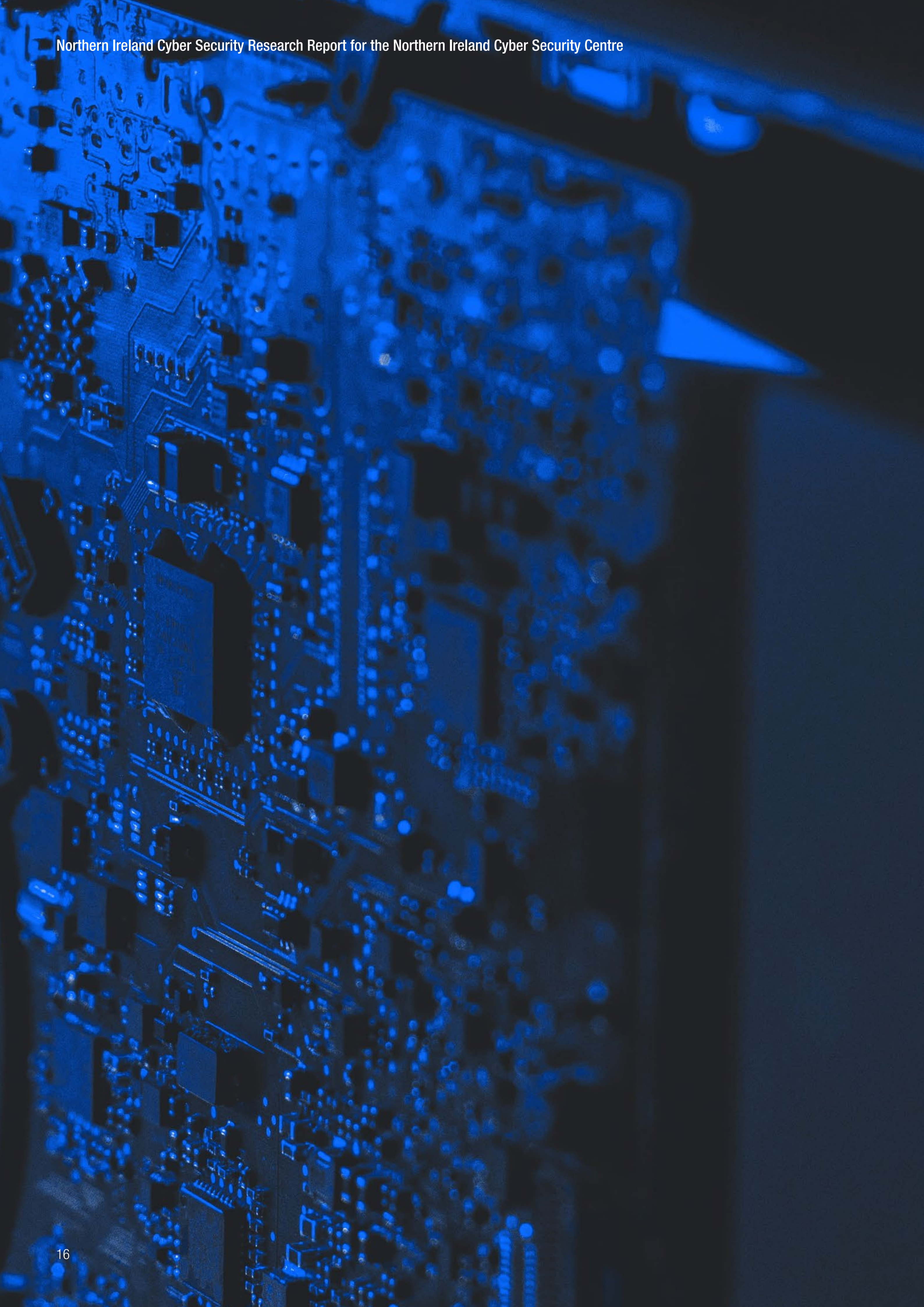
Figure 1: Main purpose of charity organisations



Base: Charities (147)

Having ascertained the profile characteristics of the organisation all participants were informed that for the rest of the survey, the interviewer would be asking them about cyber security. This term ‘cyber security’ was defined for them as meaning:

Any strategy, processes, practices or technologies that organisations have in place to secure their networks, computers, programs or the data they hold from damage, attack or unauthorised access.



4 Cyber Governance

Introduction

This section deals with cyber governance and asked participants a range of questions. These questions centred on

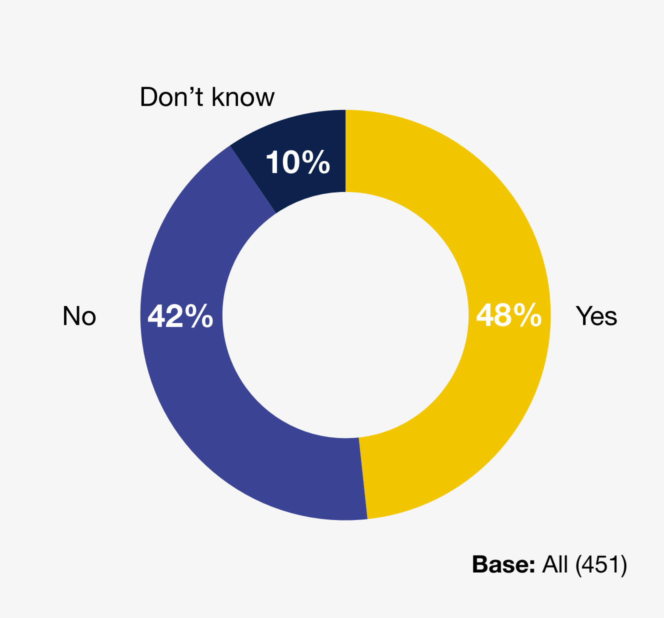
- **Complicance** with standards and accreditations,
- **Risk** analysis within the business or V&C sector organisation,
- **Identifying** security risks;
- **Documented** Cyber Policies;
- **Cyber** security audits; and
- **Management** of and support for IT and cyber security.

Compliance with Standards and Accreditations

4.1.1 Cyber as a board level risk

Approximately half of all organisations interviewed agree that their organisation lists cyber as a board level risk (48%). There is no significant difference between SMEs (48%) and charities (49%) in terms of cyber security as a board level risk.

Figure 2: Board level risk



Base: All (451)

These findings are consistent with the UK Cyber Security Breaches Study[2] which noted that just over one third of small businesses (38%) and micro businesses (36%) had a board member or, trustee with a cyber security brief.

[2] Department for Digital, Culture, Media and Sport Cyber Security Breaches Survey. Ipsos MORI 2021

4.1.2 Standards and accreditations

A very small number of organisations adhere to or have any cyber security standards or accreditations. For most of the standards and accreditations there is no difference between SMEs and charities.

Table 4.1: Standards and accreditations

	Yes, have and adhere	No, do not have
ISO 27001	5%	95%
NIS Directive	2%	97%
The Payment Card Industry Data Security Standard, or PCI DSS	14%	86%
Any National Institute of Standards and Technology (NIST) standard	1%	99%
Cyber Essentials or CE+ standard	1%	99%

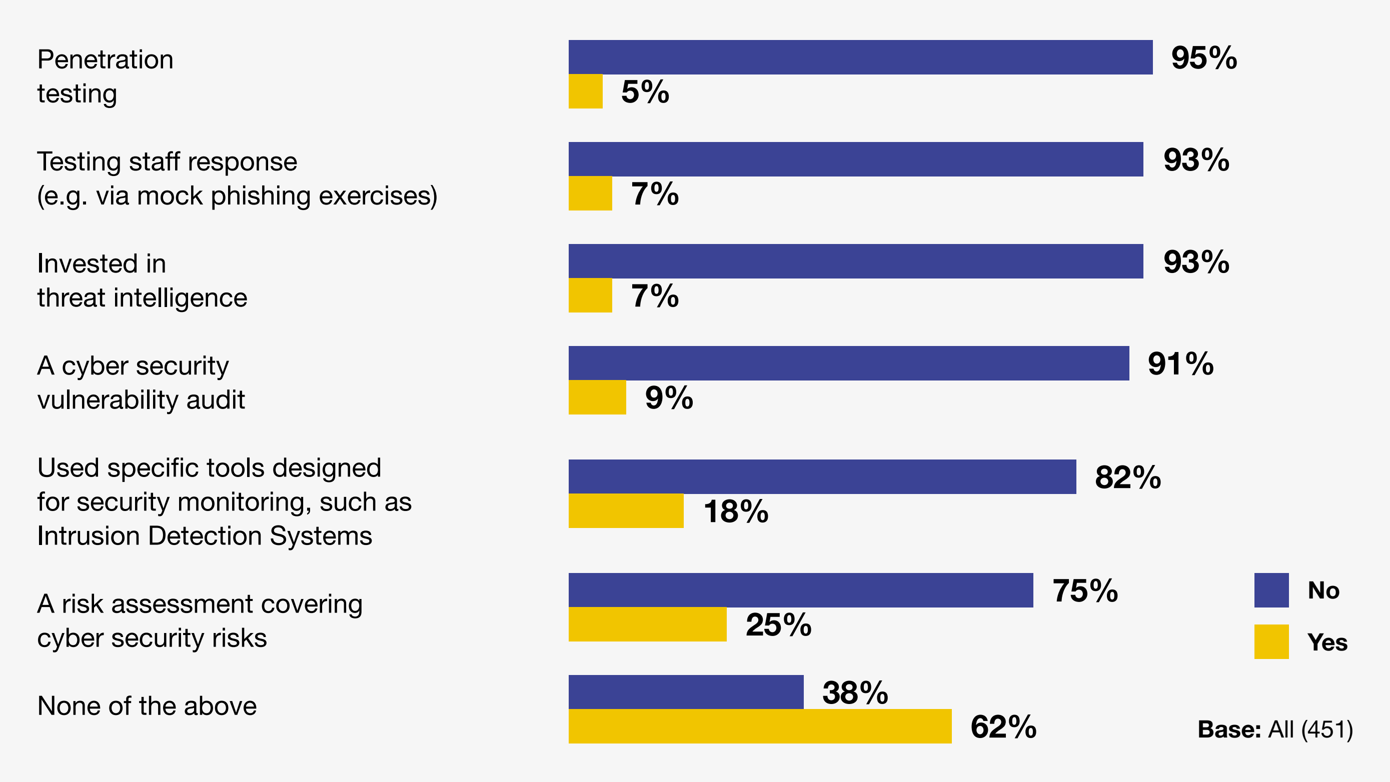
However, there was one exception with SMEs being more likely to have the PCI DSS (18%) than charities (6%). This is likely to be due to the fact that businesses are more likely to be taking payment for goods and services from individuals than charities.

The UK Cyber Security Breaches study also found very low levels of adherence to standards or accreditations, for example, a very small proportion of businesses and charities (4%) reported that they adhered to the government supported Cyber Essentials scheme. As with this study accreditation to the PCI DSS was the most common in the UK with just over one quarter (28%) reporting that they adhered to this. It is not clear if this is because there were lower levels of responses from Northern Ireland retail businesses than in the UK or, if retail in Northern Ireland have lower levels use of digital sales/card payments.

Identifying Cyber Security Risks

More than six in ten organisations (62%) have done nothing in the past 12 months to identify cyber security risks to their organisation. Whereas 38% have taken action to identify cyber security risks. Of those who have tried to identify cyber security risks to the company the most likely review is a risk assessment covering security risks and/or the use of specific tools designed for security monitoring, such as Intrusion Detection Systems. There is no significant difference between SMEs and charities in terms of likelihood to try to identify cyber security risks.

Figure 3: Identifying cyber security risks

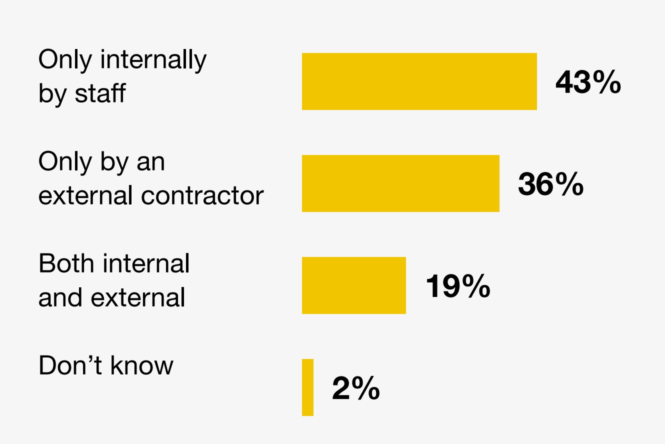


Base: All (451)

As highlighted above, whilst the majority of organisations (62%) had not undertaken any of the listed cyber security activities one quarter (25%) had completed a risk assessment that included cyber security risks. Less than one fifth (18%) agreed that they used specific tools designed for security monitoring. There was no significant differences between charities and SMEs in the extent to which they had implemented any of the cyber security activities, however a slightly larger proportion of charities than SMEs reported that they had undertaken a risk assessment which included cyber security risks (29%, compared to 23%).

The UK cyber security breaches study found that just over half (52%) of all businesses had undertaken any action to identify cyber security risks. However, it is also highlighted that large business and high-income charities are more likely to undertake activities to identify cyber security risks.

Figure 4: Who conducted the cyber security vulnerability audit.



Base: All who have completed a cyber security vulnerability audit (42)

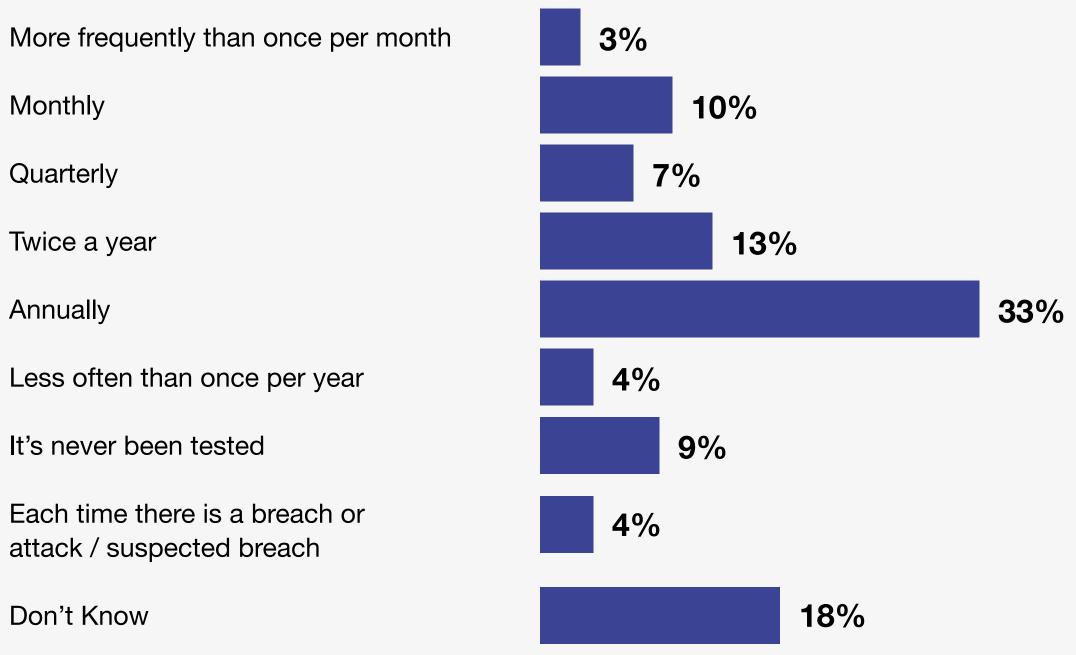
It appears that charities are more likely to use only internal staff whereas SMEs are more likely to use an external contractor. Given the potential costs involved for external contractors it would be logical that charities are more inclined to use internal staff however due the small number of responses involved firm conclusion should not be drawn from this.

Documented Cyber Policies

A minority of organisations (17%) have a documented cyber incident plan. Charities are more likely (22%) to have an incident plan than SMEs (15%), but overall 77% had no incident plan. A small proportion of organisations (6%) didn't know if they had a cyber incident plan. The proportion of organisations that have a documented cyber incident plan appears to be much lower in Northern Ireland than in the UK generally. The 2021 Cyber Security Breaches Survey[3] notes that 27% of micro firms and 53% of small firms have a formal policy covering cyber security risks.

Of those who have a plan the frequency with which it is tested varies. The most popular is to test the incident plan annually. However, one-fifth (19%) don't know how often the plan is tested.

Figure 5: Frequency of testing the cyber security plan



Base: All who have a documented cyber incident plan (77)

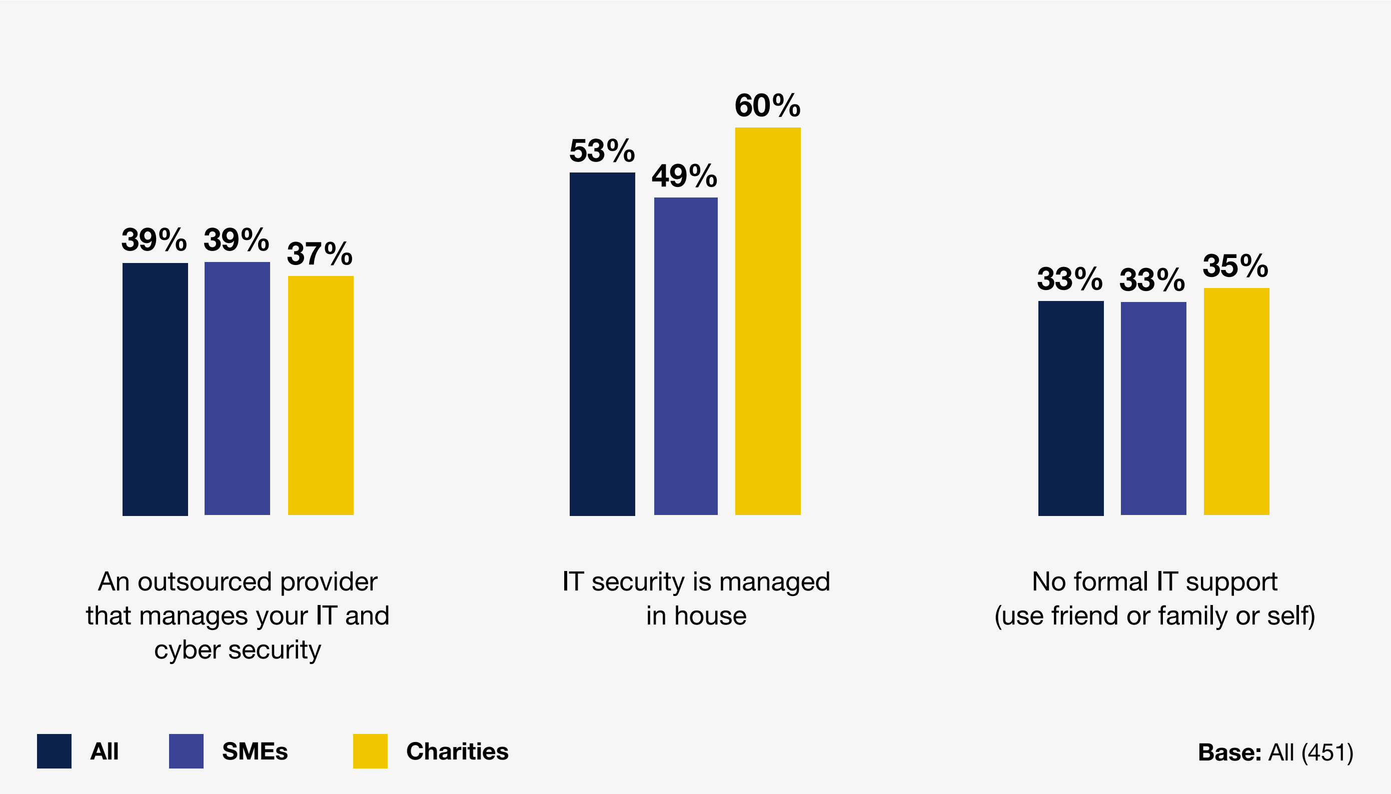
[3] Department for Digital, Culture, Media and Sport 26 Cyber Security Breaches Survey. Ipsos MORI 2021

Management of and Support for IT and Cyber Security

Organisations have a range of ways to manage their IT and cyber support arrangements and that is either internally, by outsourcing or some have informal IT support. For those who have informal mechanisms that is because they are doing it themselves or using family or friends to help support them in this area of their back-office functions. Furthermore, some are using a combination of these, so none are mutually exclusive.

Around half (53%) of all organisations manage at least some of their IT security in-house and almost four in ten manage their IT security via an external, outsourced organisation (39%) or through informal channels (34%). Whilst there are no significant differences between SMEs and charities, charities were more likely to report that IT and cyber security was managed in-house than SMEs (60% compared to 49%).

Figure 6: Management of IT and cyber security



Base: All (451)

Cyber Governance Summary

- Half of all organisations (48%) agree that their organisation lists cyber as a board level risk.

- The majority of organisations (62%) have done nothing in the past 12 months to identify cyber security risks to their organisation.

- Very few organisations adhere to or have cyber security standards or accreditations. PCI DSS is an exception to this (14%) with SMEs being more likely to have this compared to charities.

- Nearly one in four organisations have taken action to identify cyber security risks. The most likely actions are to use specific tools designed for security monitoring, such as Intrusion Detection Systems or they have conducted a risk assessment covering cyber security risks.

- Of those who conducted a cyber security vulnerability audit (9%), this was conducted by a mix of internal staff, external contractors or both. Charities are more likely to use only internal staff whereas, SMEs are more likely to use external contractors.

- A minority (17%) of organisations have a documented incident plan and are most likely to test it annually.

- Organisations use a combination of internal, outsourced and informal assistance to manage their IT and cyber support arrangements. They are most likely to primarily manage it internally.

5 Cyber Security Controls

This chapter of the report examines current cyber security processes and procedures. This centres on the following:

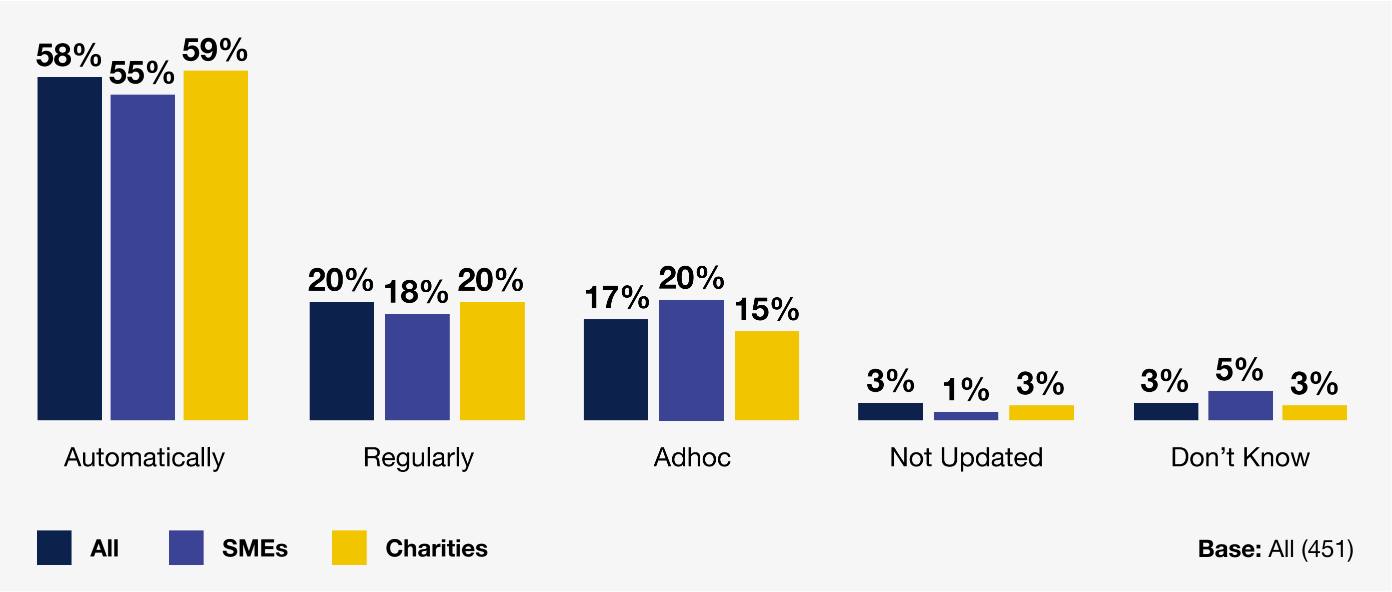
- **Updating** systems and software;
- **Confidence** about the secure configuration of systems;
- **Training** in cyber security;
- **Policy** controls; and
- **Understanding** of specific cyber threats.

Updating Systems and Software

5.1.1 Operating Systems (e.g. windows, IOS)

The majority of organisations report that their operating systems (e.g., Windows, IOS) update automatically and there is no difference between SMEs and charities. One-fifth update these systems regularly and a similar proportion update in an ad hoc manner and only a few (3%) report that their systems are not updated.

Figure 7: Updating Operating Systems (e.g., windows, IOS)



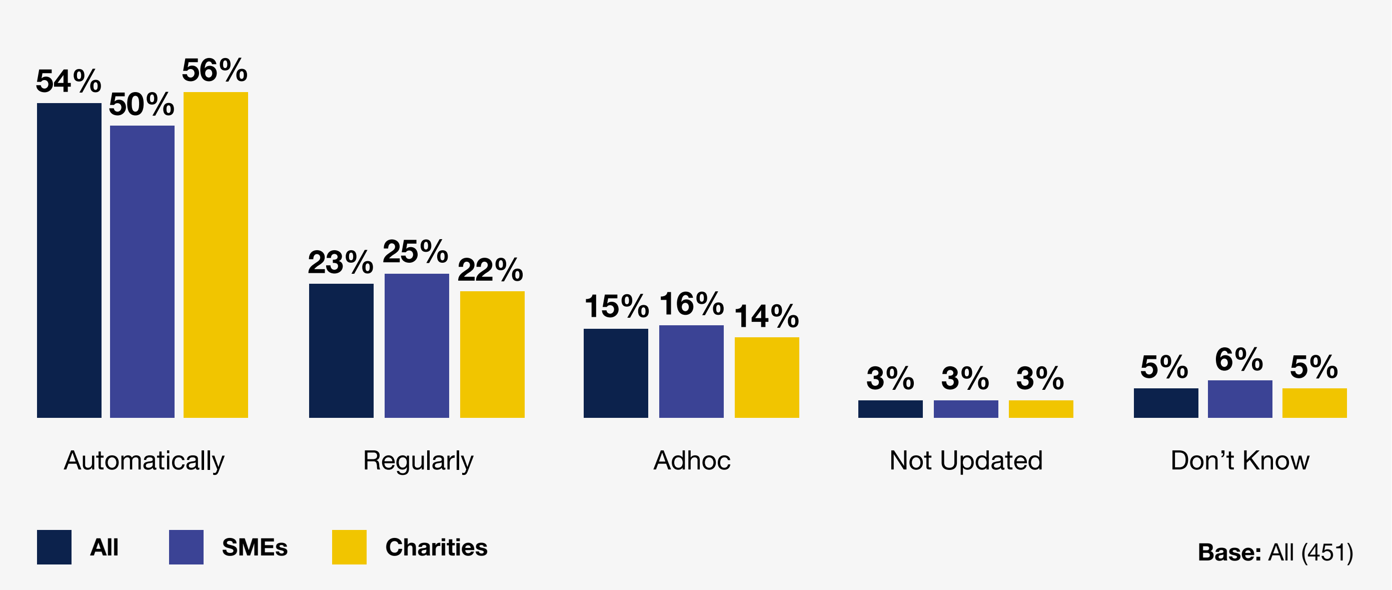
Base: All (451)

5.1.2 Anti-virus or malware software

Again, the majority of organisations update their anti-virus or malware software automatically or as a minimum regularly.

A smaller proportion do this on an ad hoc basis and only a very small proportion do not update their anti-virus or, malware software (similar to the operating systems).

Figure 8: Updating anti-virus or malware software



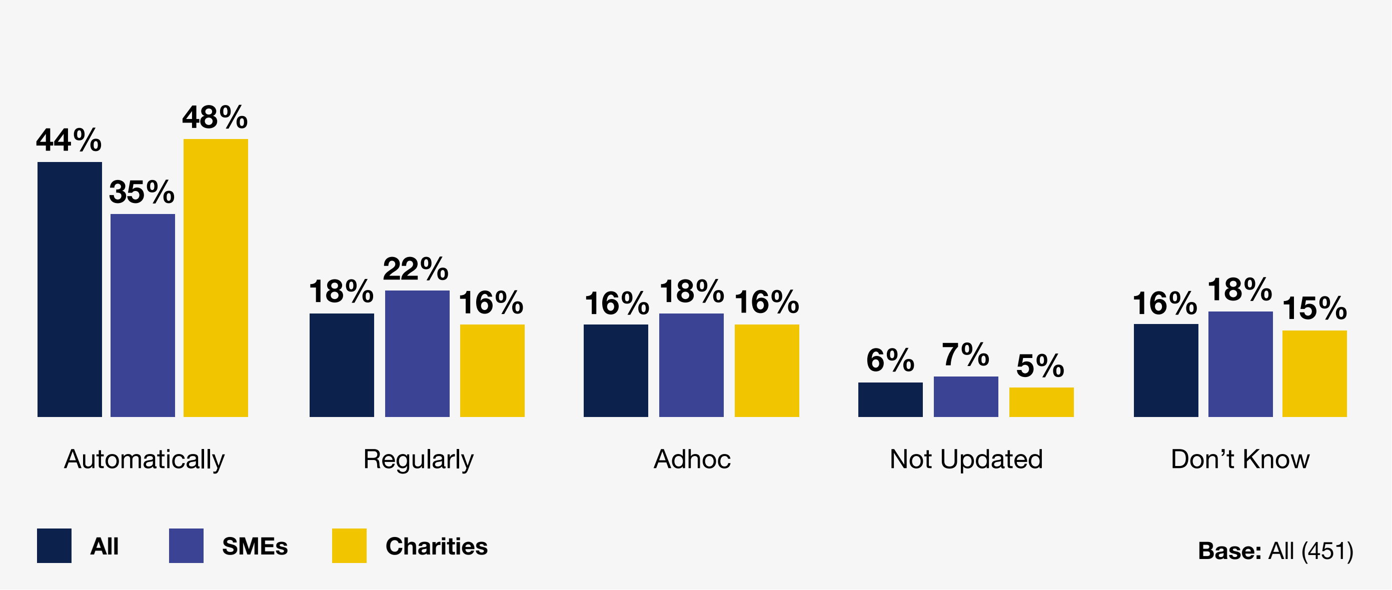
Again, there is no significant difference between SMEs and charities in terms of updating their anti-virus and malware software.

5.1.3 Other applications

There is some variation in terms of updating other applications compared to the automation with which the operating system or anti-virus and malware are updated. These applications are less likely to be updated automatically and a higher proportion update them on an ad hoc basis compared to updating operating systems or anti-virus and malware software.

Although still small, a slightly higher proportion (6%) do not update other applications compared to updating operating systems or anti-virus and malware software. A greater proportion of respondents also did not know if their other applications were updated compared to their operating systems or, anti-virus and malware software (16%, 3% and 5% respectively). There is no difference between SMEs and charities.

Figure 9: Updating other applications

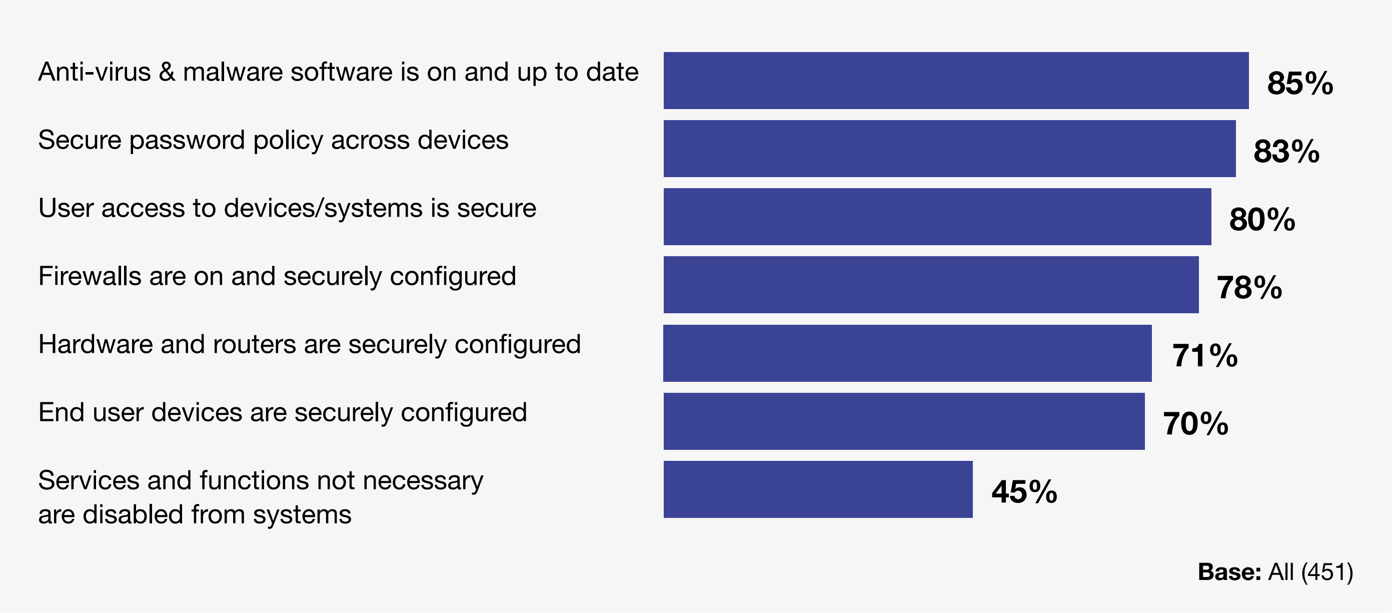


Base: All (451)

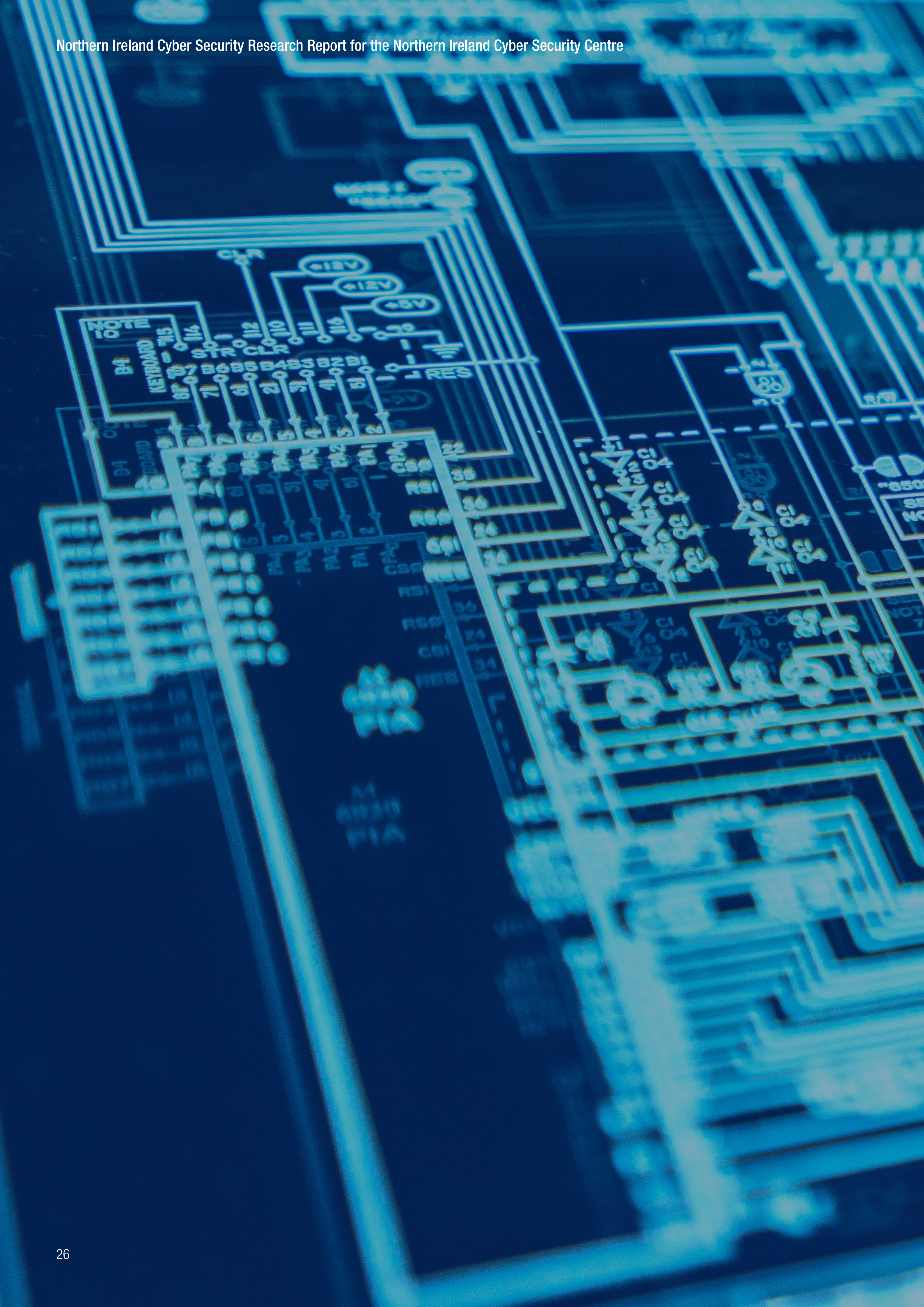
Confidence About the Secure Configuration of Systems

At least eight in ten participants are confident about the secure configuration of anti-virus and malware software, secure passwords, user access to devices/systems and firewalls. There is slightly less confidence about hardware, routers and end user devices.

Figure 10: Confidence in the secure configuration of systems



Base: All (451)


CLR
+12V
+12V
+5V
NOTE
IO
B4
KEYBOARD
STR
CLR
B7 B6 B5 B4 B3 B2 B1
RES
CS0
RS1
RS0
CS1
A1
6820
PIA
R/W

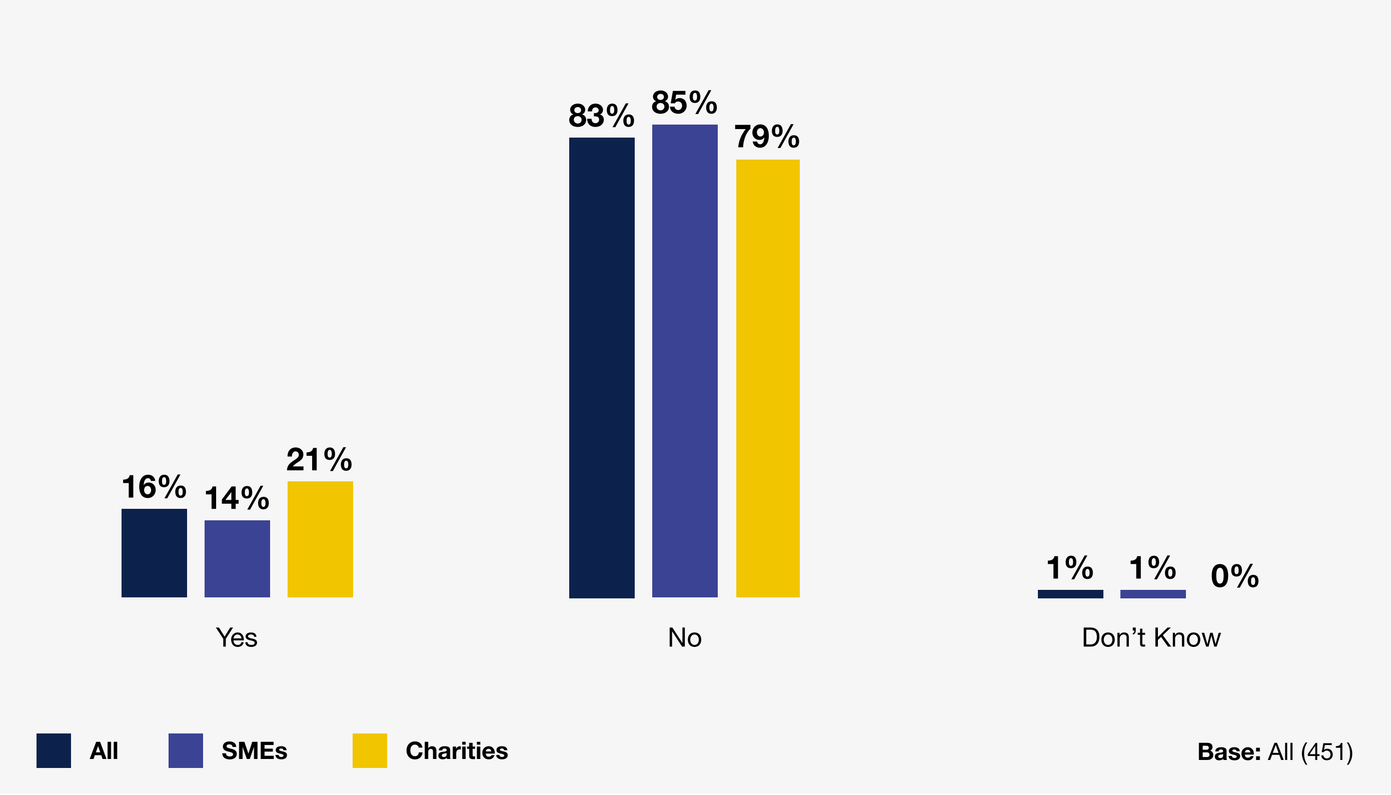
Finally, there is much less confidence around the secure configuration of services and functions which are not necessary being disabled from systems.

These findings are very similar to the results from the UK study which found that 83% of businesses and 69% of charities have up to date malware protection and similar proportions (79% and 57% respectively) have a policy to ensure users set strong passwords.

Training in Cyber Security

Few organisations (16%) report that they carried out any cyber security training or awareness raising sessions specifically for staff or volunteers who are not directly involved in cyber security. However, charities are slightly more likely to report that they have carried out cyber security training or awareness raising sessions compared to SMEs.

Figure 11: Cyber security training and awareness raising sessions



Base: All (451)

These findings are comparable to the 2021 UK study which found that 14% of businesses and 18% of charities had provided staff with training or awareness raising session on cyber security in the past 12 months.

Policy Controls

The table details the proportion of rules or controls, if any, which organisation have in place, do not have in place or plan to have in place in the next six months.

Table 5.1: Rules or controls in place

	Yes, have in place %	No, Not in place %	Planning to have in place within 6 months %	Don't know if I have it in place %
Up-to-date malware/anti-virus protection	81	14	1	4
Restricting IT admin and access rights to specific users	76	20	1	3
A password policy that ensures users set strong passwords	74	23	2	2
Security controls on company-owned devices (e.g. laptops)	65	28	2	5
Firewalls that cover your entire IT network, as well as individual devices	60	26	2	13
Backing up data securely via a cloud service	60	34	2	5
Backing up data securely via other means	66	28	1	5
Only allowing access via company-owned devices	64	32	1	3
An agreed process for staff to follow when they identify a fraudulent email or malicious website	55	40	2	3
Specific rules for storing and moving personal data files securely	53	41	1	5
A policy to apply software security updates within 14 days	38	49	2	12
Separate Wi-Fi networks for staff and for visitors	30	67	2	2
Any monitoring of user activity	28	66	2	4
A virtual private network (VPN) for staff connecting remotely	25	70	1	4

Overall, organisations appear to have very few, if any, plans in the next six months to put in place any of the rules or controls that they currently don't have. Either they have the rule or control, or they do not, with few planning to implement these and some who do not know if they have it in place.

Most organisations have rules or controls in place for up-to-date malware/anti-virus protection (81%), 14% don't have this and only 1% have a plan to implement in the next six months. Charities were much less likely to report up to date malware/anti-virus protection than SMEs (26% compared to 55%). While most organisations have rules or controls in place for up-to-date malware/ anti-virus protection and just over three-quarters (76%) have rules and controls in place for restricting IT admin and access rights to specific users. Again, charities were much less likely to restrict IT admin and access rights to specific users than SMEs (26% compared to 50%). Almost three quarters of all organisations have a password policy in place that ensures users set strong passwords (74%). Those who do not have this policy in place have very little plans to implement it in the next six months (2%). As with other rules and controls charities were much less likely to have a strong password policy than SMEs (23% compared to 50%).

The rules and controls that organisations are least likely to have are: separate Wi-Fi networks for staff and for visitors (30%); any monitoring of user activity (28%); and a virtual private network (VPN) for staff connecting remotely (25%). The majority of those who do not have these rules or controls in place have little or no plan to implement them in the next six months.

Understanding of Specific Cyber Threats

Understanding of specific cyber threats varies depending on the threat. Almost all organisations have heard of and had some knowledge of Phishing. However, more SMEs report that they have never heard of Phishing compared to charities. More than half of organisations report that that they have never heard of social engineering attacks (53%) and more SMES have never heard of this threat (56%) compared to charities (49%). Half of all organisations (49%) were completely unaware of denial of service (DOS) and just under half were unaware of supply chain attacks. Charities appear to be more knowledgeable than SMEs with regard to some specific threats. However, that could be a function of the business type or the person interviewed in the charity maybe solely responsible for cyber security. In an SME, a senior person may have a number of roles, one of which is cyber security and hence, they are not an expert.

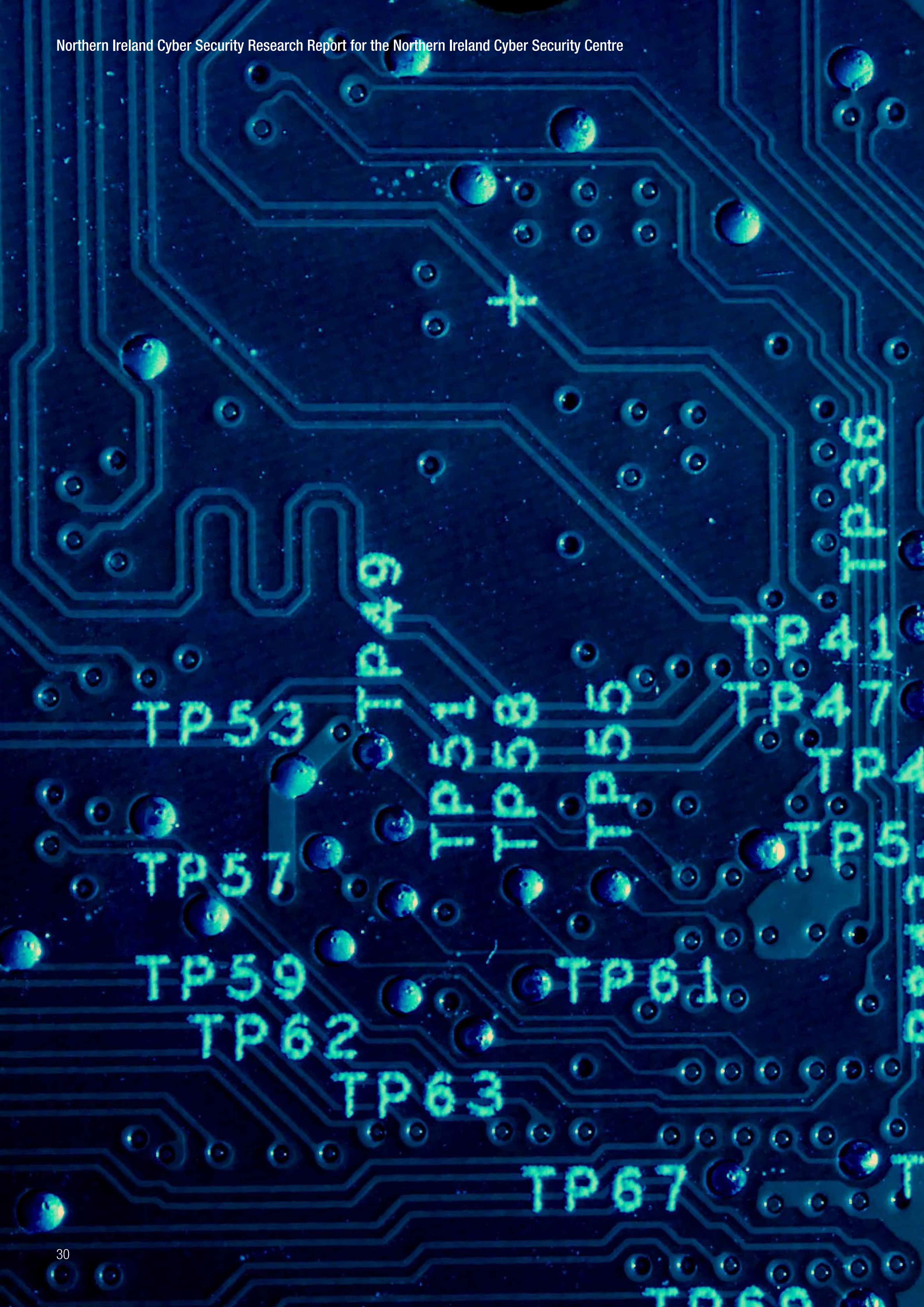
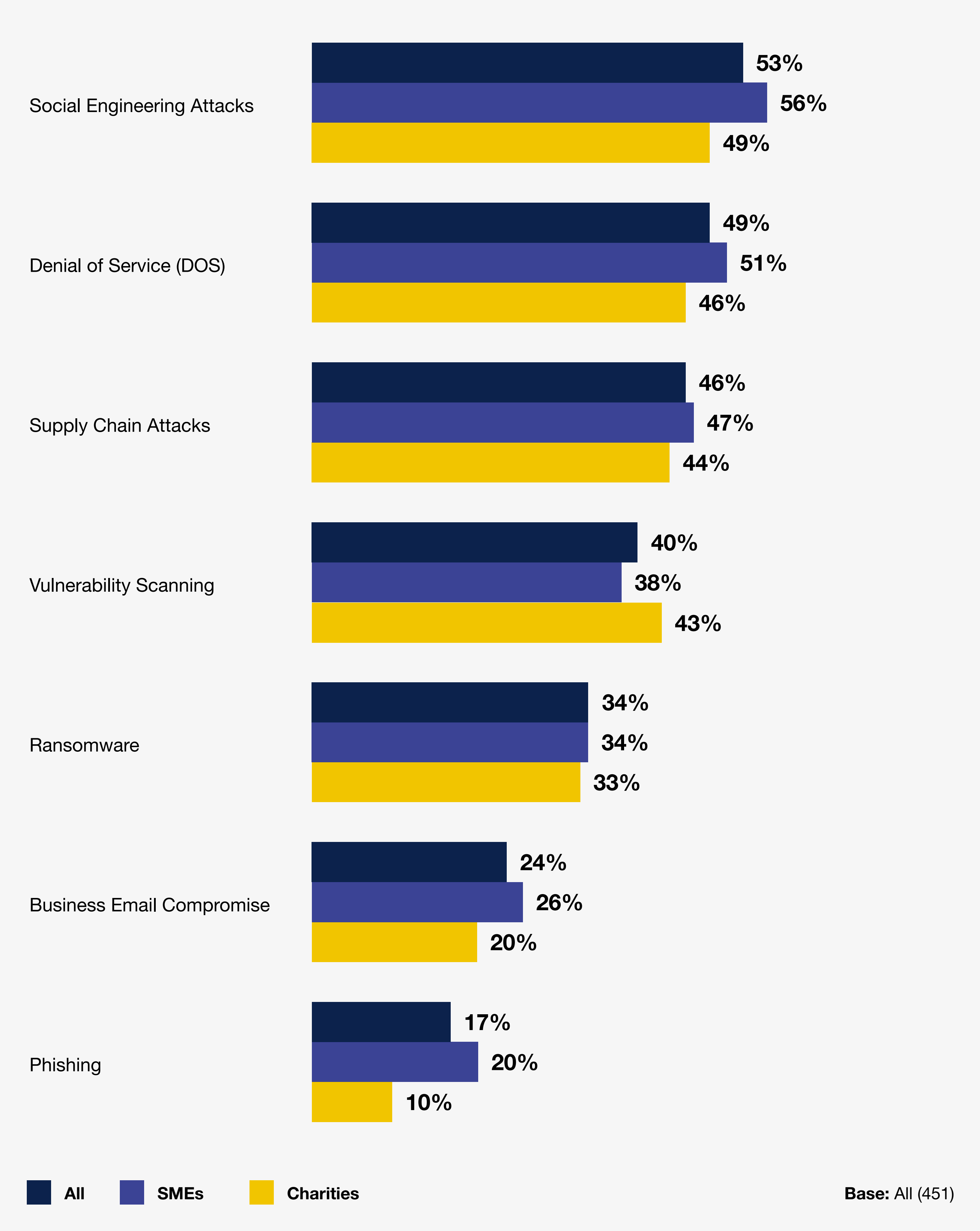

TP36
TP49
TP41
TP53
TP51
TP58
TP55
TP47
TP4
TP57
TP5
TP59
TP61
TP62
TP63
TP67

Figure 12: Never heard of specific cyber threats



Base: All (451)

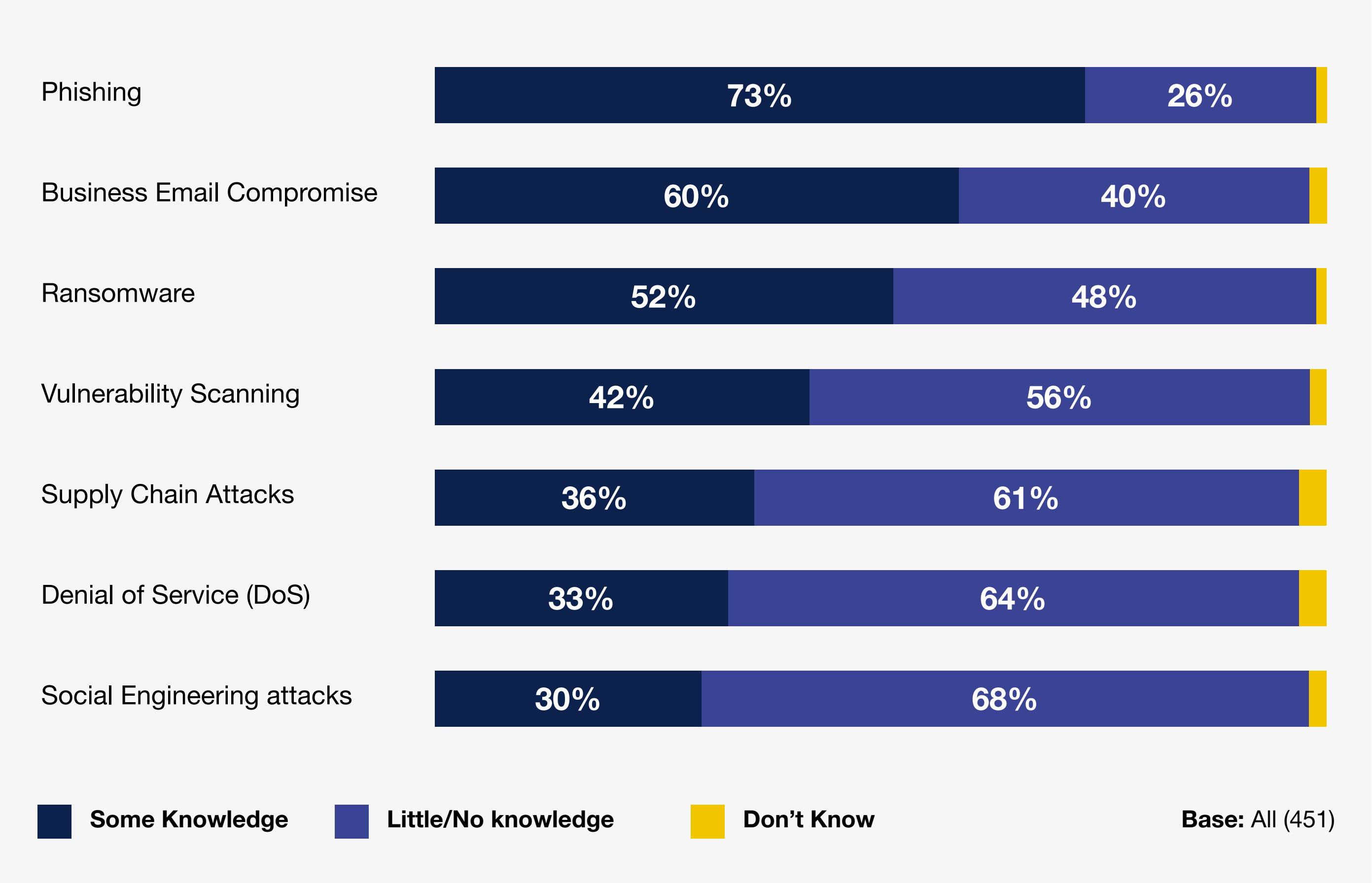
Few organisations have full understanding and knowledge of all these specific cyber threats.

Table 5.2: Understanding of specific cyber threats

	Never heard/no understanding	Little knowledge/no understanding	Some understanding & knowledge	Good understanding & knowledge	Full understanding & knowledge	Don't know
Social Engineering Attacks	53%	13%	16%	8%	8%	2%
Denial of Service (DOS)	49%	13%	16%	10%	10%	2%
Supply Chain Attacks	46%	17%	18%	8%	8%	3%
Vulnerability Scanning	40%	14%	20%	15%	10%	2%
Ransomware	34%	14%	16%	18%	18%	2%
Business Email Compromise	24%	15%	25%	16%	16%	2%
Phishing	17%	11%	24%	21%	27%	1%

Despite a relatively low proportion of organisations (17%) reporting that they have never heard of Phishing, there are varying degrees of knowledge about this term. Just over a quarter (27%) report that they have full knowledge and understanding of the term and 21% have a good understanding of Phishing. Nearly three quarters of organisations have some knowledge of Phishing whereas only three in ten (30%) have some knowledge of Social Engineering Attacks.

Figure 13: Understanding of specific cyber threats



Cyber Security Controls Summary

- The majority of organisations report that their operating systems (e.g. windows, IOS) and their anti-virus or malware software update automatically and there is no difference between SMEs and charities. Other applications are less likely to be updated automatically and a higher proportion update them on an ad hoc basis.

- At least eight in ten participants are confident about the secure configuration of anti-virus and malware software, secure passwords, user access to devices/systems and firewalls. There is slightly less confidence about hardware, routers and end user devices.

- Few organisations report that they carried out any cyber security training or awareness raising sessions specifically for staff or staff/volunteers who are not directly involved in cyber security. Charities are slightly more likely to have done this.

- Most organisations have rules or controls in place for up-to-date malware/anti-virus protection, restricting IT admin and access rights to specific users and users setting strong passwords.

- Understanding of specific cyber threats varies depending on the threat. Almost all organisations have heard of and had some knowledge of Phishing. Over half have never heard of social engineering attacks and denial of service (DOS). Few organisations have full understanding and knowledge of all specific cyber threats.

6 Cyber Incidents

This chapter of the report examines the prevalence and outcome of any cyber incidents experienced by the organisations. This centres on the following:

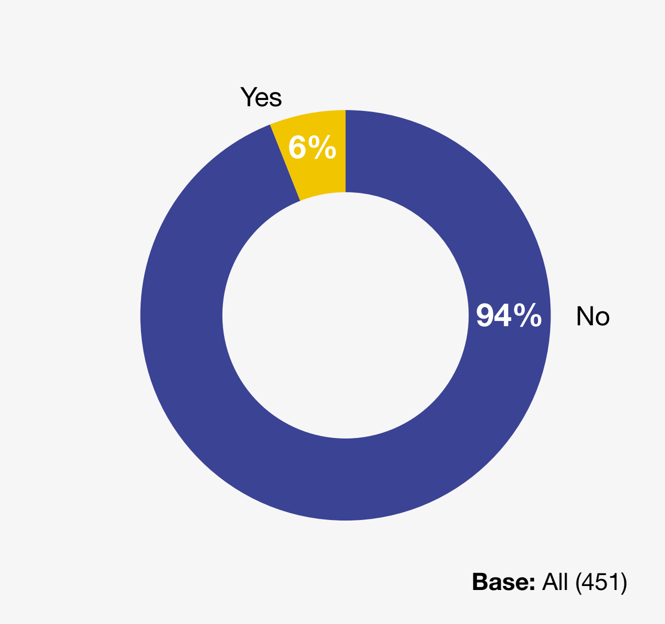
- **Prevalence** of cyber incidents;
- **Nature** and type of incident; and
- **Recovery** from the incident.

Prevalence of Cyber Incidents

6.1.1 Experienced a cyber attack

Only a very small proportion (6%) of organisations have experienced a cyber incident in the last 12 months. There is no difference between SMEs and charities in terms of prevalence of cyber incidents.

Figure 14: Cyber incident in the last 12 months.



Base: All (451)

The proportion of organisations who reported that they had experienced a cyber incident in the past 12 months is much lower than those reported in the UK. The 2021 UK study found that 37% of micro firms, 39% of small firms and 26% of charities had identified a breach or attack in the last 12 months.

Nature and Type of Incident

Of those who did experience cyber incidents the majority only recall one incident. One charity and one SME recalled three incidents and another charity recalled seven, while another recalled 12 incidents. Despite few incidents being reported, they have been varied and mostly focused at charities. The following table outlines the number and type of cyber incidents.

There is no difference in the number of incidents between charities and SMEs.

Table 6.1: Type and number of cyber incidents

Cyber attack	Charity	SME
Hacking or attempted hacking of online bank accounts	1	1
People impersonating your organisation in emails and online	2	0
Phishing attacks	2	6
Unauthorised accessing of files and networks by people outside your organisation	1	0
Business Email Compromise	1	3
Ransomware	2	1
Denial of Service	0	2
Takeovers (or attempts) of websites, social media accounts or email accounts	0	1
Other answers:		
Phone hacked and tried to order equipment from your phone provider	0	1
Hacked into head office, shut down the intranet, as a result, there was limited service at an operational level	0	1
Supplier email intercepted	1	0
Malware	0	1

Recovery from the Incident

The majority of organisations report that they were able to recover from the incidents which they experienced. One charity and one SME reported that they were not able to recover, and one charity and one SME only partially recovered. In order to recover from the attack, the majority of organisations required help or support to deal with the effect of the attack. Organisations use a variety of assistance including banks, local computer centre, anti-fraud agency, independent IT person, external cyber expert, an investigator, the phone company and local private computer consultancy.

As a result of these cyber attacks organisations report a number of outcomes. The most frequent mentioned is temporary loss of access to files or networks and then the website, applications or online services being taken down or made slower. The order they occurred by frequency are listed below:

1. Website, applications or online services were taken down or made slower;
2. Temporary loss of access to files or networks;
3. Compromised accounts or systems used for illicit purposes (e.g. launching attacks);
4. Software or systems were corrupted or damaged;
5. Personal data was altered, destroyed or taken;
6. Permanent loss of files (other than personal data);
7. Money was stolen;
8. Lost access to any third-party services you rely on;
9. Physical devices or equipment were damaged or corrupted;
10. Data loss;
11. Email intercepted; and
12. Nothing happened.

Cyber Incidents Summary

- Only a very small proportion (6%) of organisations reported that they experienced a cyber incident in the last 12 months. This was much less than the UK study in which 37% of micro business reported that they had experienced a cyber security breach of attack.

- Of those who did experience cyber incidents the majority only recall one incident. Phishing attacks were the most prevalent.

- The majority of organisations report that they were able to recover from the incidents which they experienced.

- Organisations use a variety of assistance to help them recover.

- The most frequent outcome from the attacks is temporary loss of access to files or networks.

7 Barriers and Services

This section of the report details the barriers to implementing good or better cyber security. The focus of this section is two-fold: what makes it difficult to manage any cyber security risks in their organisation or supply chain or partners; and what value they put on a range of services to protect their organisation.

- **Barriers** to implementing good cyber security; and
- **Value** of a range of services to protect the organisation.

Barriers to Implementing Good Cyber Security

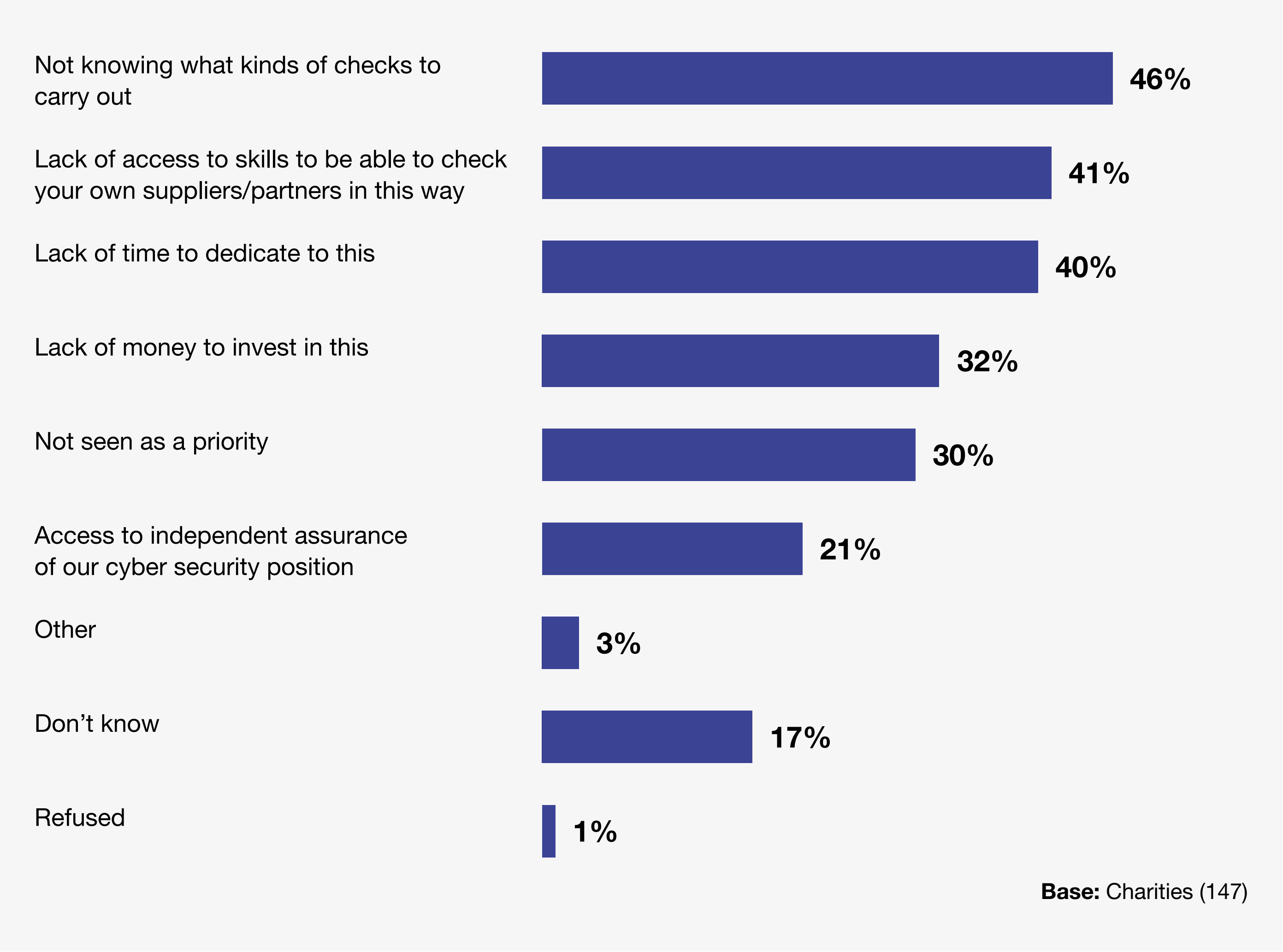
The main barriers that organisations face when managing any cyber security risks in their organisation or with their supply chain or partners is not knowing what kind of checks to carry out, lack of access to skills to be able to check suppliers/partners and lack of time to dedicate to this.

Charities are more likely to suggest that lack of money to invest is a barrier compared to SMEs. Just over a quarter of organisations report that cyber security is not seen as a priority in their organisation. Almost one fifth (17%) do not know what the barriers are in their organisation to implementing good cyber security. All of this suggests that lack of awareness and training of good cyber security is prevalent within these organisations and there is little difference between SMEs and charities.

Value of a Range of Services to Protect the Organisation

Four in ten of all organisations (41%) had no interest in certification of the organisation’s security (similar to council hygiene rating schemes) but one quarter of organisations (24%) would pay up to £500 for this certification. However, almost four in ten organisations (38%) would pay up to £500 for staff training and awareness whilst one quarter (26%) had no interest in staff training and awareness.

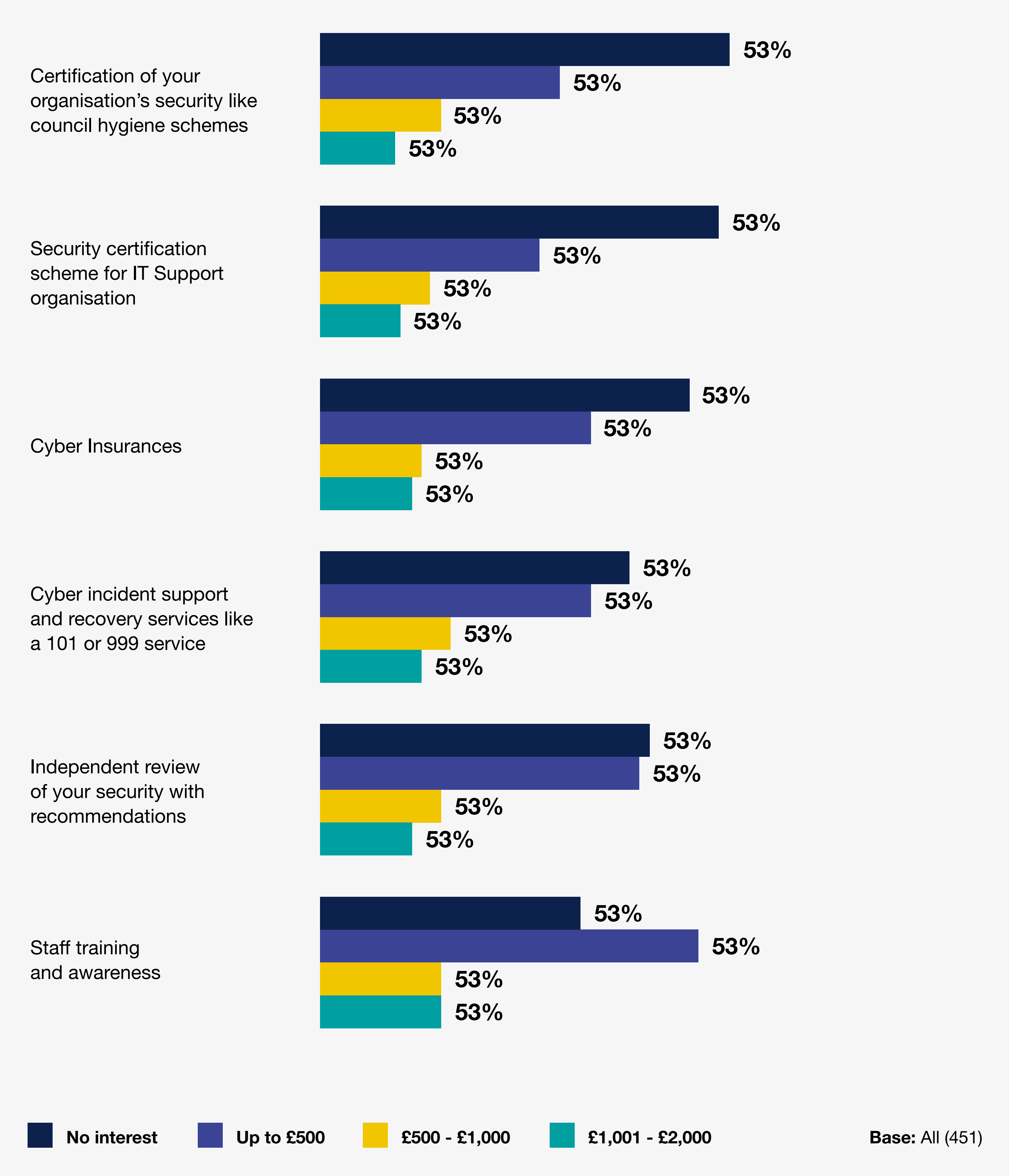
Figure 15: Barrier to implementing good cyber security



Base: Charities (147)

With regard to staff training and awareness charities (17%) were less likely than SMEs (31%) to say that they had no interest in this service. Almost half of charities (46%) were willing to pay up to £500 compared to one third of SMEs (33%).

Figure 16: Value of a range of services to protect the organisation



Base: All (451)

Barriers and Services Summary

- The main barriers that organisations face when managing any cyber security risks in their organisation or with their supply chain or partners is not knowing what kind of checks to carry out, lack of access to skills to be able to check suppliers/partners and lack of time to dedicate to this.

- Organisations were least likely to pay for certification of the organisation's security like council hygiene schemes but over a third (38%) of organisations would pay up to £500 for staff training and awareness.

8 Conclusions

This is the first study of cyber security amongst businesses and charities in Northern Ireland.

Unlike other, similar UK studies, it focused on SMEs, which is more reflective of economic demographics in Northern Ireland. It should also be noted that the fieldwork for this study took place during the COVID-19 pandemic, during which time many businesses were closed due to a national lockdown and those that remained open were operating in exceptional circumstances, meaning that business and charities may have been more focused on short term business goals than would normally be the case.

A number of common themes emerged from the survey results firstly, there were no significant differences between SMEs and Voluntary and Community Organisations in their level of understanding of cyber security and the extent to which they have implemented actions and policies to be more secure. The majority of organisations (62%) has not undertaken any actions within the past 12 months to identify cyber security risks. Despite this, almost half (48%) of organisations interviewed had cyber security listed as a board level risk.

Whilst there are a range of government supported accreditation schemes relating to cyber security there appeared to low levels of awareness of or, adherence to them. Low levels of adherence to standards and accreditations were also noted in the UK Cyber Security Breaches Survey (2021)[4], therefore this is not just a Northern Ireland phenomenon. This would suggest that the NICSC could promote government supported schemes further. Given that cost and lack of understanding were noted as barriers to implementing cyber security amongst organisations in NI costs, the benefits of these schemes should be highlighted. Another UK study[5] noted that businesses require jargon free information to make schemes such as Cyber Essentials more accessible to non-IT experts. This is also something to be aware of when promoting cyber security activities

[4] Department for Digital, Culture, Media and Sport 1 Cyber Security Breaches Survey 2021: Ipsos MORI.

[5] DCMS Cyber Essentials Scheme – process evaluation and message testing. TNS 2016

to SMEs and Voluntary and Community Organisations in Northern Ireland.

The most common barrier that organisations reported in managing their cyber security risk was a lack of knowledge. This is consistent with the finding that around half of the organisations interviewed had never heard of a number of common cyber security threats (such as Social Engineering Attacks, Denial of Service and Supply Chain Attacks). The NICSC may wish to consider working with sectoral representative groups such as the Federation of Small Businesses (FSB) and the Northern Ireland Council on Voluntary Action (NICVA) to increase digital literacy, raise awareness of the potential cyber security threats to their organisations and to sign-post organisations to sources of support and advice.

A very small proportion (6%) of organisations reported any cyber security incidents within the last 12 months. Given that other studies have noted incident rates of between 65%[6] and 39%[7] for SMEs, this could suggest that there may be a lack of awareness of cyber security threats amongst organisations in Northern Ireland. Another study on Cyber Security in SMEs[8] noted that SMEs often do not have the resources to identify or protect themselves against cyber threats, meaning that *"threats can go unnoticed, investigated or, ignored"*. This is consistent with the relatively low levels of understanding of common threats amongst SMEs and V&CO in Northern Ireland. Further research would be required to fully understand how SMEs and V&CO in Northern Ireland perceive the level of cyber security threats to their organisation.

Of the cyber attacks that were reported, most common were Phishing (or attempted) attacks. The majority of organisations reported that they successfully recovered from the incident. This may be why many organisations reported that they had no interest in services that could help to protect their cyber security (such as security certification schemes). The one area with the most interest amongst organisations was staff training, as more than half of organisations noted that they would pay for staff training. This could suggest that the training should be focused on how to reduce human exposure to threats. The NICSC may wish to engage with local providers of cyber security solutions to gauge the current level of demand and appetite for their services amongst SMEs and V&CO and to assess if these firms are interested in becoming providers of cyber security training, advice and accreditation.

Whilst the number of reported cyber security incidents was low, levels of knowledge and existence of policies relating to cyber security were also low. This suggests that there are several areas where organisations could potentially take more action, such as:

[6] Cyber Security Attacks and Threats. Towergate (2020)

[7] Department for Digital, Culture, Media and Sport 1 Cyber Security Breaches Survey 2021: Ipsos MORI.

[8] 'The state of cyber security - SME report 2019'. Senseon (2019).

- Investing in basic, outsourced cyber security provision;
- Moving away from legacy systems (e.g. Exchange, Windows XP/7, etc.);
- Implementation of basic administrative rights, systems updates etc; and
- The introduction of firewalls.

Given the relatively low levels of awareness and knowledge of cyber security issues across SMEs and charities in Northern Ireland, the NICSC may wish to consider having tailored events to:

- Raise awareness of the range of threats to cyber security for organisations in Northern Ireland;
- Provide basic, non-technical guidance on effective cyber security; and
- Highlight the organisational benefits of investing in systems and processes to improve cyber security.

It may be most beneficial if these are arranged on a sectoral basis, so that comparable companies can get the most useful experience from these and can share learning and experiences.

Our standards and accreditation

Ipsos MORI's standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a "right first time" approach throughout our organisation.

ISO 20252

This is the international market research specific standard that supersedes BS 7911/MRQSA and incorporates IQCS (Interviewer Quality Control Scheme). It covers the five stages of a Market Research project. Ipsos MORI was the first company in the world to gain this accreditation.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos MORI endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation. We were the first company to sign up to the requirements and self-regulation of the MRS Code. More than 350 companies have followed our lead.

ISO 9001

This is the international general company standard with a focus on continual improvement through quality management systems. In 1994, we became one of the early adopters of the ISO 9001 business standard.

ISO 27001

This is the international standard for information security, designed to ensure the selection of adequate and proportionate security controls. Ipsos MORI was the first research company in the UK to be awarded this in August 2008.

The UK General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 2018

Ipsos MORI is required to comply with the UK GDPR and the UK DPA. It covers the processing of personal data and the protection of privacy.

HMG Cyber Essentials

This is a government-backed scheme and a key deliverable of the UK's National Cyber Security Programme. Ipsos MORI was assessment-validated for Cyber Essentials certification in 2016. Cyber Essentials defines a set of controls which, when properly implemented, provide organisations with basic protection from the most prevalent forms of threat coming from the internet.

Fair Data

Ipsos MORI is signed up as a "Fair Data" company, agreeing to adhere to 10 core principles. The principles support and complement other standards such as ISOs, and the requirements of Data Protection legislation.

For more information

Ipsos MORI
3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

ipsos-mori.com
twitter.com/IpsosMORI

About Ipsos MORI Public Affairs

Ipsos MORI Public Affairs works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.

NI Cyber Security Centre

Working to create a cyber safe,
secure and resilient Northern Ireland

NI Cyber Security Centre
ECIT, Catalyst
Queens Road
Belfast, BT3 9DT

Email: info@nicybersecuritycentre.gov.uk
Web: www.nicybersecuritycentre.gov.uk
Twitter: @NICyberSC

Ipsos MORI