Department for Digital, Culture Media & Sport

Ipsos MORI Social Research Institute

August 2017

Cyber security among charities

Findings from qualitative research

Dr Rebecca Klahr, Jayesh Navin Shah, Kelly Finnerty, Krishna Chhatralia and Tom Rossington

Contents

Summary

This summary covers the findings from qualitative research with UK registered charities exploring awareness, attitudes and experiences around cyber security. A total of 30 in-depth interviews were undertaken in February and March 2017 with a range of charities by income, location and charitable area. The research was commissioned by Department for Digital, Culture, Media and Sport (DCMS) as part of the National Cyber Security Programme and carried out by Ipsos MORI.

Awareness and attitudes

Pre-existing awareness and knowledge around cyber security varied considerably across the charities interviewed. Those in charge of cyber security, especially in smaller organisations, did not feel well informed about the topic, and several noted that they had not seriously considered it before or proactively sought out any information, often leaving it to an outsourced IT provider to deal with.

In this context, there was often a low awareness of the Government support available on cyber security. This was despite the fact that the Government and other public bodies were considered as trustworthy sources of information. Some participants assumed that if the issue was important enough for them to address, they would hear about it through their established communication channels, via the Charity Commission or voluntary support bodies, such as NCVO.

In some cases, participants assumed cyber security was more of an issue for businesses than for charities. These participant assumed that businesses would be more at risk as they would be more likely to hold customers' financial details and generally be expected to have more cash in the bank.

On the other hand, there were several instances where charities recognised the relevance of cyber security for their organisations, and this prioritisation of the issue could be traced to many things:

- holding personal data on donors or service users
- having trustees or staff with private sector experience of the issue
- meeting the standards laid out by commissioning organisations (in cases where charities were involved in Government service provision).

Approaches to cyber security

Across the charities interviewed, it was typically the case that organisations did not have internal specialist staff with the technical skills to cover cyber security. Responsibility for cyber security internally was often held by someone with a different core role, or with multiple responsibilities, such as Chief Executives or finance staff. Competing demands on time and resources – with greater focus often given to areas such as fundraising and delivery – meant that cyber security was often deprioritised and could lack investment. As a result, there was often a reliance on outsourced IT providers, as well as informal sources of support such as friends, family or other local charities.

Various participants highlighted that more could be done to raise basic awareness of cyber security among staff and trustees. However, it was uncommon to find charities that had provided cyber security

training to any of their staff or volunteers. This reflected the various barriers that charities faced to providing training. Many assumed training would be expensive, and did not prioritise spending on training above other areas that might need funding, such as IT equipment upgrades. Charities also lacked the expertise to put on training by themselves – those that had done so had typically worked with outsourced providers to run training. Smaller charities also found training hard in general given that many of their trustees and staff tended to work remotely. In this context, some were interested in free or low-cost online training options.

Cyber insurance was similarly often seen as too expensive to consider. Some charities noted that they had wider insurance policies such as public liability insurance or business continuity insurance, but were not clear on whether these would cover them in the result of a cyber attack.

Perceptions and experiences of breaches

Charities were often highly concerned with potential loss of funds or of personal data on donors or service users, and these were typically seen as existential threats that helped heighten the importance of being cyber secure. By contrast, the loss of day-to-day (non-personal data) files was less of a concern, with some charities not realising the potential implications for business continuity from losing non-personal data.

Indeed, the research came across examples of charities that had incurred cyber security breaches where non-personal data were lost, and where organisations spent considerable time getting their data restored. There were also examples where charities had incurred a sizable financial cost from a cyber security breach. In these cases, it is worth noting that the experiences of breaches often spurred charities into taking action and protecting themselves against further attacks.

Finally, the research also explored reporting of cyber security breaches. While participants were confident that they would report serious breaches with a financial impact internally to trustees and to any outsourced IT providers, they were less certain of where and when they might be required to report breaches outside of this. Some mentioned reporting breaches with a financial impact to organisations such as the Information Commissioner's Office (highlighting again the importance placed on data protection). However, none of those interviewed had heard of the cyber crime body, Action Fraud.

Conclusions

This research has highlighted that charities often see cyber security as important, and are as susceptible to indiscriminate cyber attacks as businesses. These attacks can have serious implications for charity finances and for business or organisational continuity. However, the research also flags the many barriers that charities face when it comes to engaging with the issue, including competing priorities for time and resources, and staff not necessarily equipped with the knowledge and skills to deal with the issue.

There is a need for basic awareness raising among staff and trustees, and upskilling of those responsible for cyber security – so they know the basic technical controls they can put in place. It may also help to disseminate Government information and support via the organisations with which charities already have established relationships, such as the Charity Commission. Finally, making use of private sector expertise among trustees may also help individuals within charities to champion the issue.

1 Introduction

1.1 Background and research aims

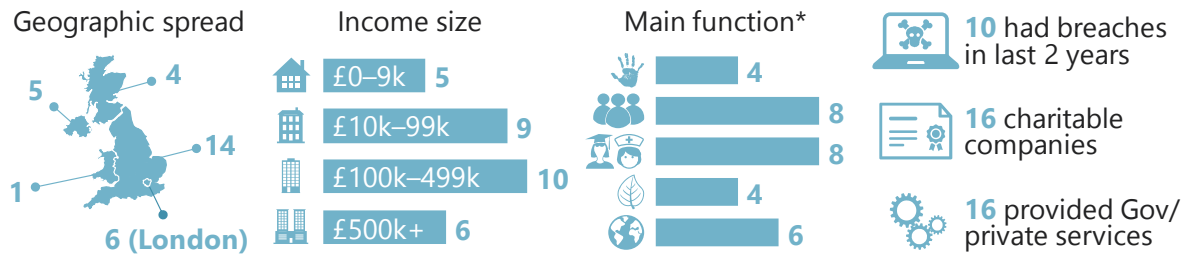
This report covers qualitative research by Ipsos MORI with UK charities on awareness and approaches around cyber security. The Department for Digital, Culture, Media and Sport (DCMS) commissioned the research as part of the National Cyber Security Programme, following a wider quantitative and qualitative survey with businesses published in April 2017.[1]

Cyber security is an important issue for the UK economy. The Cyber Security Breaches Survey 2017 found that three-quarters of UK *businesses* rate cyber security as a high priority for their senior management. However, the awareness and attitudes of charities towards this topic are relatively unknown. This research aims to explore charities' awareness, understanding and approaches to cyber security, and their experiences of cyber security breaches or attacks. It will also aim to draw out whether there are any indicative differences between charities and businesses in how they view and manage cyber security, by making broad comparisons to the qualitative findings in the Cyber Security Breaches Survey 2017.

1.2 Methodology

Since this was an exploratory piece of research, a qualitative approach was adopted. A total of 30 depth interviews were undertaken in February and March 2017 with UK registered charities, sampled from the respective Charity Commission databases for England and Wales, Northern Ireland, and Scotland.[2] This included 25 telephone interviews and 5 face-to-face interviews. Each interview lasted around 45 minutes.

The achieved sample profile included a wide range of charities, by income, location, charitable function, organisational status (including Charitable Interest Organisations, CIOs, as well as charitable trusts), service provision, and past experience of cyber security breaches.[3] The achieved profile is summarised in the following graphic.



*Main function bars in following order: arts/culture, community groups/other, education/health/social care, environment/conservation, international

[1] See https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017 for the Cyber Security Breaches Survey 2017.

[2] This sampling approach excluded unregistered charities (not registered with the Charity Commission) and unincorporated associations, as there was no readily available sample frame for these, and these organisations tend to be much smaller, and therefore less likely to face organisational issues around cyber security. In addition, certain types of registered charities were excluded. Private schools or colleges, and UK universities were excluded as they had already been in scope for the Cyber Security Breaches Survey 2017 (although educational charities were included). Finally, community halls and churches were excluded, as these organisations were considered less likely to have electronic records, so unlikely to be able to discuss cyber security in detail.

[3] Recruitment was undertaken by telephone. Minimum quotas in each of these categories were set in recruitment, and a £50 donation to the organisation was offered, to ensure involvement from a wide range of charities.

Within each organisation the main person responsible for cyber security was interviewed, which included a mix of Chief Executives, Trustees, Treasurers, Chairs and in some cases more junior staff members.

1.3 Interpretation of findings

A qualitative approach has been used to explore in depth how charities conceptualise cyber security, and how different experiences of breaches or attacks had affected organisations. Qualitative research also offers more nuanced insights on why charities have certain attitudes or behaviours with regards to cyber security than would be possible through a quantitative survey.

However, this research is not intended to show the *prevalence* of these attitudes and behaviours across the population of UK registered charities. The findings reported here represent common themes emerging across multiple interviews, as illustrated by verbatim quotes and case studies. As with any qualitative research, they are not intended to be statistically representative.

Impact of Wannacry ransomware attack

This research was conducted before the global Wannacry ransomware attack in May 2017.[4] This helps to contextualise the findings, especially the low awareness of ransomware among some charities, and the idea that some of these charities felt less at risk of cyber attacks than businesses. Since the attack, it is possible that this outlook has changed, with charities perhaps being more aware of the risks they face.

[4] See, for example, this news coverage on the BBC News website: http://www.bbc.co.uk/news/technology-39901382.

2 Awareness and attitudes

This chapter looks at how much charities felt they knew about cyber security, and where they got their information from. It also covers where cyber security sat among their organisational priorities, and the factors that led them to either prioritise or deprioritise the issue.

2.1 Awareness and consideration of cyber security

Pre-existing awareness and knowledge around cyber security varied across charities, generally linked to how much the individual in charge specialised in the role or had previous IT experience. In some cases, generally in larger charities, there was a specific IT director or someone on the board of trustees with private sector experience in IT, and they felt naturally more aware of the issue. However, these very specific cases were the exceptions, and there was a recurring theme across charities – especially smaller ones – of those in charge of cyber security not feeling well informed about it.

Several noted that they had not seriously considered the topic before the interview, and had not felt the need to learn more because cyber security was dealt with by an outsourced IT provider. In many of these cases, simply talking about the issue had for some been an eye-opener, with participants saying that they were keen to explore any protections they could take and the Government support available.

"I'm starting to realise that after this interview that people need to be more aware of the risks … People need a nudge, like this one, to realise there's a problem out there."
£500,000+ annual income, international aid charity

There was, however, a split in terms of cyber security being seen as an issue for charities, as opposed to one only relevant to businesses. Several participants felt that their lack of awareness was down to cyber security being viewed as more of a business issue. Common reasoning among smaller charities was that businesses would be more likely to have reserves of cash to target, whereas they would spend their funds immediately and not hold on to them. Some also felt that, overall, charities could be expected to have less to steal than profit-making businesses, which were more likely to hold onto, say, credit card details.

"We don't have a lot of money in our bank right now … we spend money straight away."
£0–£9,999 annual income, community group

On the other hand, various participants countered this viewpoint. They noted that it was particularly important for charities to stay informed about cyber security, over and above businesses, because of their specific circumstances. Some noted that charities had a significant duty of care to donors because they relied on them entirely – and this included keeping funds cyber secure – and were likely in many instances to have donor membership lists. In the case of larger charities, the size and complexity of the organisation also meant that those in charge did not see them as being very different from businesses.

"Personally I don't see why you should think differently at all. We are, in a way, a business. We're doing public things, we're handling money and we are registered with Companies House."
£10,000–£99,999 annual income, search and rescue charity

2.2 Information and advice sources

Across charities, there was often a reluctance to simply use search engines to find information about cyber security. This reflected that several participants, who were responsible for cyber security at their respective charities, did not feel they had the technical knowledge to navigate the information out there, and were worried about coming across poor information and advice without being able to judge the quality of what they were seeing.

In this context, three broad sets of information and advice sources emerged:

- Due to their restricted budgets, many charities tended not to have in-house expertise on cyber security. Therefore, where charities had an external IT provider, this was typically the first port-of-call for cyber security issues. The use of outsourced providers is covered further in Chapter 3.

- Many charities highlighted the regulatory organisations that charities would come into contact with in carrying out their functions, which they saw as credible sources online. Examples included the Charity Commission, Ofsted (for educational charities) and, in one instances, the Care and Social Services Inspectorate in Wales. Local councils were also considered credible potential sources of information, particularly among charities that already focused on local service provision. Government websites generally were considered to be credible and trustworthy on this issue, although there was not a clear sense with most participants of where they would search for Government information on cyber security.

- Informal information sources were also mentioned on several occasions. This ranged from friends and family members – for example, the chair of one small local community group had asked their ex-business partner's son to set up their antivirus software – through to trustees who had wider experience, sometimes in the private sector, and other charities. In one instance in a mid-sized[5] advocacy organisation for disabled people, the Chief Executive remarked that they also knew an external IT consultant who they could telephone for help informally when needed, but that most charities would not be lucky enough to have such a relationship.

Awareness and use of Government information and support

In terms of Government information and support, there was a sense that the Government had an important role in providing tailored information on cyber security for charities. Many participants said they would find Government recommendations or endorsements, for example of training providers as well as of general guidance, especially helpful. Other mentions included having a cyber security checklist for charities, or even a booklet outlining charities' responsibilities in this area.

"I think government should play a role … they could do a collective training programme … whenever we do training we don't want it half full so we invite other organisations."
£100,000–£499,999 annual income, community group

[5] Throughout the report "mid-sized" refers to organisations with between £10,000 and £499,999 in annual income (the two mid-range income band quotas used in recruitment).

"Charities need to be provided with a straightforward, easy to do checklist, which they can work through themselves and which doesn't cost them money."
£10,000–£99,999 annual income, health and social care charity

Despite this, many participants had in fact not proactively sought any Government information on cyber security, partly due to their lack of awareness around the issue, and partly feeling that it was not a priority for them. This included Government information and support, such as through the Cyber Aware campaign, Government-endorsed Cyber Essentials scheme and the Government's 10 Steps guidance – participants were prompted on all of these during interviews, and were typically unaware of them.

As a result, several participants had simply assumed that there was not Government information out there available for charities. Some were broadly aware that there was Government support for businesses, but again had assumed that this was not tailored for charities and so would not be relevant. There was also a generalised assumption that, were cyber security an important enough issue for charities to be engaging with, this information would be available from their established information sources, such as the Charity Commission website, and from other voluntary support bodies – examples mentioned included NCVO and the Northern Ireland Council for Voluntary Action.

It is worth noting that information and guidance on cyber security is already widely available for charities on the Charity Commission website[6] and the Charities against fraud website[7] This indicates that charities often had low awareness of it and were not actively searching for this information themselves; instead they expected to be receiving the information directly from the various support organisations.

This again reflects findings among businesses in the Cyber Security Breaches Survey 2017 – many businesses also expected that information would be tailored to their sector and would ideally come via their existing information networks, through regulators or trade bodies.

"I haven't seen communication from the Charity Commission or Companies House … they must just work on the basis that charities take responsibility for themselves."
£10,000–£99,999 annual income, search and rescue charity

"Small organisations in the voluntary sector tend to go to places where there is a support network and infrastructure to support people … something that has been tailored for charities."
£100,000–£499,999 annual income, educational charity

Awareness of Data Protection Act 1998 and the General Data Protection Regulation

Awareness of data protection law, including the upcoming General Data Protection Regulation (GDPR) was mixed, but there was nonetheless a sense that, across all charities, data protection was very important for them. This was particularly the case where charities worked with vulnerable clients, such as children, older people or disabled people. Linked to this, the Information Commissioner's Office (ICO) was often raised as another potential source of information on cyber security, given the existing link with data protection.

[6] See here for regulatory alerts from the Charity Commission: https://www.gov.uk/government/collections/regulatory-alerts-charity-commission
[7] http://charitiesagainstfraud.org.uk/

However, a belief in the importance of data protection did not always translate across into thinking that cyber security was important. Some smaller charities especially did not make this link between data protection and cyber security and conceptualised them as separate issues. Exemplifying this, some charities said that data protection was one of their top concerns, and that they had looked into and kept abreast of data protection law proactively, even though they had not looked proactively for any information on cyber security.

Awareness of GDPR specifically was low, reflecting that many had not looked into the upcoming regulatory changes. At most, some participants had read up on the topic but had not taken any action to adhere to GDPR yet. This typically matched the state of affairs found in the qualitative survey of businesses as part of the Cyber Security Breaches Survey 2017, where businesses were often currently unaware, and said they would take a closer look at GDPR nearer to when it takes effect.

Case study: how the focus on data protection can encompass cyber security

A large health and social care charity that provided support for unpaid carers viewed cyber security as a high priority, since they dealt with the personal data of very vulnerable people. The charity viewed their data protection obligations and strict adherence to the Data Protection Act as paramount in their cyber security responsibilities. They felt that charities, compared to businesses, should place higher importance on data protection, as charity clients are typically vulnerable.

"We deal with very vulnerable people … We do not keep data longer than we need it … We make sure we adhere to data protection regulations."

2.3 Reasons for prioritising or deprioritising cyber security

Charities' reasons for prioritising or deprioritising cyber security were often very similar to those of businesses, as established in the qualitative phase of the Cyber Security Breaches Survey 2017.

Like businesses, charities were more inclined to say cyber security was important in instances where they held personal data on groups such as donors, volunteers and charity service users. This was especially critical in charities that offered services to vulnerable user groups such as children, older people or disabled people. For example, one charity felt that the risks of a phishing email were greater for their user group of people with low literacy levels, since they would take such an email at face value and not think twice before opening any emails that came from the charity's staff. These charities also tended to cite data protection concerns as a stronger driving factor.

"Some of that personal information could be interesting for some people. There are cases where we have parents who are not together, and the mother or father is not supposed to know where that child is living."
£100,000–£499,999 annual income, educational charity

Prioritisation was also linked to how those in charge at charities conceptualised the issue. Across interviews, three broadly different ways of thinking about cyber security emerged:

1. Several participants recognised cyber security as a serious issue that required them to be alert to threats. This was more often the case where participants or those around them in the charity had a background awareness of the issue. For instance, in one charity, one trustee had private sector experience and had gained an understanding of the importance of cyber security in that role.

2. In some cases, participants saw cyber security as a common sense issue that should not require much thought or investment to get right. These tended to be individuals who lacked awareness of the issue. They felt they did not necessarily need to take pre-emptive action, but would ask staff to be sensible and avoid phishing emails when received, and expected all their trustees and staff to take a common sense approach of password-protecting sensitive files without needing further training on the topic.

3. In other cases, cyber security was considered as an unaffordable luxury. Some participants said they might invest more in areas such as awareness raising, training and outsourced cyber security if they had the funds to do this, but without these funds there was a sense that there was nothing they could do. One participant from a mid-sized health and social care charity felt, for example, that protecting themselves was not worth the cost – they were instead prepared to accept a financially damaging cyber attack on the basis that their donors would by sympathetic to lost funds, knowing that the charity does not have money to spend on cyber security.

"Cyber security needs funding, so the donors would not be surprised [if we lost money] … It would be less reputational damage. We will recover."
£100,000–£499,999 annual income, health and social care charity

Case study: assuming that cyber security is common sense

The Chief Executive of a mid-sized children's charity said they had not considered cyber security before taking part in this research, but approached it as a common sense issue, assuming that staff would know how to avoid phishing emails. Despite this, they had experienced a breach within the last two years, when a staff member's personal email was hacked, and started sending emails to staff mailing lists with a virus attached. They simply told staff to delete the email and not open it, and did not feel they needed to inform trustees as there was no material impact. With no impact, the breach has not encouraged them to change their approach. However, the Chief Executive did note that if they did lose their data through a breach, this would grind the service to a halt and they would be entirely reliant on their IT provider to help them. A successful breach of this kind would also be worrying because they personally did not back up their data regularly.

"If I had opened the email and it had wiped all the data from my laptop, it would have caused a real problem … I'm really not very good at backing up my stuff either."

Finally, another set of reasons for prioritising cyber security revolved around how professionalised the charity's operations were. Some charities noted that as they had grown, taken on more staff and registered as a charity or a company, cyber security had naturally become a bigger priority:

- Cyber security was a lower concern among smaller charities that still had paper records, as they felt that a cyber attack would not jeopardise them from keeping the charity running. Others did not use online banking, so felt they were not at risk of funds being stolen electronically. However, these charities felt that cyber security would become more important if they moved towards having electronic, or cloud-based records (which some were planning to do), started taking online donations or started banking online.

- Some charities that were contracted to provide public services had to meet accreditation standards for the organisations they worked for, such as the local council or other bodies. This was potentially a powerful nudge for them to improve their cyber security, if it was tied to wider accreditation. For instance, one children's charity was putting together a safe use of internet and IT policy because they wanted to become accredited with the London Youth network of youth clubs. This same charity had not felt a push so far to look into cyber security, but if it was part of getting this accreditation, they felt they would want to look into it.

"At the moment cyber security is not a priority, but I do see it becoming a big one in two or three years. At the moment our turnover's low … but as it gets bigger you want a lot more stuff online, like the bank stuff, so it will be quite important at that stage."
£0–£9,999 annual income, community group

Case study: registering as a charity as a nudge to look at cyber security

One mid-sized advocacy and safeguarding charity for disabled people worked a lot for other local organisations – for example receiving funding through sponsorships from their local authority. The charity wanted to demonstrate they were a professional and reliable service to these stakeholders, and felt that if they lost this trust, they would not be commissioned, so would not be able to realise their core purpose.

While they were unregistered, they had used personal Yahoo email accounts and one staff member's account had been hacked to send out phishing emails to their stakeholders. They were especially concerned these could have reached their vulnerable service users. Registering as a charity was considered a good point to review their approach. Actions taken included moving from personal email accounts to Office 365 accounts and investing in a new website. An apology email was also sent to everyone affected, which they think reflected well on them in the long term. In the future, if anything like this happened again, they said they would immediately report it to the IT consultants and the most senior person in the office on that day would be informed, who would then report the issue to the trustees.

"Registering as a charity was a great reason to review our policies and practices"

Prior experience of breaches also emerged in some cases as a reason for subsequently prioritising cyber security. This is explored further in Chapter 4.

3 Approaches to cyber security

This chapter explores the range of ways in which different charities had chosen to approach their cyber security, including those who had been placed in charge of the issue, relationships with outsourced providers, staff training, and awareness and use of cyber insurance.

3.1 Who is responsible for cyber security within the organisation?

Across the charities interviewed, it was typically the case that organisations did not have internal specialist staff with the technical skills to cover cyber security, due to this being seen as unaffordable and – where the organisation did not see themselves as a significant target for cyber attacks – unnecessary. As a result, responsibility for the issue lied with a range of different people across the charities that participated in the research.

In several cases, cyber security was overseen by senior staff such as Chief Executives, chairs and trustees, some of whom admitted that they lacked awareness of the issue. These individuals had seniority to implement changes, but had not, in many cases, seriously considered the issue before.

In other instances, cyber security had often been inherited as a role by someone in a junior position. This included in one case a communications assistant in a large environmental charity, who took on the role after the charity's previous IT manager left and was not replaced. The communications assistant had no direct contact with the board of trustees and felt that if they were not personally pushing cyber security, the issue would be forgotten by the charity. In another small conservation charity, a self-employed bookkeeper, who already dealt with the charity finances and reported on this to the trustees, had started to oversee their social media communications, and inherited cyber security through this.

"To be honest, I would probably be the only person who has reasonable proficiency in IT, so it falls on me to oversee it."
£100,000–£499,999 annual income, environmental charity

For all these individuals (senior and junior), cyber security was typically being looked at (if at all) alongside other main duties and responsibilities, such as finances, fundraising, communications or general operations. In this context, it often became sidelined, with staff not being able to focus on it.

"Because of the way we're structured, it's very difficult to have somebody that really focuses on cyber security … Particularly in the last year when people have been doubling-up on roles as well, just haven't had the time to do the things that we would like to do."
£0–£9,999 annual income, environmental charity

There were exceptions, again often linked to the private sector experience of individuals. For instance, in the mid-sized charity providing advocacy and safeguarding support for disabled people, the trustees had private sector experience, and would always get involved in cyber security on this basis. Each trustee, for example, had taken on a specific role in the implementation of a new cyber security policy.

3.2 Relationships with outsourced providers

Various participants highlighted that it was typical for all except the largest charities to outsource their IT (and consequently their cyber security) – again reflecting the Cyber Security Breaches Survey 2017 findings where outsourcing was most common among smaller and medium businesses. This was a method of keeping costs down as the contractual relationship was cheaper overall than hiring an in-house specialist – although it is worth noting that not all charities could afford an outsourced contractor either, leaving some with effectively no IT help beyond their informal information sources such as friends and family. Having an outsourced provider also allowed charities to gain access to more comprehensive support than would be covered by a single in-house specialist.

Relationships with external providers tended to be very passive, and this was linked to the fact that charities did not have the technical expertise to deal with the external provider. There was a sense from some charities that by outsourcing their IT, the issue of cyber security was kept at arm's length, and that they did not necessarily need to engage with the topic internally, as it was all dealt with by the highly-trusted external provider. One Chief Executive noted that they would only get in touch with their IT provider when something went wrong, and would not proactively contact them otherwise. In another case, with a large charity providing support for unpaid carers, the guidance around data storage followed by staff and volunteers had been produced directly by the outsourced IT provider.

Choosing outsourced providers

In some cases, participants had not been involved in choosing the outsourced IT providers they now worked with, as these relationships and contracts had been agreed before the participant entered into their current role. Where they had had a say in these contracts, or in instances where these contracts were currently undergoing renewal, there were various approaches used to find new providers. In larger charities, there were examples of formal tendering exercises, and participants felt that by introducing competition, they would typically end up with a higher quality provider. On the other hand, some participants noted that charities would, via this approach, typically discriminate on cost given their overall focus on keeping costs low – and this meant that some charities would inevitably choose less secure providers who charged the lowest cost.

There were instances where charities had attempted to validate the security of their providers. One charity had tried to find a secure provider by simply using the same provider as their local authority (and assuming the local authority would have checked the provider's security credentials). Similarly, another large healthcare charity was based in a UK university, and felt it was safest to use the university's IT infrastructure, which they assumed would be cyber secure. However, in other cases, participants admitted that they could not judge for themselves whether the outsourced provider was doing a good or bad job. This indicates that some charities struggled to identify appropriate providers and to manage the contracts effectively. This is similar to the business findings in the Cyber Security Breaches Survey 2017, where there was appetite from businesses for more advice in this area.

3.3 Staff training

Across interviews, it was uncommon to find charities that had provided cyber security training to any of their staff or volunteers, and this reflected the various barriers that charities faced to providing training

(discussed in the rest of this section). Where training had been provided, this ranged from charities providing a basic overview as part of an induction process, through to ad hoc training. One large conservation charity had used one of their two annual staff development days to give one-off training on cyber security, but this was a one-off, and was one of many topics they had selected for training.

Like many small businesses (as established in the Cyber Security Breaches Survey 2017), the kind of training that charities wanted was typically basic, for example covering aspects like logins and passwords, or how to spot malicious emails. Some suggested that they simply needed awareness raising across all their staff and trustees of the issue and the potential threats.

The most significant barrier in several charities was the perceived cost of cyber security training, and the fact that training as a whole was not prioritised in terms of spending in small and mid-sized charities. One participant noted that if they had extra budget, they would sooner spend this upgrading their old IT equipment rather than on staff training. Many participants felt that they would be happy to look into training if there were free resources available, but had assumed that training would come at a cost.

Case Study: applying for cyber security training as part of a wider training overhaul

A junior staff member in a mid-sized environmental charity was placed in charge of cyber security after the IT manager left the organisation, leaving no dedicated IT staff. The former IT manager had been on a few cyber security courses. The junior staff member wanted to get training for themselves – an introductory course on how to minimise risks within the organisation and giving them an overview of the basic actions people can take. The organisation is currently undertaking a wider overhaul of all staff benefits, and as part of this, the junior staff member is going to ask them to fund a training course on cyber security (which would otherwise not be funded on its own).

"I would certainly benefit from staff training … It's something we're trying to implement within a range of staff benefits."

Other barriers highlighted were as follows:

- Charities lacked the knowledge and skills to pull together training themselves. Some highlighted that the Government could help to signpost organisations that offer free online training materials – especially ready-made presentations – or that these materials could be hosted online by the Charity Commission, or other volunteering bodies. Where charities had put together training, the materials were often compiled in collaboration with the charity's outsourced IT provider.

- In smaller charities, there were specific barriers. Some smaller charities felt they were too small to require training, since only a few people would have IT access. In other small charities, frequent remote working and long gaps between when trustees met face-to-face meant that face-to-face training sessions were impractical. While face-to-face training was noted as a preferred approach in some cases, these charities were often open to online training options, particularly if free.

"We're just too small for [cyber security training] to be relevant really. I just don't think that there would be a case for it."
£10,000–£99,999 annual income, search and rescue charity

- A final attitudinal barrier was the sense that cyber security training was not necessary if the charity had not been breached before. Some charities said that only having a breach and understanding the impacts would incentivise them to offer training.

3.4 Cyber insurance

There was a general lack of awareness of the notion of cyber insurance among participants in this research. Some charities noted that they had wider insurance policies such as general business insurance, public liability insurance, business continuity insurance or other insurance around data protection, but were not clear on whether these would cover them in the result of a cyber attack. In some cases, participants said that their insurance broker had gone over the range of coverage with them in a meeting, but they could not recall what was mentioned about cyber security specifically. These findings are similar to those among small and medium businesses in the Cyber Security Breaches Survey 2017.

Only one of the charities interviewed had specific cyber insurance. This was a large charity running an independent schools network, with centralised IT and an IT manager – so with a much larger budget than most of the other charities interviewed.

Other participants felt that cyber insurance, like training, would be too expensive for their organisations, and that they could not justify the cost if their organisation did not hold any personal data and took other sensible precautions already, such as backing up files.

3.5 Barriers to improvement for charities

While charities faced many of the same issues and challenges as businesses when it came to their approaches to cyber security (as found in the Cyber Security Breaches Survey 2017), charities also faced many unique barriers, summarised in the following graphic and covered in this section.

Competing demands

Charities had several major competing demands that could lead to lack of investment in cyber security. Activities such as core service provision, fundraising, monitoring finances and other Charity Commission reporting requirements were all viewed as more pressing and more important overall to keep the charity afloat. Since cyber security was not typically considered as a business continuity issue (which is discussed further in Chapter 4), it was treated as a desirable rather than essential activity. Where charity funds were allocated was often up to trustees or commissioning bodies (in cases where they provided Government

services), and some charities stated that if their budgets increased, they would sooner spend the money on other areas.

"We need to make sure we are taking the right precautions to safeguard our information … but we have other priorities – difficulties with cash coming in, and a restructure last month."
£500,000+ annual income, international aid charity

Trustee and staff skills

Participants noted that smaller and long-running charities often tended to have older trustees, who might lack IT skills and work only part-time, as well as in multiple roles. This made it particularly hard for these charities to get engagement with cyber security among trustees and also to find people internally who could champion the issue.

"The businesses I've been involved with have always seemed to have considerable manpower and money to deal with that sort of thing, whereas we're a charity and the 3 trustees at the moment, the youngest is 69, so obviously we don't have the expertise."
£0–£9,999 annual income, community group

Focus on costs and cost-cutting

Across different sized charities, there was a strong cultural emphasis on costs and cost-cutting, which made spending on cyber security more challenging to justify. This reflected the idea that charities felt particularly accountable for all money spent, as it came from donations.

This had significant implications in terms of the outsourced providers that charities used, and how much outside help they would ask for. For example, the charity offering advocacy and safeguarding support to disabled people noted that every call to their outsourced provider cost them money, so they often had to make a decision on whether to involve external support, or try to deal with the problem in-house. The same charity suspected that budget constraints had led other charities in their local network to make more reckless decisions without understanding the consequences, for example in choosing less secure IT providers based on cost. This cost focus was also evident in terms of charities' reluctance to upgrade equipment – for example in sticking with unsupported Windows XP software or using personal emails rather than group emails.

Case study: incurring several minor breached due to outdated software and systems

One small environmental charity has incurred several minor breaches related to website hacking and phishing emails. On occasions, their website was taken down and linked instead to a spam site as a result of the breach. On another occasion a virus got through because an individual staff member had not updated the antivirus software on their computer. The charity felt there was no notable impact from either of these breaches.

Despite these incidents, the organisation was reliant on their IT provider to protect them and did not feel they understood the extent to which they were protected. Overall, the charity still perceived their organisation to be low risk, as they were not well known, were not a profit-making business and were not a Government Department. They thought that charities would not be a valuable target for hackers.

Lack of a central office and remote working

Smaller charities and the mid-sized ones that had restructured to save money often lacked a head office, instead opting for staff to work from home, sometimes using their own personal devices. The changes in the board of trustees each year also meant that locations moved around. This made face-to-face training more of a challenge, and also made these charities more susceptible from breaches via personal devices.

"I guess you could compare us to a small business, but then a small business – even one that's operating from home – is usually in one location. We are in multiple locations, which can change every year depending on who is elected."
£0–£9,999 annual income, environmental charity

4 Perceptions and experiences of breaches

This chapter looks at how charities considered themselves to be at risk (or not) from cyber security breaches or attacks. Where charities had suffered from breaches, it looks at the impact of these and how charities responded.

4.1 What do charities feel more or less at risk from?

A common theme across interviews was that charities were particularly concerned about keeping their funds secure. As noted in Chapter 2, this linked back to the strong duty of care that charities felt they had to their donors, and the sense that the money did not belong to the charity. The strength of feeling here was such that some charities had chosen consciously to remain low-tech in their operations, for example by avoiding online banking or cloud storage, so that they did not have to address cyber security risks.

"I think it's the issue of trust … If someone is giving you money, or has given you money, they want to know that their money isn't going to be stolen."
£100,000–£499,999 annual income, arts and cultural charity

Alongside loss of funds, loss of personal data (for example donor lists) was also considered to be a major risk. Both these threats were treated as existential threats, because losing data or money through a cyber attack would lead to a loss of trust and confidence among donors, service users and other stakeholders such as commissioning organisations. Maintaining trust in the charity was identified as being integral to a charity's survival, especially for those providing Government-commissioned services to vulnerable adults. As these charities saw it, if trust dissipated, they could lose donors and contracts, meaning they would no longer be able to fulfil their core purposes.

"Confidence from the people who donate to us would be the first thing we would lose … If our contact list was stolen that would erode confidence that we were handling their details properly."
£100,000–£499,999 annual income, international aid charity

In this context, the idea of funds or personal data being stolen electronically seemed to outweigh other cyber risks, such as loss of day-to-day (non-personal data) files, for instance through ransomware attacks. Much like the businesses interviewed as part of the Cyber Security Breaches Survey 2017, many charities did not understand the inherent value in their non-personal data, which they felt would be of less interest to malicious hackers. Some felt that losing these data would not impact the day-to-day running of the charity assuming the data had been backed-up. Related to this, loss of business or operational continuity was not typically raised as one of the major concerns around cyber attacks – although it was mentioned, it was not seen (unlike other threats) to lead to loss of trust among donors or stakeholders in the same way, so was not viewed therefore as an existential threat.

4.2 Experiences and repercussions of breaches

The charities interviewed had experienced a wide range of breaches or attacks, including viruses, phishing emails, ransomware attacks, identity theft and website takedowns. This included examples where charities, their staff or volunteers had incurred financial losses through the breach. For instance, in

one mid-sized community development trust, one of the volunteers had unintentionally downloaded Trojan horse malware onto the shared laptop for volunteers, which lead to two other volunteers having money stolen after they made personal payments from the laptop.

There were further examples of where charities had lost non-personal data or control of their website, preventing them from carrying out their main functions, and then relied on external IT providers to resolve the issues. In one case, a mid-sized arts organisation had their website taken down several times, with the first attempt at recovery taking their hosting company 10 days. They felt that they were lucky with the timings of this attack, taking place at a relatively quiet time for them in September. However, if the attack had occurred in January, they would have incurred several business continuity issues. This highlights how loss of business or organisational continuity can have important impacts on charities, even though some considered this as a less significant risk.

Case study: incurring a website hack which caused reputational damage

One small horticulture charity was concerned about the trustworthiness of their external website hosting provider, after Google Search Console picked up some of their webpages as having malicious code. The same issue happened around two years ago but on that occasion they were able to delete the information and reload the affected webpages in order to rectify the situation. The charity felt these breaches had a negative impact on their reputation, as Google search results came up with a warning about their website saying it could have been hacked. Neither the charity nor the host can find out what the issue with this code is. As a result, the charity may need to pay the host to investigate further. These breaches were reported to the trustees and some charity members were aware after noticing the issue. In the long term, the charity was looking at moving the website, as they did not trust the IP address used by the existing provider.

As with businesses (from the Cyber Security Breaches Survey 2017), the experience of having a breach was often enough to spur charities into action. For example, in the aforementioned case where the volunteers' money was stolen, the charity ultimately ended up changing their written policies for volunteers, having an ad hoc face-to-face training session for volunteers to help them avoid bad practice, and replacing the laptop (since the old one was no longer usable). On the other hand, there were several other examples of charities experiencing breaches, such as websites being taken down or staff emails hacked, but these breaches had not made any impact on their operations, so the charity had continued without any changes – highlighting that charities were not necessarily learning from these attacks.

Case study: incurring a breach with a substantive financial impact

The CEO of a large charity that delivered music lessons and events in their local community had their email hacked. It sent out a fraudulent message to the charity's financial manager, instructing them to release funds to pay for new equipment. The financial manager used Faster Payments to transfer the cash.

The breach was identified the next day, when another fraudulent email was sent asking for the release of more funds. The charity could not recover the funds and ultimately lost £13,000. As a result of the breach the charity revised their policies on authorising payments, with at least two members of staff and the CEO subsequently having to sign off any payments.

"Because it's the CEO, you think, 'oh he must know what he's doing,' and if he's told you to do something you do it, you're less likely to question it."

4.3 Reporting of breaches

Participants commonly noted that if there was a serious breach, they would inform both the charity trustees and, where they had one, any external IT providers who might help them resolve the issue. Beyond this, participants were often unsure of when and where they might report breaches externally – this was again a similar finding to that in the Cyber Security Breaches Survey 2017 with businesses.

Some participants made a distinction between cyber attacks that resulted in financial losses versus those that did not, even if these were successful at breaching IT systems. If a breach resulted in the loss of charity funds or was otherwise financial in nature, some said their first port of call would be to the charity's bank, and one participant mentioned that they would involve the police in such breaches.

Participants were less certain when it came to breaches that were not necessarily financial, such as malware or ransomware attacks – both in terms of whether they should report these and where they could be reported. Some noted that they would need to look into their reporting obligations if individual membership or donor data was compromised. Once again, the ICO was mentioned as a potential reporting destination, highlighting the high importance that many charities placed on data protection.

Charities were also prompted in interviews on their awareness of Action Fraud. Generally, awareness of the organisation was low and these discussions typically followed initial references to the ICO and the Charity Commission.

Case study: reporting a malicious attempted attack to the police

One large education charity that oversaw a group of schools and also ran training courses for adults had a situation where one of their foreign students was facing deportation to their home country. Shortly after this, they found that somebody had tried to access and deface their website in what they thought was a related attempted attack.

The charity called in the police and also reported the attack to the Education and Skills Funding Agency. The police took action and the information they provided was useful as they were able to trace the attack back to a terrorist organisation. The charity's Deputy Chief Executive felt it was right to report this malicious attack, but noted that they could not report every attempted or even successful website hack to the police, as they would then be in constant contact with them – they noted that attempted hacks took place every day. In this context, it may be useful for the charity to understand a bit more about what attacks are worthwhile to report.

This breach was ultimately unsuccessful, so the Deputy Chief Executive felt it had limited impact. However, they said that if somebody did manage to hack into their website or servers it would have a significant negative operational impact. Currently, they felt relatively well protected from cyber attacks due to having robust security systems in place, with any suspected attacks immediately reported to the IT Director.

5 Conclusion

This research, when considered alongside the Cyber Security Breaches Survey 2017, suggests that UK registered charities are not fundamentally different from businesses in how they view and approach cyber security. Many charities treat cyber security as an important issue and, in certain cases, see cyber attacks as an existential threat to their organisations. This research has also demonstrated that charities can and do suffer substantive cyber security breaches with financial repercussions.

However, charities do face some unique constraints and challenges that will be important for organisations to recognise when trying to discuss cyber security with this audience.

Understanding the context in which charities consider cyber security

For some, there was a sense that cyber security was more of a business issue than one for charities to address, or that it was a common sense issue – one that only required minimal staff or volunteer engagement when something goes wrong. On the other hand, some participants acknowledged that if charities assumed that businesses were more likely to be targeted, and so deprioritised their own cyber security, they would inadvertently make the charity sector a softer target.

This highlights that there is still a need to raise basic awareness of cyber security among charities. This can help them to understand that cyber attacks can be indiscriminate in who they target, and that there are certain basic controls that they can implement, beyond asking their staff to take a common sense approach (such as the technical controls laid out in the Government-backed Cyber Essentials scheme).[8]

Across charities, there was an especially strong concern about funds or personal data being stolen, as these were seen as existential threats. Some charities therefore seemed to focus less on threats to non-personal data, even though others acknowledged that losing access to non-personal data would also stop their organisation from functioning. Focusing on the risks that already worry charities and linking cyber security to data protection may help to raise awareness of the issue, but it may also be important to help charities understand the implications of losing non-personal data (e.g. from ransomware).

Communicating cyber security to charities

This research has highlighted the barriers that charities face when it comes to addressing cyber security, and this has implications for how to engage with them on the topic.

The emphasis on cost control and the typical lack of in-house IT skills in charities suggests that many would benefit from free or low-cost training, ready-made presentations and checklists. The tendency towards remote working in many smaller charities also suggests a need for online training options.

It is also worth noting how and where charities expect to receive information and guidance on this topic. In the interviews, many had not proactively sought information, and assumed that if the issue was something they needed to address, they would receive notice of this via their established communication

[8] See the Government's Cyber Aware website for an overview of Cyber Essentials, at: https://www.cyberaware.gov.uk/cyberessentials/.

channels, for example through local authorities or the Charity Commission. Charities also wanted to receive guidance that felt tailored towards them rather than at businesses.

However, the findings also suggest that the information needs for both groups are similar. Many participants wanted materials to aid with basic awareness raising among trustees, staff and volunteers. Where staff had responsibility for cyber security but felt they lacked the technical knowledge and skills to carry out the role more effectively, they also wanted training on the kinds of risks their organisation should be addressing and how to deal effectively with outsourced providers.

Changing attitudes and behaviours

Across the interviews, there were recurring milestones, tipping points or drivers that participants suggested had changed their organisation's attitudes towards cyber security and led to them taking preventative actions.

- The individuals pushing the importance of cyber security within organisations sometimes lacked understanding and support from more senior colleagues. By contrast, where charities had trustees or staff with relevant private sector experience, they tended to be more familiar with the issue, and the staff responsible for cyber security at these organisations were typically better supported. Bringing in this expertise from the private sector, possibly via trustees, may help encourage investment in cyber security.

- In cases where charities had experienced serious cyber security breaches, these occurences had often lead to wholesale changes in how the organisation approached cyber security. Many charities also said that they would only consider training or insurance if they experienced a breach and saw that this was an issue that could affect them. Case studies such as those in this report may be helpful to explain the impact of breaches to charities, and encourage action.

- Some charities mentioned that they would look more at cyber securityin the future, when the scale of their operations increased. Examples raised included taking on more staff, starting to receive online donations, moving to internet banking, moving from paper to electronic records (or moving existing electronic records online), upgrading their website, registering with the Charity Commission for the first time, and – where relevant – becoming a charitable company for the first time. These may be natural touchpoints for the Government or public bodies to engage with charities on this topic.

Topic guide

Prompts and probes	Timings and notes
Introduction	**Very briefly**
• Introduce yourself and Ipsos MORI – independent research organisation (i.e. independent of Government) • Commissioned through the Government's National Cyber Security Programme • Explain the research: *We are speaking with 30 charities to learn more about how they approach and deal with cyber security* • Confidentiality: *all responses are totally confidential and anonymous, and no identifying information will be passed onto the Government or anyone else* • Length: around 45 minutes • Get permission to digitally record ADD IF NECESSARY: *The purpose of the survey is to help the Government to understand what charities currently do to prevent and deal with cyber security breaches or attacks, how important they think the issue is, and how any breaches or attacks have affected their business, including financially. The findings will inform Government policy and the guidance offered to charities.* ADD IF NECESSARY: *By cyber security, we mean 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.*	The welcome helps to orientate the participant and gets them prepared to take part in the interview. Outlines the "rules" of the interview (including those we are required to tell them about under MRS guidelines). Make this very brief.
Section 1: Context	**2–3 minutes**
Could you tell me a bit about your organisation and how it might be affected by cyber security issues? • Nature of work (e.g. international, partnerships with businesses, Government, other organisations etc.) • Number of trustees/employees/volunteers/donors • Electronic data held by the organisation (e.g. personal/financial data on donors, other data they consider valuable) • How are files stored/shared (use of cloud?) • What is done online/using IT (e.g. ability for donors to donate online) • Level/kinds of access volunteers have to these areas/systems? **Could you briefly describe your role?** • Main responsibilities (just cyber security or broader?) • Length of time in current role • Any other people working on cyber security, or just them? **Do you outsource any part of your cyber security?** IF OUTSOURCE: • Reasons for outsourcing (e.g. due to breach/attack, changes in staff, to get external advice/information) • How did you choose your contractor? How easy/difficult was this?	This section provides context to follow up on later in the interview, in terms of their potential exposure to cyber security risks, and who deals with it in the organisation. Make this brief.

Prompts and probes	Timings and notes
• What are external providers (and you) responsible for? • What information do you get from them? How informed do you feel about what your provider is doing/how well they are protecting you? • How much do you trust the contractors to protect you?	
Section 2: Perceived importance and culture towards topic	**10 minutes**
How much of a priority is cyber security in the organisation? • Where does cyber security fit in terms of other priorities and issues (e.g. fundraising, campaigning, projects etc.)? • Where does it fit in terms of other regulatory requirements for charities? More/less important than other areas? IF VIEW CYBER SECURITY AS LOW PRIORITY: **What makes it a low priority?** • Gets in the way of people doing their jobs? Other organisational priorities? • What would have to happen for cyber security to be a higher priority? • Low priority for everyone or for certain people (trustees, senior management, employees, volunteers etc)? **What are the biggest cyber security risks to your charity?** • What do you think could happen to your organisation if there was a breach/attack? What do you stand to lose? What are you most worried about? • What's the motivation (reputation, being stopped from carrying out day-to-day work, compliance with regulations, protecting donors/privacy etc)? • Perceived value of data they hold? • Who poses the biggest risk (e.g. volunteers, suppliers etc)? Any weak links? • How might charities have different risks to private businesses on this issue? **How do you try to manage these risks? How manageable are they?** • What measures or practices/technical controls/training do you have in place to manage these risks? • How effective do you think the measures you have in place are? • Risks from volunteers, suppliers etc? **How do attitudes to this issue differ for different groups within or working for your organisation towards cyber security?** • How well different groups are aware of/understand the topic • How much do senior management/trustees discuss it? How much has it been discussed in the past? How have these discussions taken place (e.g. board meetings, all-staff etc)?	This section aims to understand more about the organisational culture and attitudes towards cyber security and their confidence and knowledge in dealing with cyber security. It also aims to explore to what extent it is considered a priority, including any differences between different players (trustees, staff, volunteers etc).

Prompts and probes	Timings and notes
• Different for trustees/senior management than for employees/volunteers? • Ever raised by others, e.g. donors, partners, suppliers, regulatory bodies? How important is it for these groups? Their expectations of you? **How might being a charity make you think differently about cyber security than a private business? What makes you say this?**	
Section 3: Seeking information	**10 minutes**
I'm interested to find out more about the kinds of information and support organisations like yours get regarding cyber security. **What areas of cyber security have you sought information on before?** **Who/where would you expect to get information, advice or support from?** • E.g. software/security firms, outsourced providers, other charities, Government, Charity Commission etc? • Where would you go if you were actively looking for information or support? • Which sources would you trust/not trust? What makes you say this? **Who do you share this information with, within the organisation (trustees, senior management, employees, volunteers etc)?** **How do you keep up-to-date on the topic? How much do you feel up-to-date on the topic?** **Have you come across conflicting advice on cyber security?** • What did you find conflicting advice on? • How easy/difficult was it to know what to do/who to trust? • What did you do in this instance? **What information have you seen or heard about from the Government on cyber security?** • Probe Cyber Aware, Cyber Essentials, 10 Steps to Cyber Security • How helpful was this information? What was missing? Improvements? • What have you done with it? • How much is relevant to charities like yours? Applies to businesses more than to charitable organisations? What would reflect charities' needs better? **How much do you know about the Data Protection Act 1998?** • How closely do you think you adhere to the Data Protection Act? **What do you know about the new General Data Protection Regulations?** IF HEARD OF THEM: • What measures, if any, have you put in place to adhere to the changes? • How easy/difficult has this been?	This section explores information and support received (and actively sought) by organisations. We want to know if it's easy to get what they need, what is lacking, where they are looking and who/what they trust. We want to probe awareness and use of Government information and support in particular. Do they feel that the support out there is relevant to them, or is it just seen as something for private businesses?

Prompts and probes	Timings and notes
Section 4: Training	**6–8 minutes**
Now I'd like to ask about some specific things your organisation might do or have. **Does your organisation provide any kind of cyber security training?** IF PROVIDE STAFF TRAINING: **What does this involve?** • Compulsory/voluntary? • Who is it for? Who attends? Trustees, senior management, employees, volunteers etc? Probe whether volunteers treated same as employees. **How useful is the training? What difference does it make? Has it changed attitudes/behaviours?** **How easy/difficult was it to get training set up?** • Challenge finding good training providers/materials? • Do they feel they have the necessary training/expertise themselves? • What more advice/support around training might be helpful? IF DO NOT PROVIDE STAFF TRAINING: **What are the reasons for not having cyber security training? Have you looked into it before?** **What would incentivise your organisation to start training on cyber security?** **What more advice/support around training might be helpful?**	This section looks at whether they provide any training on cyber security, and specifically how easy it is to find good training, or set it up internally. It's also looking for any good practice examples.
Section 5: Insurance	**5 minutes**
How much have you heard about cyber security insurance before? • What heard and where? • How much they feel they understand? Complexity of it? Support needed? • How could the cyber security insurance market be improved? What's missing? **Does the organisation currently have insurance which would cover you in the event of a cyber security breach or attack?** IF HAVE INSURANCE: **Can you tell me what you know about the policy you have?** • Is cyber security part of a wider insurance package or stand alone? • Type of cover (1st or 3rd party losses)? • Reasons for getting it in the first place **How was it set up? What was the process/challenges you went through?** • Who in the organisation set up the policy (e.g. legal department)? • How involved were people with cyber security oversight in setting this up? • Any comparison between different policies? How did they make a decision? **What are the benefits of having cyber security insurance? Probe why they need it if they're already taking action to manage risks.**	In this section we want to know how much they know about/have considered the cyber security insurance market, how aware they are of their own coverage and what kinds of discussions they have had about it. Make very brief if they don't know much about this topic.

Prompts and probes	Timings and notes
IF DO NOT HAVE INSURANCE: **What are the reasons for not having cyber security insurance?** • Have you considered insurance before? • What conversations have you had? Who was involved? • Probe barriers: cost, complexity, lack of awareness/time/resources etc **Do you think you will get cyber security insurance in the near future? What do you think will make the difference?**	
Section 6: Experience of cyber security breaches	**6–8 minutes**
IF HAVE HAD CYBER SECURITY BREACH (IN SCREENER): *I'd like to talk a bit about the breach(es)/attack(s) you had within the last 2 years.* **Can you tell me briefly what it was and how it occurred?** • Type of breach/attack • Where it emanated from (e.g. employees, volunteers, external etc) • Motives behind it **Can you tell me what impact it had?** • How disruptive was it? How long did it take to recover? • Who was affected? • What did this mean for the organisation? Probe reputational damage, being stopped from carrying out day-to-day work, breaking compliance/regulatory requirements, breaching privacy etc. • How did this compare to your/others' expectations? Any unexpected/bigger-than-expected impacts? **How well do you think your organisation dealt with the attack?** • What plans/policies did you have in place? How well did these work? • Where did you get information/advice? • How much were you expecting this kind of an attack? How much of a surprise was it? • What worked well/what didn't? Any gaps/weaknesses discovered? **What did you learn when dealing with the cyber security breach?** • How has this informed your approach for dealing with cyber security? • What has changed now? Any changes to incident response plans, policies, software, general spending on cyber security? If nothing, why not? • Any change in awareness/understanding resulting from the breach (for trustees, senior management, employees, volunteers etc)? • How likely is it to happen again? **Who did you report the breach to?**	We want to have case studies of breaches/attacks to be able to use in the report. We also want a sense of what changed afterwards – how big a turning point was the breach? Did it raise any surprises, things they hadn't considered etc?

Prompts and probes	Timings and notes
• Probe trustees, senior management, donors, partners, Government etc. • Who would you usually report something like this to? • What makes it significant enough to report? • When would you ever not report an attack/breach? UNLESS COVERED EARLIER IN SECTION 2: **How likely do you think breaches or attacks are?** • What kinds are you most likely to face (malware, ransomware etc)? • Staff/volunteer-related, external, international, accidental breaches etc? • How well prepared do you think you are? UNLESS COVERED ABOVE: **Who would ever need to report a breach to?** • Probe trustees, senior management, donors, partners, Government etc. • What makes it significant enough to report? • When would you ever not report an attack/breach?	
Section 7: Cyber security in future	**5 minutes**
I would like to ask briefly about how things are expected to change over the coming years. **What do you see as the main cyber security challenges likely to emerge for the next 5 years?** • For your organisation? Any plans for moving more things online, changing how data are stored, any outsourcing plans etc? Have risks of these been considered in terms of cyber security? Do they get considered in that way? • For charities specifically? Different from private businesses? • Generally? **What do you think needs to be put in place to deal with these challenges?** • Probe on hiring more staff, training, changing organisation's policies etc. **What more information, guidance or support do you think you will need to deal with cyber security? What's available/missing right now?**	A brief section to understand how the charity views the challenges regarding cyber security for the next few years (for their organisation and in general), and if they think they are in a good place to deal with them.
Section 8: Wrap-up	**2 minutes**
Is there anything that we haven't discussed that you would like to raise? Overall, what do you think is the one thing I should take away from the discussion today? Reassure about confidentiality. THANK AND CLOSE.	Wrap up interview, summarise suggestions for further support/guidance.

About the Ipsos MORI Social Research Institute

The Social Research Institute 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. This, combined with our methodological and communications expertise, helps ensure that our research makes a difference for decision makers and communities.

For further information about Ipsos MORI please contact:

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

Department for Digital, Culture Media & Sport

4th Floor, 100 Parliament Street
London, SW1A 2BQ
www.gov.uk/dcms