PROTECTIVE
INTELLIGENCE

Cyber Security And Data Protection In The Voluntary Sector

2016 Report

CYBER SECURITY AND DATA PROTECTION IN THE VOLUNTARY SECTOR — 2016 REPORT

Welcome

The voluntary sector feels like it's under attack at the moment. Adverse media coverage, investigations into fundraising methods and the fallout from Kids Company have all dominated the headlines in recent months.

It's also under attack from hackers and serious organised crime and, as regulation becomes tighter, there will be more frequent and stiffer penalties handed out for serious data breaches. Currently the Information Commissioner's Office (ICO) can levy fines of up to £500,000 per infringement, but the proposed EU General Data Protection Regulation could see fines as high as €20m or 4% of global revenue – whichever is the higher. Whilst we seriously doubt that charities will be punished at the top end of the scale, it is an indication of how tough the new rules will be.

The average cost of a data breach for an organisation of less than 50 staff is now £193,000 – for organisations over the 500 staff mark, this rises to a staggering average cost of £2.3m. With even small businesses expecting to be attacked at least four times a year, and larger ones suffering on a daily basis, the time has come to accept that information protection needs to be a core principle of your organisation's daily routine.

Sadly, you cannot count on your charitable status to protect you from your data being lost, exposed or corrupted in today's world. According to the ICO, data security incidents within the voluntary sector rose by 35% from Q2 to Q3 2015.

Simply put, the sector can no longer treat data protection as an afterthought. It's time to get serious about security.

We've commissioned this report to gain an understanding of where the voluntary sector in the UK sees itself in relation to cyber security. There are encouraging signs that the sector is taking the threats seriously, but there's also evidence that there is still a long way to go to make sure the data of your staff, trustees, donors and clients is kept as safe as possible.

The sector provides much needed help and support to the vulnerable, especially in times of austerity. We hope you'll join us in thinking that we need to do all we can to protect the vital services the sector provides.

Finally, I'd like to thank the team at Third Sector Insight for their assistance and, most importantly, those of you who took the time out of your day to complete the survey.

Enjoy the report.

VINCE WARRINGTON
DIRECTOR
PROTECTIVE INTELLIGENCE

Contents

BACKGROUND TO THE REPORT

Introduction

Cyber crime, it seems, is never out of the news.

Over the past few years there have been a number of high-profile victims of attacks by hackers, or have accidentally disclosed confidential information, or even had an insider leaking data.

You're probably aware of the hack on Talk Talk's customer database in 2015, maybe you've also heard of the Saudi Aramco attack – which could have had a massive knock-on effect for the global economy if the oil giant had been forced to stop production – and you've definitely heard of a certain Mr. Edward Snowden.

One of the dangers of the media reporting on such events is the impression that only large businesses and government departments are under threat. The reality is somewhat different, with organisations large and small and individuals from all walks of life constantly having their data under threat from hackers, criminals and accidental loss or exposure.

Cyber Crime: Easy to commit, difficult to trace and highly profitable

The scale of the problem is immense. Some reports put the income generated from cyber crime as high as £500 billion per year, and in 2015 it overtook the international illegal drugs trade in terms of profitability.

The players in this market are serious indeed – no longer do you just need to worry about a teenager sitting in his darkened bedroom trying to break your website.

Information Protection will become a core corporate function

In the future securing your data will become as commonplace as holding a fire drill in your office, or making sure you've locked your doors and windows before you leave the house. However, we're not there yet and the risks are going to be with us for a very long time to come.

Protective Intelligence teamed up with Third Sector Insight to undertake a survey of the current state of cyber security within the voluntary sector, as we felt that there was a significant risk to charities from cyber crime, hacking and data loss. We wanted to find out just how seriously the problem was understood and this report is the outcome of that survey. We hope the information contained within will provide an awareness of the risks posed by data breaches, as well as showing where improvements can be made.

Data Gathering

Overall, there were 398 respondents. As with any survey of this type, we would not expect everyone who completed it to know the answers to all of the questions.

BACKGROUND TO THE REPORT

However, we have left in the 'Don't Know' answers in our results, as this helps to give an indication of how widespread knowledge and awareness of data protection and cyber security is within the sector.

The respondents came from a wide range of professions within the sector, which helps us to understand the overall picture much better than if the survey had just been targeted at IT professionals – this is an important point, as the foundation of a secure organisation is understanding that the protection of data is everyone's responsibility, not just that of a few technical staff or the CEO.

Comparison to Private Sector

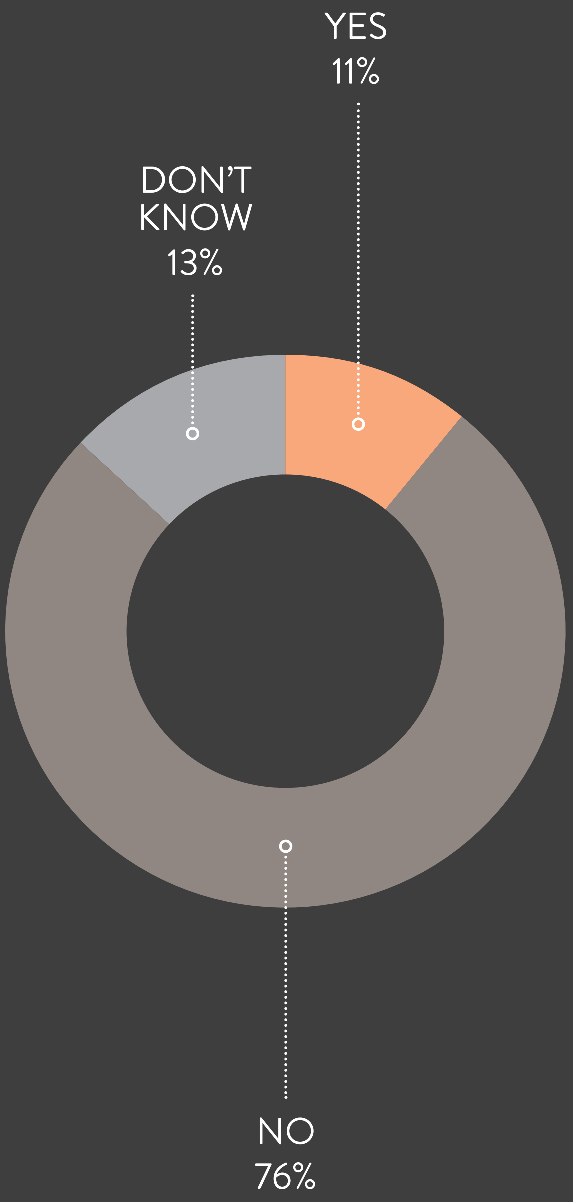
For comparison we have included data from PwC's 2015 Information Security Breaches Survey (available at www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html), which provides representative figures for SME and large businesses. This will give an indication into how well the voluntary sector is coping when compared to the private sector.

The PwC survey classes small businesses as those employing less than 50 staff, whilst large businesses are classed as those with over 250 employees. Unless otherwise noted, businesses with between 50 and 249 staff had similar results to those classed as small.

We have included a number of case studies in this report to demonstrate real-world examples of serious security incidents within the voluntary sector. These are included purely to illustrate some of the key information security risks, and are not intended to cause any further embarrassment to the parties concerned.

DATA COMPROMISED BY ACCIDENT

Has your organisation ever had the confidentiality, availability or integrity of its data compromised by accident? This could include losing laptops or USB keys, or accidentally publishing confidential information.



This is an encouraging sign, as it would seem that charities have generally managed to keep their data secure from accidental loss or exposure. The number of positives (11%) is lower than that of small businesses (33%) and large businesses (76%) who suffered a 'self-inflicted' data loss in 2015 – even if we were to assume that all of the 'Don't Know' answers had suffered a breach; it would still put charities in a better position than the private sector.

This result may, in part, be attributed to the greater sense of connection to the goals of a charity that staff feel in the sector, and to the increased sense of wanting the organisation to succeed when compared to workers in the private sector, combined with an understanding of the value of computer hardware and the burden it imposes on a charities finances. Whilst such an intangible is hard to measure, there is some evidence to suggest that those in the voluntary sector are less likely to lose laptops than those in the corporate world.

There is, however, little room for charities to rest on their laurels. Humans are always the weak link in the security chain, and even the best of us make mistakes. Our survey has revealed similar stories of data loss when compared to businesses. Amongst the missing laptops and USB keys were stories of confidential information being printed out and lost (including examples of papers being left in public places) and emails containing sensitive data being emailed to the wrong recipients.

DATA COMPROMISED BY ACCIDENT

Case Study: 56 Dean Street Clinic

On Tuesday 1st September 2015 an email newsletter was sent out from the 56 Dean Street HIV and Sexual Health Clinic, part of the Chelsea and Westminster Hospital Trust, to 780 patients. Unfortunately, the member of staff sending the email made a very simple and easy to commit mistake and placed all of the recipient email addresses in the 'To' field, rather than the 'BCC' field. This resulted in anyone who was sent the email being able to see the names and email addresses of everyone on the list.

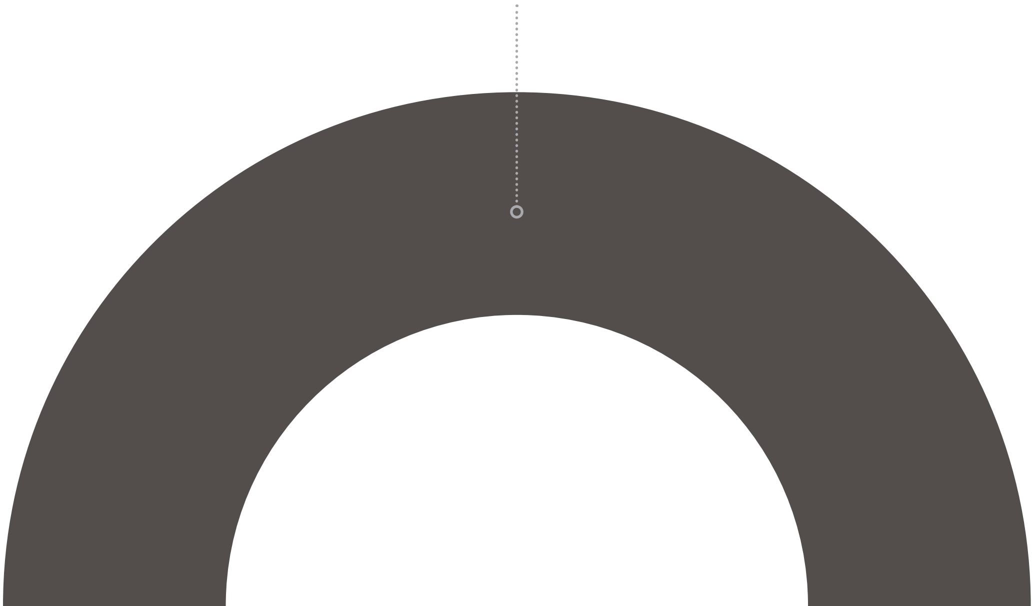
This caused much discomfort for many of those on the list. Some had not revealed their HIV status to anyone outside of the clinic, and feared that the breach could cost them their friends, partners or even their job.

The error, despite a rapid response from the clinic, was quickly picked up by the media and the clinic subsequently was at the centre of a media storm, with Alan McOwan, the Trust's Director for Sexual Health, being interviewed live by the news programmes from the BBC, ITV, Channel 4 and Sky. The story was even reported in newspapers in the US and Australia.

The clinic attempted to rectify the situation as soon as the mistake was discovered, apologised profusely and promised to address the issues internally. In this case the clinic had not recognised that the email addresses of their patients should have been classified as confidential data, and treated them accordingly.

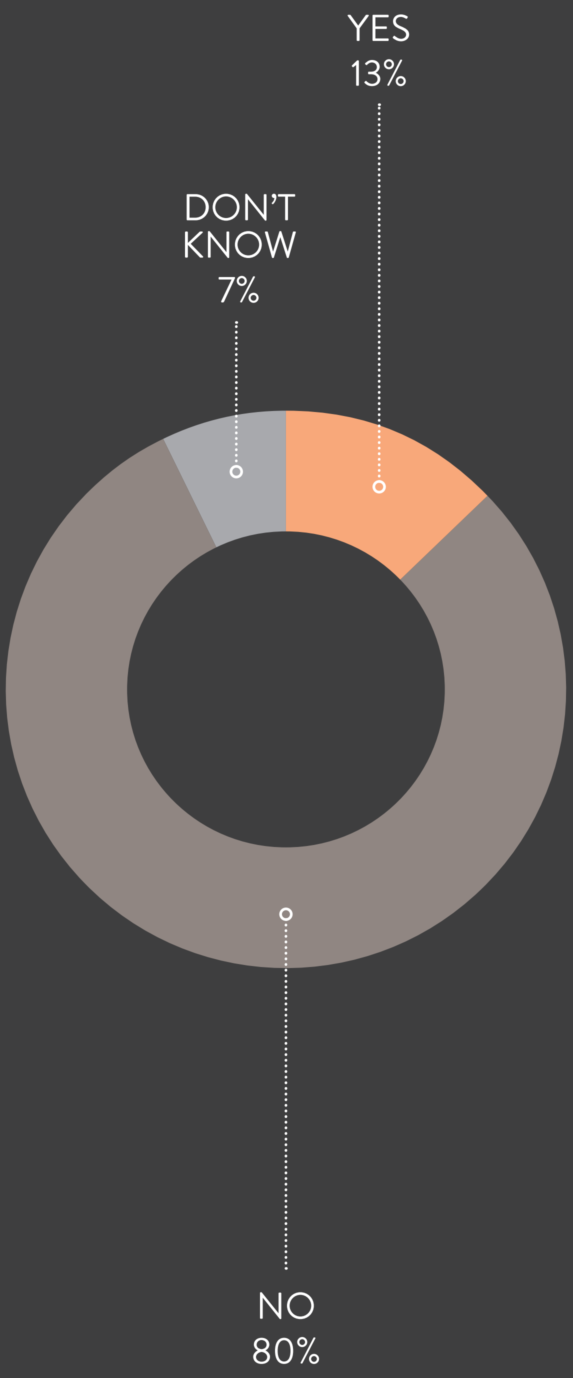
50%

OF THE WORST SECURITY BREACHES OF 2015
WERE CAUSED BY INADVERTENT HUMAN ERROR



DATA COMPROMISED BY CYBER ATTACK

Has your organisation ever had any data stolen, or been subject to a cyber attack?



Again, this result is an encouraging sign when compared to the private sector, where 38% of small businesses and 69% of large organisations suffered some form of attack by an unauthorised outsider in 2015. This low figure is likely due to a current lack of targeted attacks on the sector, as there is a perception amongst cyber criminals that whilst charities are probably lacking in security when compared to businesses, they also have little data of value worth stealing in the first place.

This is in stark contrast to the private sector, where even those who preach good security are targeted and can still be hacked. Verizon – a US telecoms company which also publishes an annual report on the state of cyber security – recently had a database of 1.5m customers stolen by a hacker and offered for sale on a closely guarded underground cybercrime forum for $100,000.

Worryingly, however, there is a change of emphasis from the illegal marketplaces on the 'Dark Web'. Whilst an individual credit card number may sell for as little as £1, a full medical record can fetch as much as £200. This has resulted in a significant increase in attacks on hospitals and healthcare providers in the US in 2015, with cyber criminals looking to exploit a lack of security to obtain valuable data. It is conceivable that the voluntary sector could also be targeted for attack, especially those that manage any form of medical data.

The variety of attacks reported by our respondents is in-line with what is seen within the private sector – namely ransomware, DDOS attacks, phishing attempts, viruses and malware and websites being hacked. Ransomware is an increasing problem, with the number of attacks reported in the UK in February 2016 alone being higher than that reported in the first six months of 2015.

Given the random nature of the majority of ransomware infections and the profitability they generate for cyber criminals (one attack in the US in 2015 netted the attackers over $1m), we expect to see more and more charities becoming victims.

DATA COMPROMISED BY CYBER ATTACK

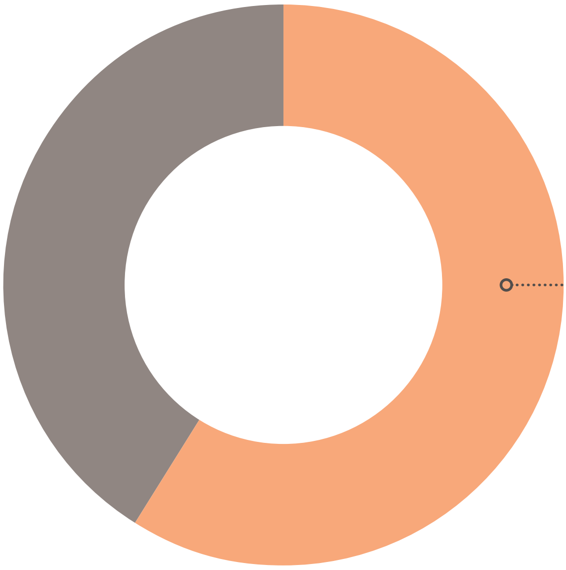
Case Study: The CALM Website Hack

On 24th July 2015 the website of CALM, the charity which exists to prevent male suicides in the UK, was attacked and defaced by unknown hackers. The attack was not believed to have been specifically targeted, displaying all the hallmarks of similar attacks on other businesses which appears to have exploited an unpatched vulnerability associated with WordPress software.

Whilst also defacing the website, the hackers potentially accessed the personal data of users of the website, which included their name, user name, email address, passwords, phone numbers and address.

Thankfully, any data relating to calls, texts or webchat to the support lines nor any financial information was accessed. Had the hackers accessed the personal data and understood it's significance, there could have been the potential for attempted blackmail of vulnerable people, as well as the usual risks of phishing attacks and identity theft.

CALM responded quickly and appropriately, issuing a warning to those affected and contacting the Police and the ICO, and the vulnerability within the website was fixed. The random nature of the attack shows that the approach of 'Why would anyone want to hack us?' is now inappropriate.

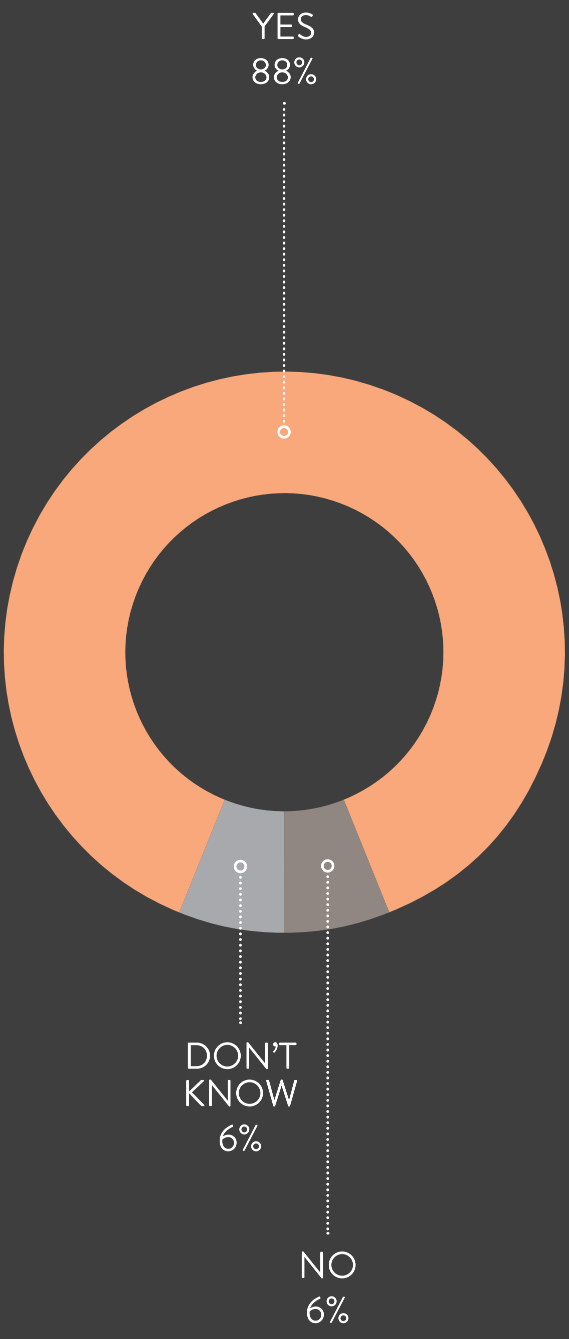


59%

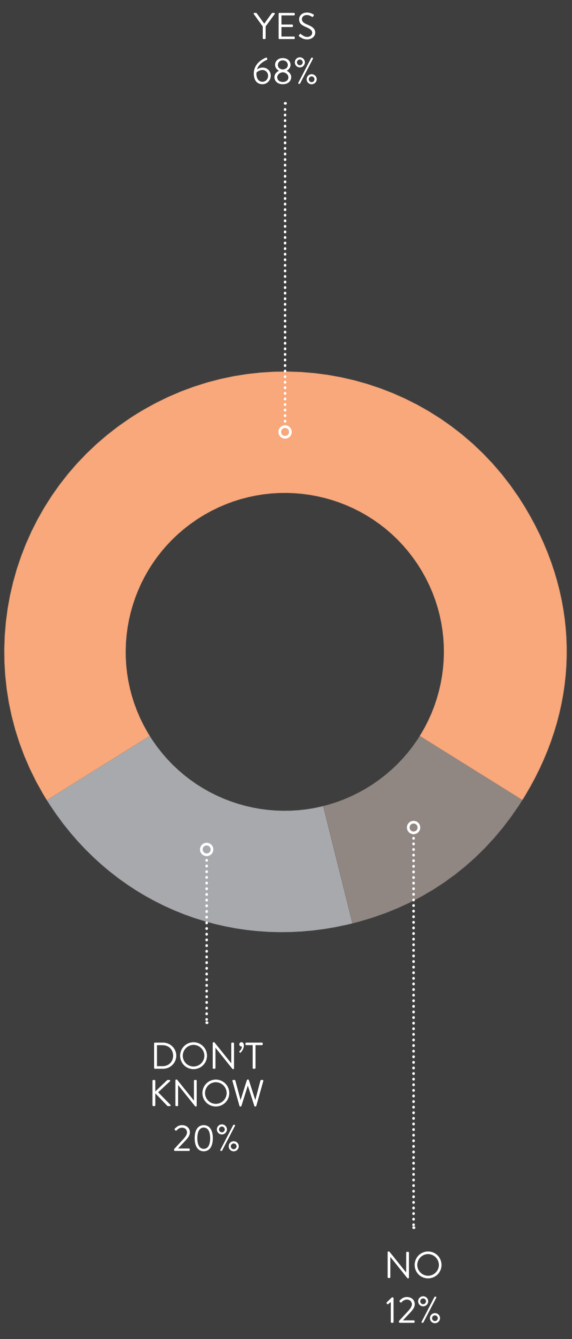
OF UK BUSINESSES EXPECT THERE TO BE MORE SECURITY INCIDENTS IN 2016 COMPARED TO LAST YEAR

REPUTATIONAL AND FUNDING IMPACT

Do you think the loss or theft of your data would have an impact on your supporter's opinion of your organisation?



Do you think the loss or theft of your data would have an impact on your current funding, or your ability to obtain funding in future?



REPUTATIONAL AND FUNDING IMPACT

This is in-line with what we see in the private sector. Whilst the PwC report does not cover the damaging effect of a security breach on consumer confidence, other sources indicate that up to 86% of customers would shun a business if they leaked their credit or debit card details, their home address or their phone number – this increased to 91% when the respondent was female. Given that studies show women are more likely to donate to charity than men, a security breach should be of grave concern to fundraisers.

Whilst larger charitable organisations could absorb some of the fallout it's conceivable that for smaller organisations a significant and public breach could severely impact donations, and possibly even force redundancies or closure. The incoming EU Data Protection Regulation will also likely have implications on how and when you must reveal your data loss to the regulators and the public.

The question on funding is perhaps unique to the voluntary sector. Currently there has not been any research to indicate whether banks or investors are less likely to fund businesses that have suffered a significant data loss or cyber attack, and from our work in the private sector it doesn't seem to form a part of the decision-making process on whether to fund or not – at least, not yet. However, given the very different sources of funding available to charities there is a significant risk of a downturn in income after a breach.

Not only is there the impact of donors deciding to channel their money into other charities (or even away from the sector completely) should you lose their data, there's an ongoing movement within government to force organisations that it funds into becoming more secure. There are already restrictions in place on certain central government contracts that stipulate at least Cyber Essentials accreditation for bidders, and this is likely to be extended over the coming years to any organisation which is directly or in-directly funded by a public body. We're also likely to see large businesses adopting a similar position in future with their third party suppliers, and this could well extend to charities in receipt of donations or grants from large businesses.

Reputational damage is one of the reasons why data protection and information security need to considered as a business risk, not an IT problem. Whilst your IT provider, whether in-house or an external third party, can – and should – be providing your organisation with the technology to help prevent security breaches, it is important to remember that these are only tools.

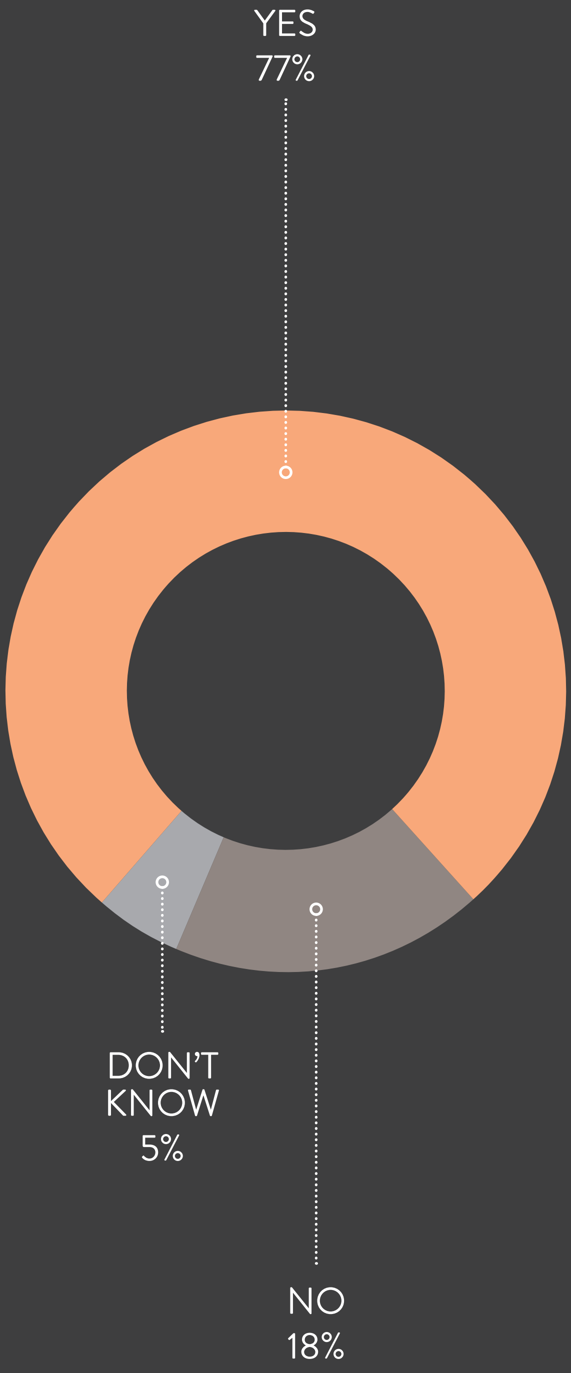
For your organisation to minimise the risks you need to not only make sure the tools are in place, but that your staff and volunteers know how to use them. Creating a culture of security goes a long way to preventing an embarrassing data loss.

£380,000

IS THE ESTIMATED AVERAGE COST OF REPUTATIONAL DAMAGE FROM A CYBER ATTACK

TRAINING IN INFORMATION SECURITY

Have you trained any of your staff on the importance of protecting information?



Taken at face value this result would seem to show that the sector is leading on providing training on information protection, with a better result than large (72%) and small businesses (63%). However, the results may not be directly comparable as the PwC survey asks about ongoing information security awareness training, whereas we have only asked if any training has been given.

This is an important distinction. The cyber threat environment is constantly developing, and attacks which were prevalent a few years ago have dropped out of favour to be replaced by new techniques. Whilst the vast majority of us would instantly recognise an email purporting to offer us millions of dollars in exchange for our bank account details, rather significantly less of us identify the threat of an email claiming to be from Amazon or our bank asking us to open the attachment to view our invoice, or click on the link to verify our details. Whilst the scam itself is almost as old as civilisation itself – variants of the 'Nigerian 419' con have been around since at least the Sixteenth century – the techniques and technology used to defraud us of our money have constantly evolved.

Most organisations we have seen in the sector provide a single, brief introduction to information security – usually through a short introduction on data protection when an employee starts. Whilst acceptable ten years ago, this is now a completely inadequate preparation for today's multi-threat environment. If possible, we would recommend an annual refresher for all staff and trustees (and volunteers too, if they are able to access confidential information). This could take the form of an online course, although bringing in a qualified trainer is always preferable. In phishing tests in the private sector, staff are always significantly better at detecting suspect emails after having a face-to-face training session when compared to an online course.

Do your people know what to do if they receive a suspicious email? Are all your PC's locked when the user is away from their desk? Are all laptops left secured? Are there no papers left unclaimed on the printer when you leave at night? Are visitors always escorted around your offices? If you answer 'no' to any of these questions, you should look at developing your security awareness training.

TRAINING IN INFORMATION SECURITY

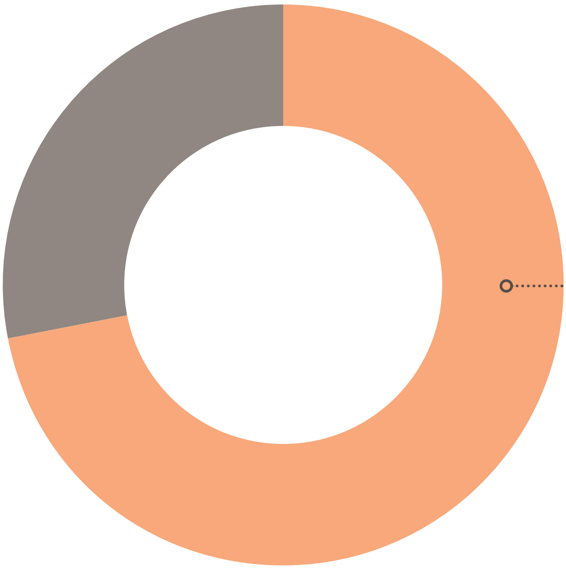
Case Study: Alzheimer’s Society

In January 2016 the ICO issued an Enforcement Notice on the Alzheimer’s Society, in response to two separate security breaches. Whilst one related to an attack on their website, the second regarded 15 volunteers who were using their personal email addresses to share information about people who use the charity, were storing unencrypted data on their home computers and were failing to keep paper records locked away. None of the volunteers, who were recruited in 2007, had received any training on handling sensitive data.

Combined with previous incidents, the ICO has warned the charity it could face prosecution if the Enforcement Notice is not complied with.

The Alzheimer’s Society has stated that it is committed to complying with the Notice, and it is confident that no personal data has passed into the wider public domain.

Training on data protection is now mandatory for all volunteers who have access to personal data.

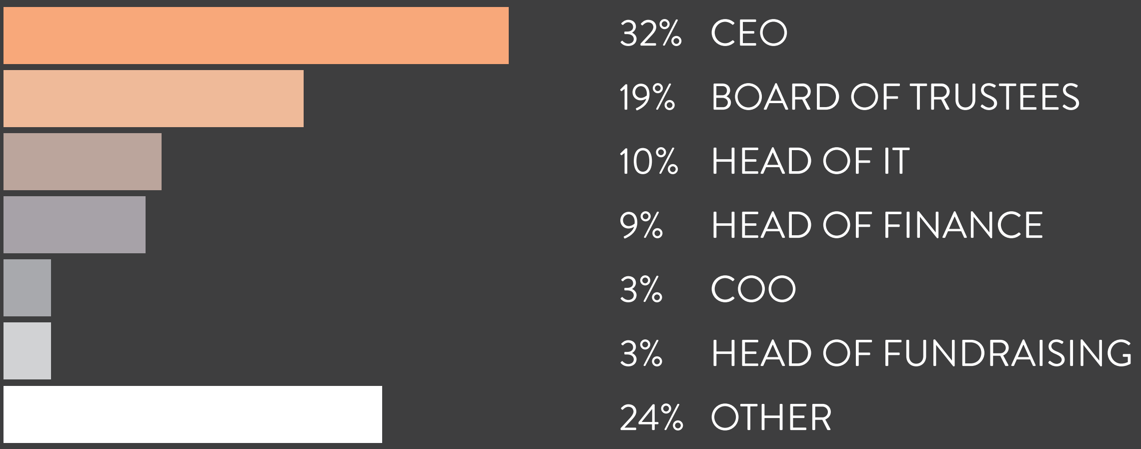


72%

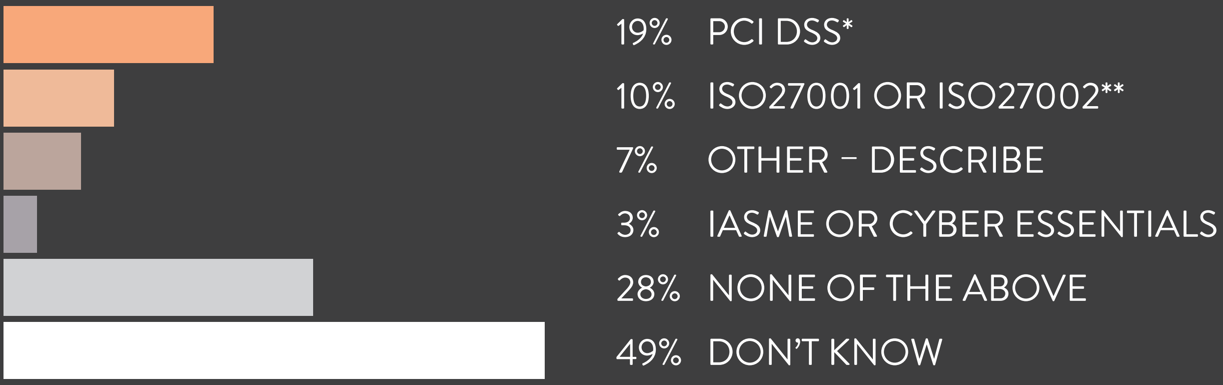
OF COMPANIES WHERE THE SECURITY POLICIES ARE POORLY UNDERSTOOD HAD STAFF-RELATED SECURITY BREACHES IN 2015

COMPLIANCE & STANDARDS

Who is responsible for ensuring your organisation is compliant with legislation such as the Data Protection Act?



Is your organisation compliant with any of the following security standards? Chose all that apply.



* PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

** INFORMATION SECURITY MANAGEMENT SYSTEM / CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

COMPLIANCE & STANDARDS

Having over 50% of organisations placing responsibility for compliance with data protection legislation with the senior management is a very encouraging sign, as traditionally security was seen as a technology problem that sat squarely within the IT Department. After all, your IT experts can tell you how to utilise the features of Microsoft Word, but they can't tell you how to write the novel.

Nowadays we encourage organisations to think of information protection as a risk to be managed centrally, rather than having it spun off to a section of the business. After all, should the worst-case scenario occur it isn't the Head of IT who is being interviewed on live TV, or being called to explain a breach to the ICO.

The organisations which are most effective at protecting their data understand that the drive to become secure comes from the top, where everyone from the CEO and Board of Trustees to the cleaners understand and – most importantly – adhere to the policies and procedures designed to keep confidential data out of the wrong hands. If you can embed a culture of security within your corporate identity, you will go a significant way towards reducing your overall risk.

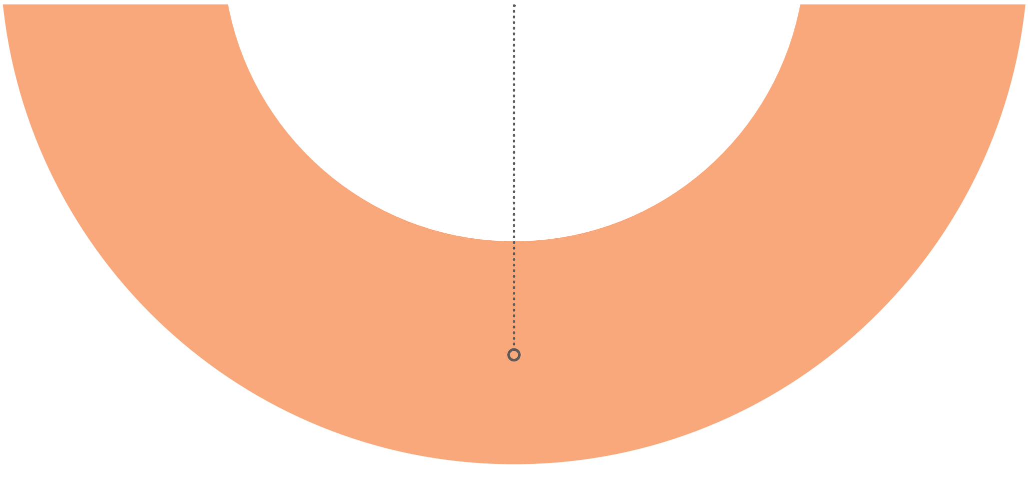
Not only will your people be more effective in protection techniques, the hackers and cyber criminals are less likely to target you in the first place – the reason why joyriders steal older cars is because they are significantly easier to break into than more modern types with the latest security features.

Less encouraging, however, is the lack of charities which have attained a cyber security accreditation. Whilst PCI DSS is mandatory for any organisation which processes even a single credit card, the others are (currently) optional. Whilst the various ISO accreditations are very comprehensive and can be a drain on resources, they should be the de facto standard for larger charities. For smaller ones, Cyber Essentials or Cyber Essentials Plus is an ideal start to introduce the basic of data security within your organisation.

Cyber Essentials requires the organisation to complete a self-assessment questionnaire, with the responses independently reviewed by an external certifying body, whilst with Cyber Essentials Plus the external certifying body undertakes tests of your systems, using a range of tools and techniques. Both are designed to offer protection from the most common cyber threats, whilst being affordable for even the smallest of organisations.

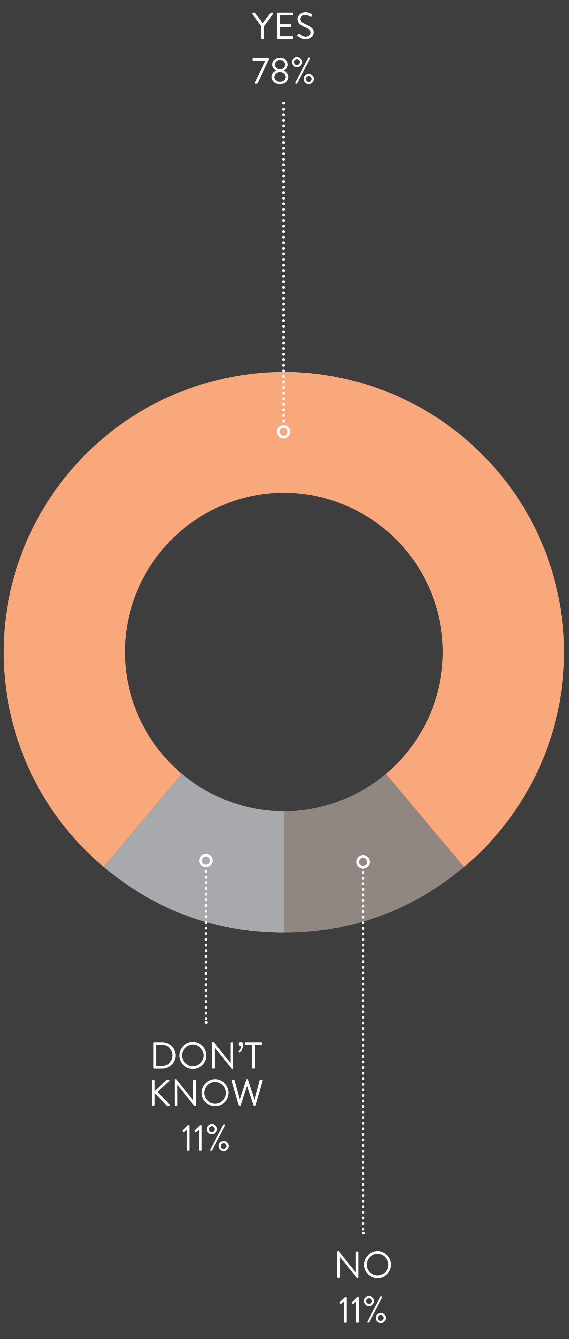
49%

OF UK BUSINESSES ARE ON THEIR WAY TOWARDS CYBER ESSENTIALS ACCREDITATION OR ALREADY ACCREDITED

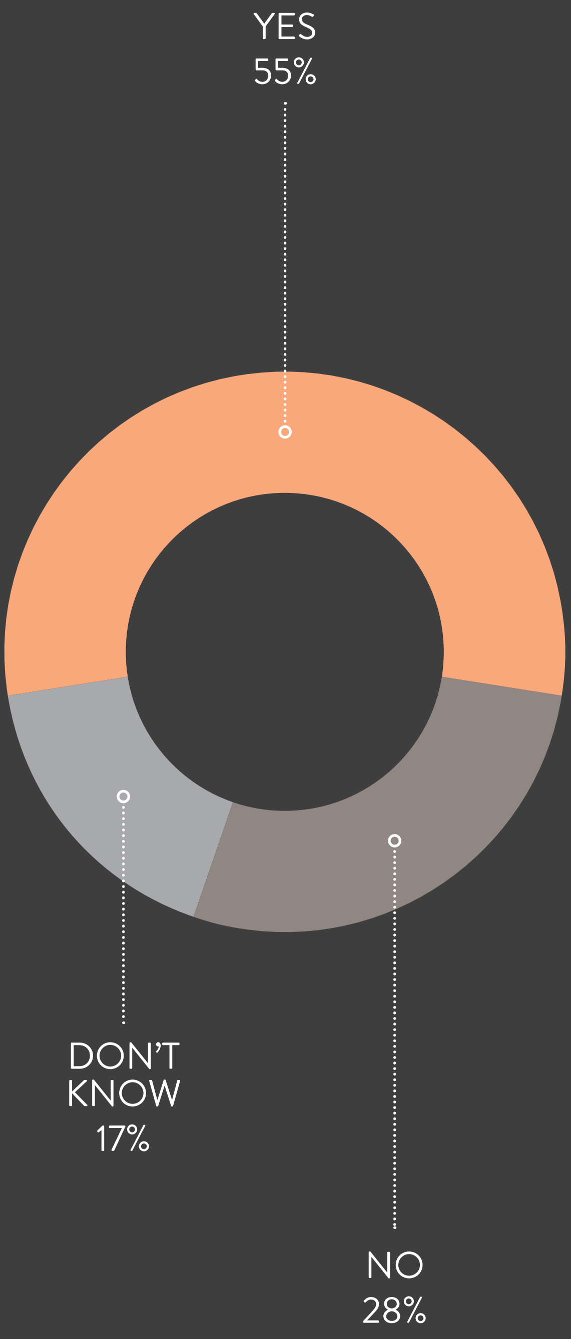


STRATEGY & RISK MANAGEMENT

Does information protection form a part of your risk management processes?



Does your organisation have a defined information protection strategy?



STRATEGY & RISK MANAGEMENT

As with the responses to the data protection training question the figure of 78% of charities factoring in information protection as part of their risk management processes is encouraging – this compares well to 68% of businesses. However, further research would be required to understand whether the quality of that risk management is acceptable, or whether it falls as a simple checkpoint within the overall risk management strategy.

Many organisations fail to understand where their confidential information is, how it is used and accessed, and what level of protection is required. We've worked with companies who have spent tens of thousands of pounds on protecting their email systems, ensuring that they have a 99.9% uptime, where the actual cost of losing access to that system for two to three days is minimal. Equally, we've seen businesses spend little to no money on protecting their sales systems, even though losing it for half a day could cost thousands.

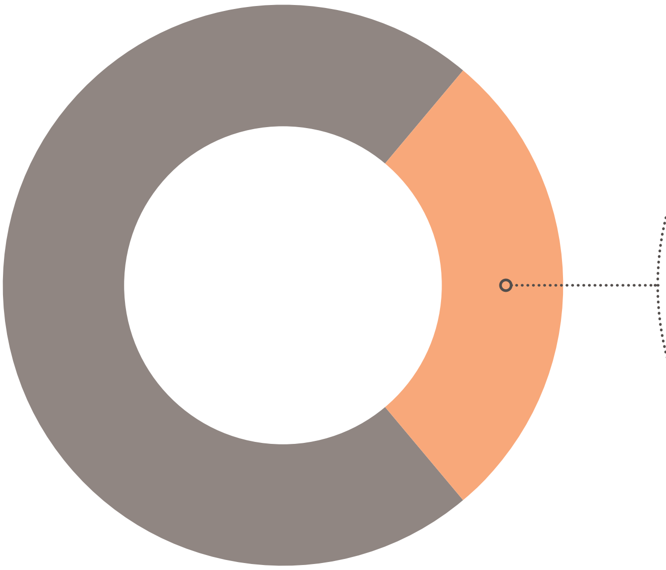
Most organisations do not understand how reliant they are on their computer systems and data until the unthinkable happens – and by then, it's too late. We recommend running regular Business Impact Assessments as part of your risk management processes, so you can recognise where your strengths and vulnerabilities are. Being armed with this knowledge will enable you to make smart decisions on how and when you spend money on protecting your valuable data.

The most worrying of all the results of this survey is discovering only 55% of charities have a defined information protection strategy.

This should be the foundation of all your data protection activities, as it defines your attitude and appetite to cyber security risks, describes how and when you will educate your employees and volunteers, provides them with the policies and procedures they need to be able to undertake their work effectively but securely, and gives everyone a clear understanding of the risks posed by handling sensitive data, as well as the consequences for failing to follow the guidance.

Organisations that are effective in protecting data understand that security is more about putting the right culture in place, where there is a continual cycle of improvement and 'marginal gains', than it is about one-off purchases of expensive technology.

This gives your senior management and Board of Trustees the confidence that the whole organisation is working towards a more secure environment, enables them to see where funding on security technologies should and shouldn't be spent and provides a framework within which your supporters and donors can be confident you are treating their personal information responsibly and securely.



28%

OF THE WORST SECURITY BREACHES OF 2015 WERE PARTLY CAUSED BY SENIOR MANAGEMENT GIVING INSUFFICIENT PRIORITY TO SECURITY.

INFORMATION PROTECTION

Top Ten Tips For Organisations

01

Create and regularly review your information protection strategies and procedures and work towards attaining ISO 27001 or Cyber Essentials accreditation.

02

Make sure all within the organisation, from the cleaning staff to board members, adhere to the policies and procedures – good security practice comes from the top.

03

Identify where your confidential information is held – both physically and digitally – and regularly review who can gain access to them.

04

Training staff in how to protect information is a vital tool. Technology alone cannot prevent security breaches.

05

Make sure any third parties you share confidential information with are aware of the need to protect your data – make this a contractual obligation if necessary.

06

Use secure technologies to share information, such as encryption, a Virtual Private Network or Private Cloud storage, to help mitigate against staff using vulnerable methods.

07

Create an Information Protection function within the organisation for dealing with security issues.

08

Most security breaches come from within, mainly due to accidental mishandling of confidential information. But be aware of malicious insiders as well – If Edward Snowden can steal the NSA's secrets, then your staff can steal your data too!

09

Consider taking out cyber liability insurance. Many insurance companies now offer a range of benefits such as cyber forensics and public relations advice, as well as insuring against financial loss, regulatory fines and brand damage.

10

For further help and guidance, come and talk to us.

TESTIMONIALS

“Protective Intelligence helped us add value to our ISO27001 certification, by developing a tailored Information Security Awareness training programme for all staff. They delivered a bespoke solution which highlighted that Information Protection is a ‘Whole Business’ problem, and is not just IT-related. Recent and relevant examples on information breaches were incorporated in the training to get the messages across.

They demonstrated the value of our information, both from a business and personal perspective, and highlighted how it could be compromised.

They reinforced the secure framework in which to operate and to reduce the threat of cyber-attacks and intrusions. In fact, several members of staff remarked that it was one of the most valuable training programmes they had ever attended.”

MARK COLLINS
DIRECTOR OF FINANCE
PICKER INSTITUTE EUROPE

“We used Protective Intelligence to help us develop our in-house Security Awareness Training Programme. They delivered bespoke training packages that were tailored to the specific needs of a wide range of roles — such as specific Social Engineering courses for Reception staff and password protection training for countries where working practices were inconsistent with our desired approach. They also evaluated our online training content, and advised where changes could be made, as well as holding Security Awareness Workshops and Drop-Ins, where they passed on their knowledge of current security threats, allowing staff to understand how best to protect themselves and our company from increasingly sophisticated cyber attacks.”

ANDREW MORRIS
INFORMATION SECURITY SPECIALIST
DIAGEO

“Protective Intelligence helped us develop our Information Security Strategy, bringing their expert insight in cyber security threats and delivering a well packaged product that has enhanced the information security processes and policies of our business. Through working closely with us to understand our environment and ethos, they have developed a security strategy that is tailored to our needs, allowing us to protect our data without compromising our ways of working.

We now see Information Protection not as a barrier to business, but as a vital mechanism which allows us to safely operate in today’s environment.”

TAREK MARJI
VICE PRESIDENT, INFORMATION SECURITY
POINT 72 ASSET MANAGEMENT

THE CORNER HOUSE
24 NORRIS ROAD
UPPER ARNCOTT
BICESTER
OXFORDSHIRE
OX25 1NZ

+44 (0)1869 247814
info@protectiveintelligence.co.uk

protectiveintelligence.co.uk