The currency of cyber trust

Your customers' attitudes towards cyber security

Your report into cyber security in the UK today and the data behind our Digital Vision for Cyber Security

Atos

Contents

We surveyed over

3,000

UK consumers who use Britain's businesses and public services every day

Foreword

Half of all UK organisations fell victim to a cyber attack in the 12 months leading up to April 2017, according to **UK Government Data**. A quarter of those suffered a temporary loss of files, a fifth had software or systems corrupted, one in ten lost access to third-party systems they rely on and one in ten had their website slowed or taken down altogether.

In the digital age, cyber security is critical to safeguarding businesses, public service providers and consumers alike. What's more, given recent high-profile cyber attacks, cyber security is on the public's radar more than ever before. For organisations, this presents a challenge: how to keep customers secure and make them feel secure in order to win and retain their trust.

We wanted to deepen our understanding of consumer trust and expectations when it comes to cyber security. Is there now more pressure on organisations to do more to protect systems and data? And how can organisations keep their customer base loyal in the event of a cyber attack?

We undertook independent research to help inform UK organisations on how to win and retain the 'cyber trust' of their customers. We surveyed over 3,000 UK consumers who use Britain's businesses and public services every day.

We asked them about their attitudes to cyber crime, what they would expect from organisations when it comes to keeping their data safe and what technology they would like to see more of.

This research is summarised within this report and complements our **Digital Vision for Cyber Security**, which combines contributions from subject matter experts both within Atos and from other leading organisations to examine the fast-evolving threat landscape and what steps businesses must take to ensure they're protected.

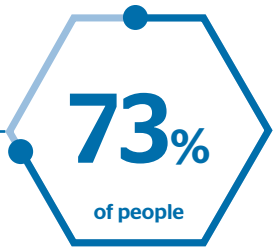
Summary of findings

Perceptions and awareness

Consumers are more aware of cyber threats, with 73% aware of global cyber attacks and 63% saying recent attacks have made them more aware of cyber security as an issue that may impact their daily lives.

Cyber trust is decreasing, with only 13% saying their trust in organisations has increased in the last two years and 38% saying they do not trust organisations with their data.

Communication about cyber security is important for trust, with 58% not sure they would trust an organisation after an attack and 82% saying they expect an organisation to inform its customers in the wake of an attack.



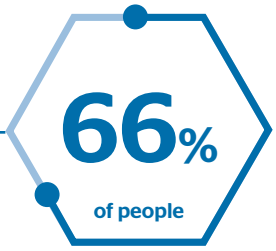
are aware of global cyber attacks

Responsibility and accountability

Consumers want to see more accountability, with 69% agreeing that organisations should be fined in the event of a breach and 80% agreeing that organisations should be more accountable in the event of an attack.

Consumers recognise individual responsibility for cyber security, with 87% agreeing that individuals need to take responsibility for keeping their information safe and 85% agreeing there is room for people to take their responsibility more seriously.

Despite awareness, there is a lack of understanding and proactivity, with only 24% taking active steps to stay informed, 40% admitting they don't take any steps to protect themselves and of this 40%, over half (52%) say this is because they don't know how to protect themselves.



expect organisations to fully protect their customers

Customer choice and experience

Consumers want more rigorous cyber security, with 58% saying that cyber security is a reason to choose an organisation and 66% expecting organisations to fully protect their customers.

There is a willingness to go through more cyber security steps, with 56% willing to compromise their experience for better security, 66% happy to compromise on the speed of a service and 59% happy to compromise on the complexity of logging in.

Consumers want more innovation, with 67% saying they would trust an organisation more to know it was investing in advanced technology, 52% saying there needs to be more human intervention and 69% saying more innovative technology is needed to maintain cyber security.

What tech disrupters and cyber criminals have in common is understanding the power and value of other people's digital data. The first step for any Board is therefore to understand their organisations own data, to define what they care about most, and to understand the rapidly changing nature of the threat. From this platform, they can make sensible risk judgements and spend proportionate amounts on securing their networks.

Robert Hannigan
Advisor to BlueVoyant LLC

Chapter 1:

Trust in the digital age

Public awareness of today's cyber security threats has grown and trust is seen to be decreasing. High-profile incidents have alerted consumers to the potential consequences of their personal information falling into the wrong hands and there is a perception that the cyber threat is growing.

Cyber security awareness

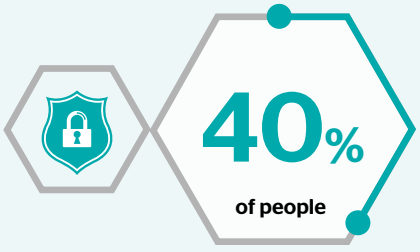
Looking at levels of awareness of cyber attacks, 73% of respondents say they are aware of global cyber attacks and 63% say recent cyber incidents have made them more aware of cyber security as an issue that may impact their daily lives.

66% feel the threat of cyber attacks on organisations has changed over the past 12 months, with 47% saying that they feel the level of risk to them personally suffering a cyber attack has increased compared to 12 months ago (and 23% unsure).

Perceptions are that the cyber threat is still growing, with 59% of respondents admitting they are concerned that a cyber attack will have a significant impact on their life in the next 12 months.

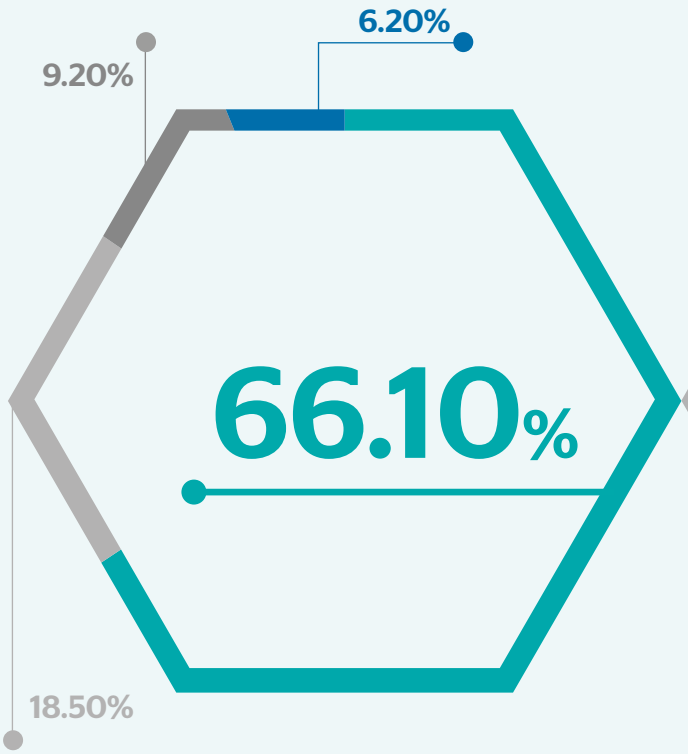
When it comes to being affected by cyber attacks today, 50% of those affected say they have experienced phishing attacks. This is the most common threat that consumers have experienced, followed by malware viruses (30%) and data breaches (25%).

However, there are still gaps in cyber security awareness, with some respondents unaware or confused about threats today. 15% say they are not aware of any cyber attacks and 1 in 10 don't know if they have been affected by a cyber attack.



don't proactively protect themselves from cyber threats, despite high profile global attacks

Do consumers think the threat of a cyber attack happening to an organisation has changed over the past 12 months?

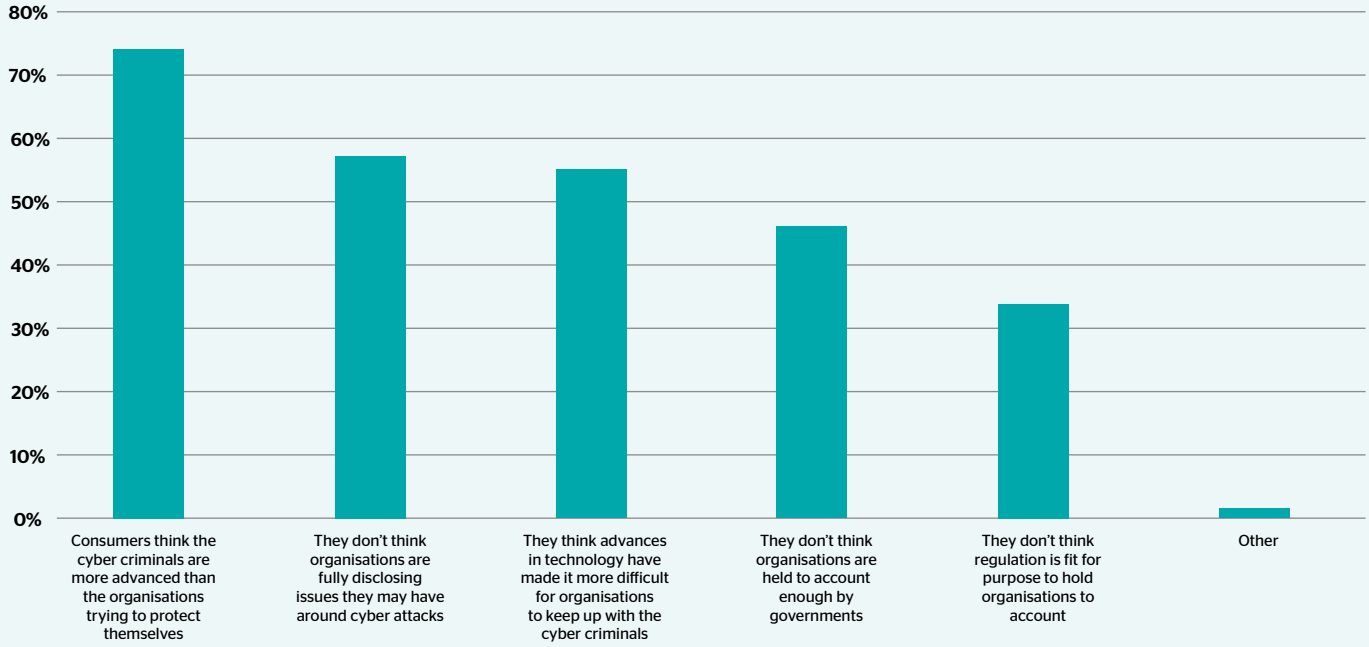


- **Yes, the threat has grown**
- No, it's stayed the same
- Not sure
- Yes, the threat has decreased

63%
of people

say recent cyber incidents have made them more aware of cyber security as an issue that may impact their daily lives

Why has the level of trust consumers have for organisations decreased?*



* Please note, respondents were asked to tick all that apply

Public trust in organisations

Levels of public trust in organisations are decreasing, with only 13% of respondents saying that their trust in organisations has increased in the last two years. Almost a third (30%) say that their trust in organisations has decreased in the last two years, with almost three quarters (74%) of those citing that the reason their trust has decreased is because cyber criminals are more advanced.

Sharing personal information is a concern, with 38% of respondents admitting that they do not trust organisations with their personal data.

Looking at perceptions of different types of organisations, respondents believe those able to protect themselves most were financial services and banks (25%), then defence (22%) and then government (21%).

Feeling reassured about cyber security is linked directly to trust in organisations. When respondents were asked to cite why they perceive certain organisations to be their most trusted brands, 53% say that the biggest reason is that every time they log on, they go through a rigorous security process that reassures them. Similarly, 49% said the reason they trust their chosen organisation is that they have never had any security issues with it before, while 47% stick to organisations they believe to be more secure.

When it comes to identifying the areas of their lives that are at the highest risk from a cyber attack, these are financial services (39%), personal details and identity (24%) and police and national security services (15%).

say their trust in organisations has decreased

say the biggest reason they perceive an organisation as a trusted brand, is that every time they log on, they go through rigorous security process

Perceptions in the event of an attack

Looking at perceptions and attitudes towards organisations in the event of an attack, trust can be difficult to win back once an organisation has been hit.

58% of respondents are not sure if they would trust an organisation after it was hit by a cyber attack. Only a quarter (25%) say that they would still trust an organisation after it was hit by an attack.

In the event of an attack, consumers want reassurance and they want to see action. In order for an organisation to regain their customers' trust after an attack:

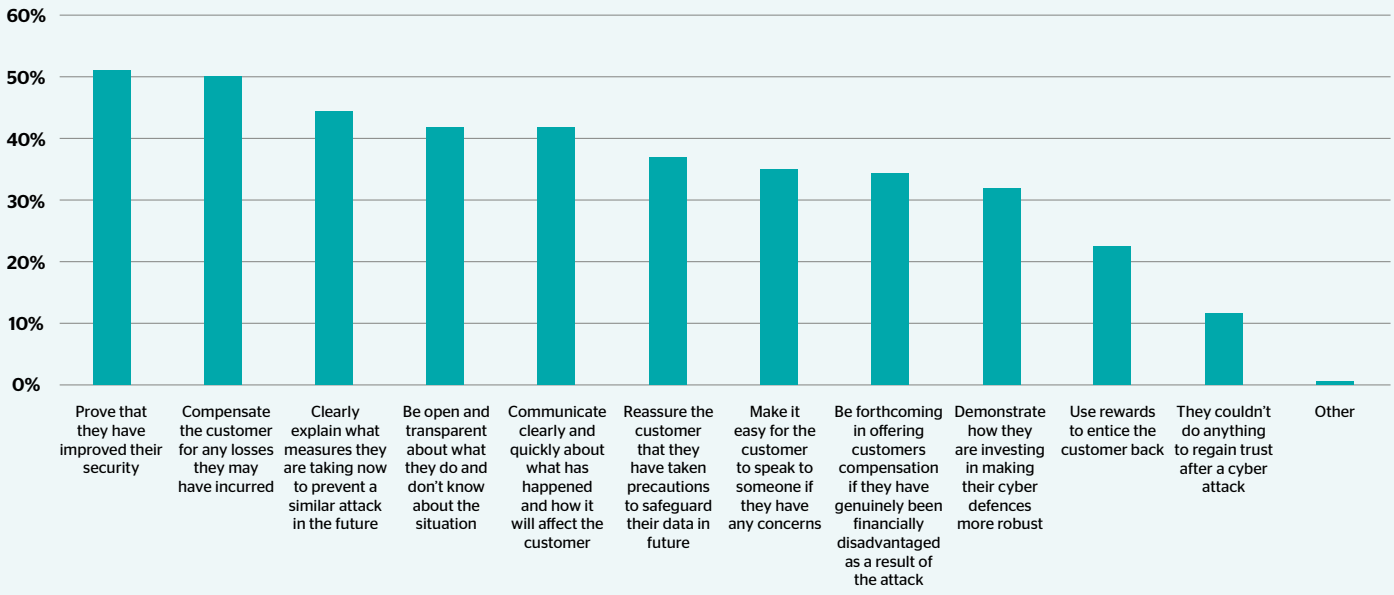
- 52% say that organisations would have to prove they had improved their security procedures and learned from their mistakes
- 45% say it's about clearly explaining what new measures are in place to avoid any future attacks
- 32% say the most important thing is how quickly they communicate about what happened and its effects.

These answers differed between age groups, with older respondents expecting more from organisations than younger age groups:

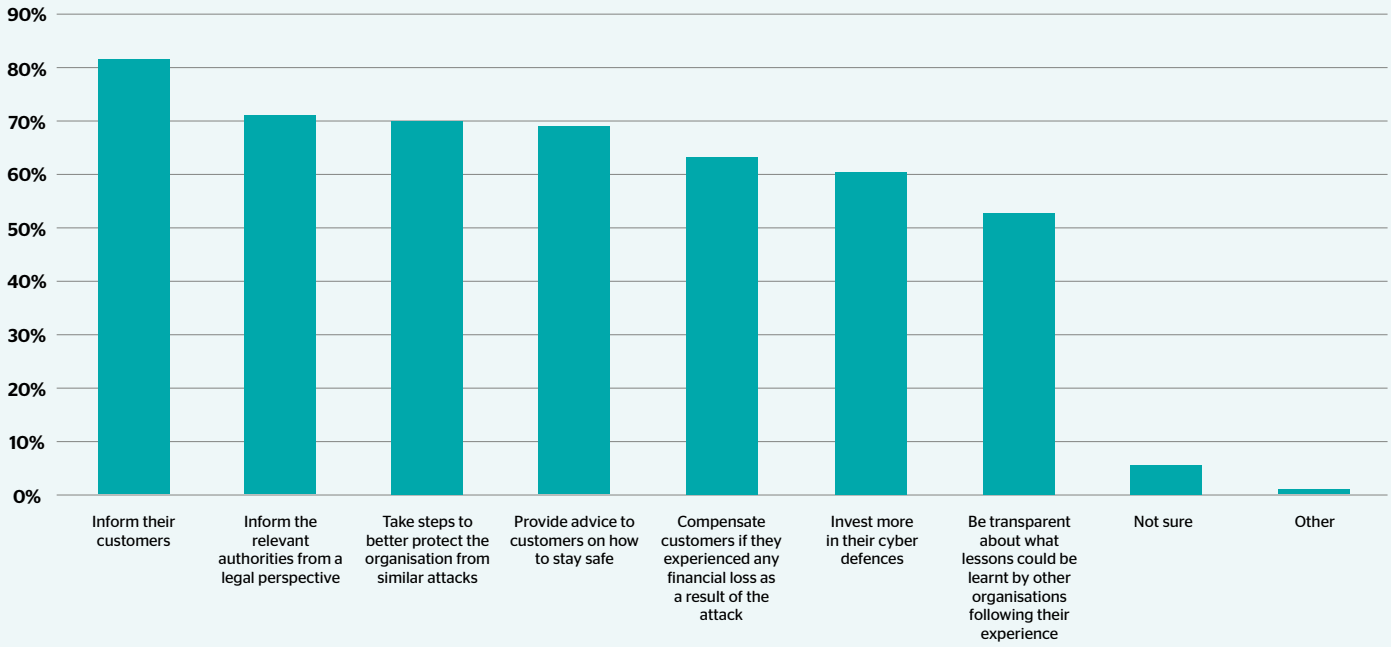
- 44% of 16-24 year olds say organisations should prove that they have improved security compared to 62% of 55+ year olds
- 24% of 16-24 year olds say organisations should explain what measures are in place compared to 46% of 55+ year olds.

In any case, what consumers want most of all is openness, communication and transparency. In the event of an attack, 82% of respondents say they expect an organisation to inform its customers and 71% say they expect an organisation to inform the relevant authorities.

What would an organisation need to do to regain the trust of its customers after a cyber attack?



If an organisation suffers a cyber attack, what would its customers expect the organisation to do once they are aware the attack has taken place?



Cyber security is another dimension of customer-centricity. You need to factor it into the way you design services and engage with your customers. This is as much about credibility as technology; and it's a great opportunity to build trust in your brand.

Defining the right security framework is about balance to avoid over investing in some areas while preventing gaps in others that could prove costly. There is also a fine balance between security measures that are convenient enough to keep customers happy, but safe enough to protect your business and reputation.

Being secretive about cyber security does not work. Increased security without increased user awareness is a missed opportunity. Customers will use services more if they think they're secure and they'll be more tolerant of cyber security measures if they understand them.

Phil Aitchison
Head of Cyber Security & Mission Critical Systems, Atos UK&I

Chapter 2:

Helping customers to help themselves

While individuals place a lot of accountability on organisations to be secure, they also believe they should take responsibility for their own cyber security. However, levels of proactivity in staying informed and protected are low in comparison to perceived levels of security-consciousness.

Risk and responsibilities

When buying something online or signing up to a new service, 52% of respondents feel that the responsibility lies with the organisation holding their information to keep personal data safe online, with 80% agreeing that organisations should be more accountable in the event of a cyber attack or breach:

- 67% think the government should take more responsibility in helping organisations and individuals to stay secure and keep their information safe
- 77% think we need more regulation around cyber security for organisations to take it seriously.

There is also a personal responsibility to consider. While 87% of respondents say greater awareness has made them more security conscious, 87% of respondents agree that individuals need to take responsibility for keeping their information safe online, and 85% agree there is room for people to take responsibility more seriously.

Active steps to stay informed

While there are high levels of security consciousness, this does not translate into the same levels of proactivity.

When asked whether they take any active steps to stay informed about the latest cyber security risks, 24% of respondents said they make a point of staying informed regularly, 61% of respondents admit that they do not actively stay informed about the latest cyber security threats and 15% say they do not take any steps at all to stay informed:

- 42% admit that the reason for this is because they don't know how to stay informed
- 22% say they do not have enough time
- 14% say cyber security is not a big enough issue to stay informed.

Do consumers take any active steps to stay informed about the latest cyber security risks?

- **Not actively, but when they see information or news around cyber security they sometimes read it**
- Yes, they make a point of staying informed
- No, they don't take any steps at all

67%
of people

think the government should take more responsibility

77%
of people

think we need more regulation around cyber security

Active steps to stay protected

Levels of proactivity to stay protected are also relatively low. When asked about the practical steps to proactively try and protect themselves from cyber threats, 40% of respondents admit that they do not take any active steps, with over half (52%) citing the reason for this is that they do not know how to protect themselves.

Levels of proactivity are higher in older respondents. 50% of 16-24 year olds admit they don't take any practical steps, compared to 40% of 55+ year olds. Yet education and awareness are lower in the older age groups, with 40% of 16-24 year olds admitting that this is because they wouldn't know what steps to take, compared to 59% of 55+ year olds who cited the same reason.

Similarly, 32% of 16-24 year olds admit it is too much of a hassle to proactively try to protect themselves, compared to just 7% of 55+ year olds.

The most popular practical steps that consumers take to protect themselves are:

- Installing the latest anti-virus software (77%)
- Being more conscious when opening emails and attachments from unknown sources (72%)
- Running software updates as soon as they are available (68%).

Over a quarter of respondents (28%) feel that because they haven't had an issue with cyber threats, they have not had a reason to protect themselves. This does change when people are hit by a cyber attack, however, at which point:

- 56% reset their passwords
- 36% run regular updates when prompted
- 30% become more reluctant to share personal data online.

Do consumers take any practical steps to try and protect themselves from cyber threats?*

* In this context, 'cyber threats' refers to any kind of breach or issue caused by an attacker.

The role of regulation

From the data, consumers appear to support the EU General Data Protection Regulation (GDPR):

- 85% agree businesses should report data breaches to the authorities within 72 hours of the event taking place
- 69% agree businesses should be fined 4% of annual global turnover or €20 million (whichever is greater) if they aren't compliant with the regulation
- 80% agree when an organisation's core business involves processing personal and sensitive data, they should appoint a data protection officer to manage it
- 83% agree organisations need to ask for its customers consent when collecting data
- 84% agree organisations must delete its customers data if they no longer want them to have it
- 80% agree businesses should implement privacy risk assessments to ensure they are compliant when dealing with personal information
- 83% agree all organisations who deal with personal information should be liable for protecting it, from data processing to data control.

61%
of people

admit they do not actively stay informed about the latest cyber security threats

50%
16 to 24 year olds

admit they don't take any practical steps, compared to 40% of 55+ year olds

Cyber security is a partnership between you and your customers, to protect your systems at the back end while preventing customers being hacked at the front end. As well as investing in end-to-end cyber security, you need to raise awareness of customer responsibilities and best practice.

Customers are more likely to accept more security measures if their digital experience is well designed. But they need to understand the benefits to them and they may need your guidance for that.

Cyber security education must be integral to customer experience, especially given prevailing knowledge gaps and poor practices that increase vulnerability. All sectors need to do more, with the introduction of GDPR providing a key opportunity for educating and communicating with customers.

Sandy Forrest
Client Executive, Cyber Security, Atos UK&I

Chapter 3:

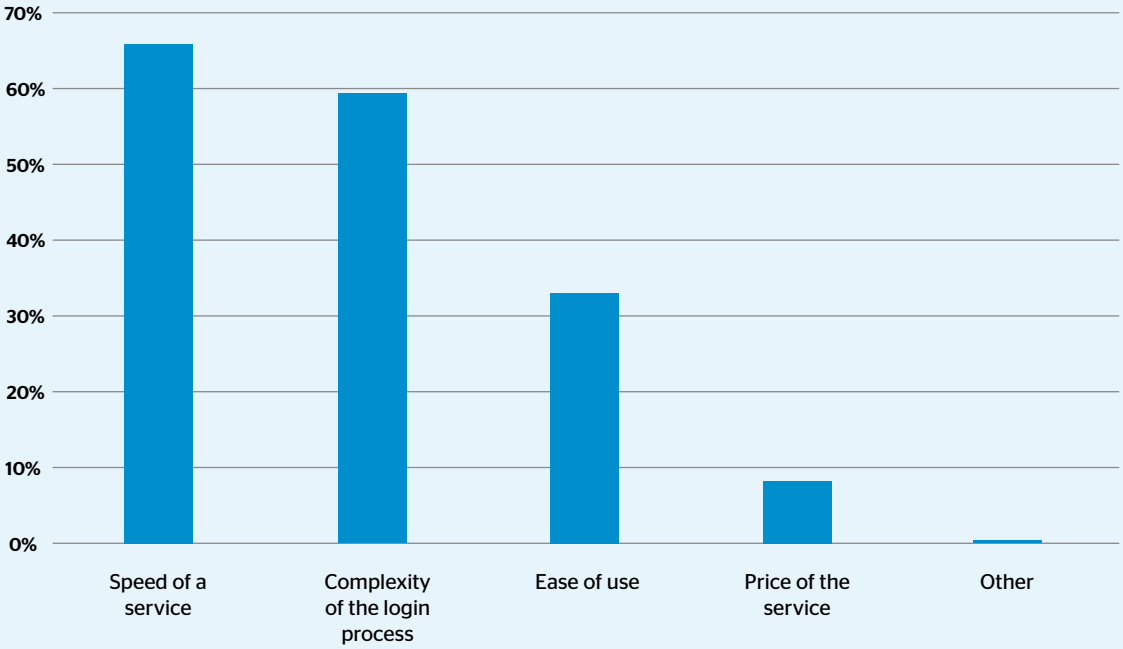
Understanding the value of cyber trust

With levels of trust falling and awareness of cyber threats growing, cyber security is increasingly a deciding factor when consumers are choosing which organisations to interact with. There is also some readiness to trade speed and simplicity for improved cyber security.

Cyber security as a differentiator

When looking at the deciding factors in choosing a particular organisation or a service, over half of respondents (58%) say that cyber security is a deciding factor. In recognition of the need for cyber security, there is some readiness to make a trade-off in exchange for more rigorous measures.

What would respondents be willing to compromise?



When looking at what consumers would compromise on for the sake of increased cyber security:

- 66% say they would be willing to compromise on the speed of a service
- 59% say they are happy to compromise on the complexity of the login process
- 56% say they are willing to compromise the user experience for better cyber security, while less than a fifth (17%) say they are not willing at all to compromise on user experience
- Only 8% say they would be willing to compromise on cost for better cyber security

In the interest of enhanced security, would respondants be willing to compromise any element of the user experience (such as have a slower login or purchase process) when using online devices?

58% of people say that cyber security is a deciding factor when choosing a particular organisation or service

Technology and innovation

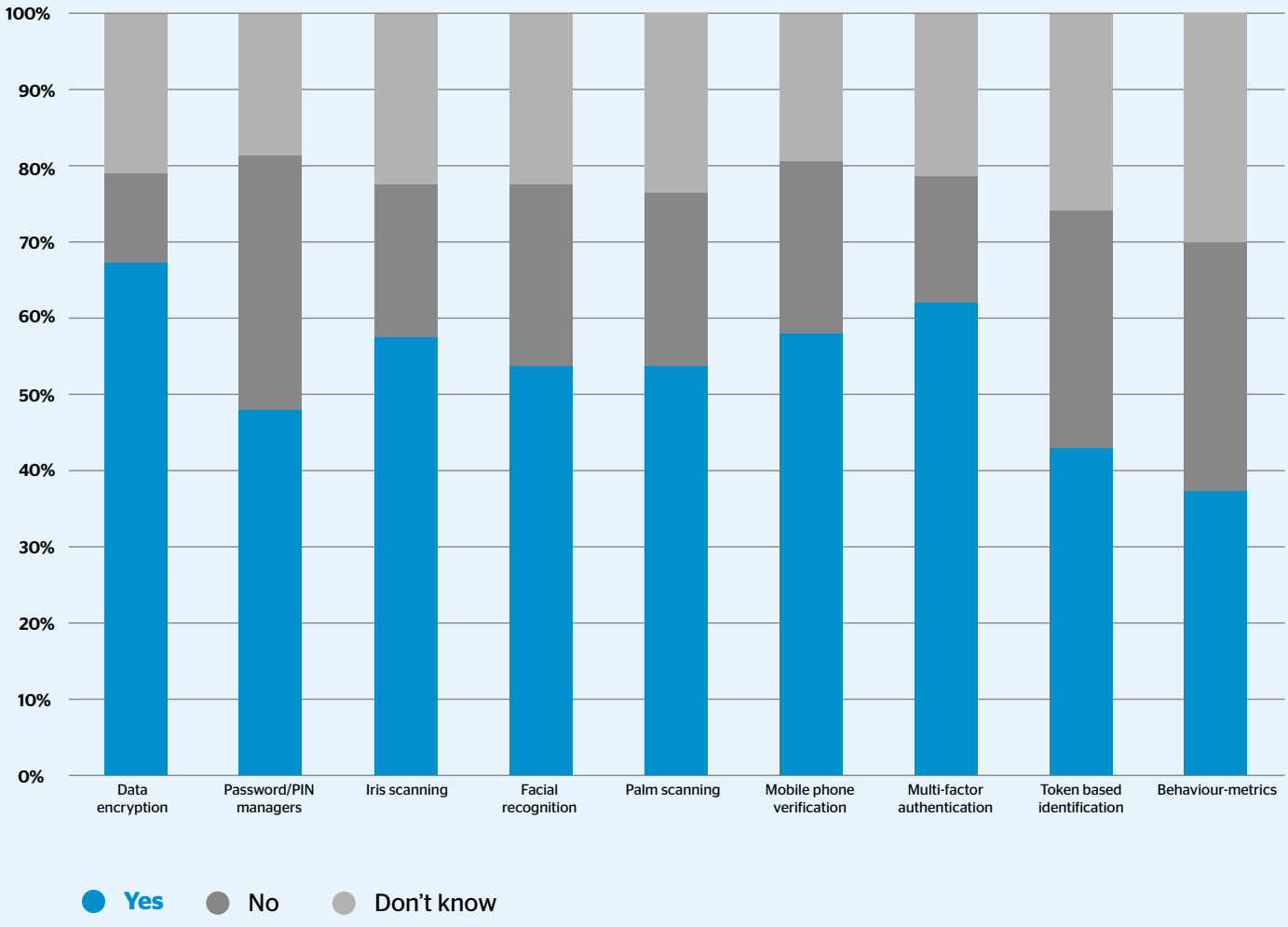
Expectations placed on organisations by their customers have never been higher. 66% expect an organisation to be able to fully protect its customers against cyber attacks today.

People are looking to organisations to use technological advances to maintain their cyber security. When it comes to trust in an organisation, 67% would trust an organisation more if they knew it was investing in advanced technology to fight against cyber criminals.

When adopting new technologies to keep secure, consumers are most willing to try data encryption to secure their data, with over 50% of respondents choosing this option. A similar percentage are also willing to adopt password or PIN managers, iris scanning, facial recognition, palm scanning, mobile phone verification and multi-factor authentication. Consumers feel these make them more secure with their personal data.

But there are some doubts. Over a fifth of respondents (23%) are not willing to try password managers to help secure their data and 25% say they are not willing to try behaviour-metrics to help secure their data.

Does the addition of the following technologies make consumers feel more secure with their personal data?



Human and machine
Looking at what people believe is needed to help combat cyber crime, 69% say that we need more innovative technology, while 52% say we need more human intervention.

58% of consumers are comfortable with cyber security defences increasingly being managed by a combination of human insight and automated technology. Interestingly 16-24 year olds feel that both human and technology are equally important. Older respondents feel that technology is more necessary than human intervention.

Would consumers trust an organisation more if they know it is investing in advanced technology, such as powerful computers, artificial intelligence (AI) and machine learning, to support its fight against the cyber criminals?

Cyber security is the golden thread that runs through all digital business opportunities. Rather than being a 'bolt-on', your cyber security strategy should enable you to get closer to your customers and achieve your business goals.

Cyber security is now a differentiator in a world where customers will not use digital services they don't trust. Digital innovation in cyber security will give you a competitive edge.

There is a direct correlation between trust, customer satisfaction and business success. That's why rigorous testing of security measures and communication processes is essential to ensure you're getting maximum return on investment.

Tom Swanson
Chief Digital Officer, Atos UK&I

Regional analysis

Risks and responsibilities

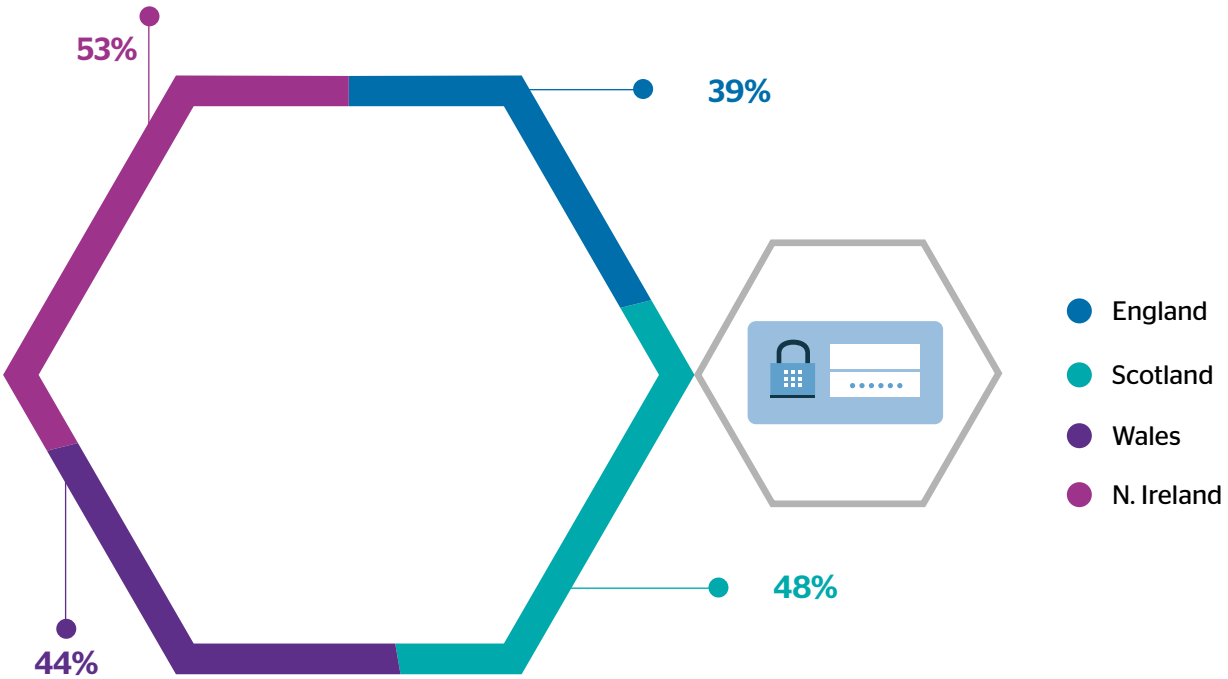
When asked about ever being affected by a cyber attack, the biggest differences are between London and Scotland. Over a fifth (22%) of Londoners say they have been affected, compared to only 9% of Scots. Only 53% of Londoners also say they have never knowingly been affected by a cyber attack, compared to 70% of Scots.

When asked about taking practical steps to protect themselves from cyber risk, the biggest differences are between Northern Ireland and London. 70% of Londoners take practical steps, while only 48% of respondents in Northern Ireland do the same.

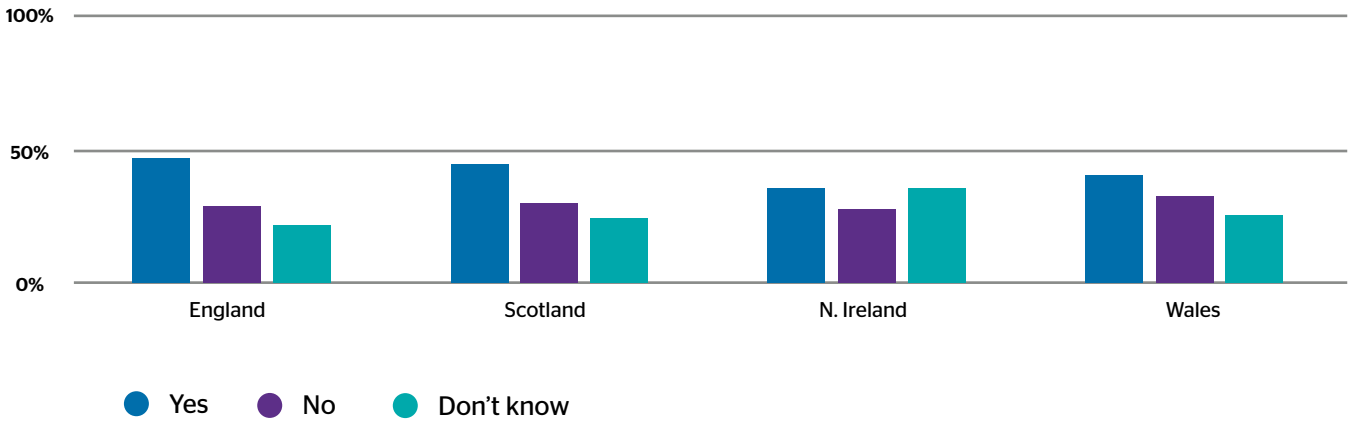
77% of respondents in Northern Ireland expect an organisation to be able to fully protect its customers against cyber attacks today (more than any other region).

78% of Londoners believe cyber security is woven into our everyday lives (more than any other region).

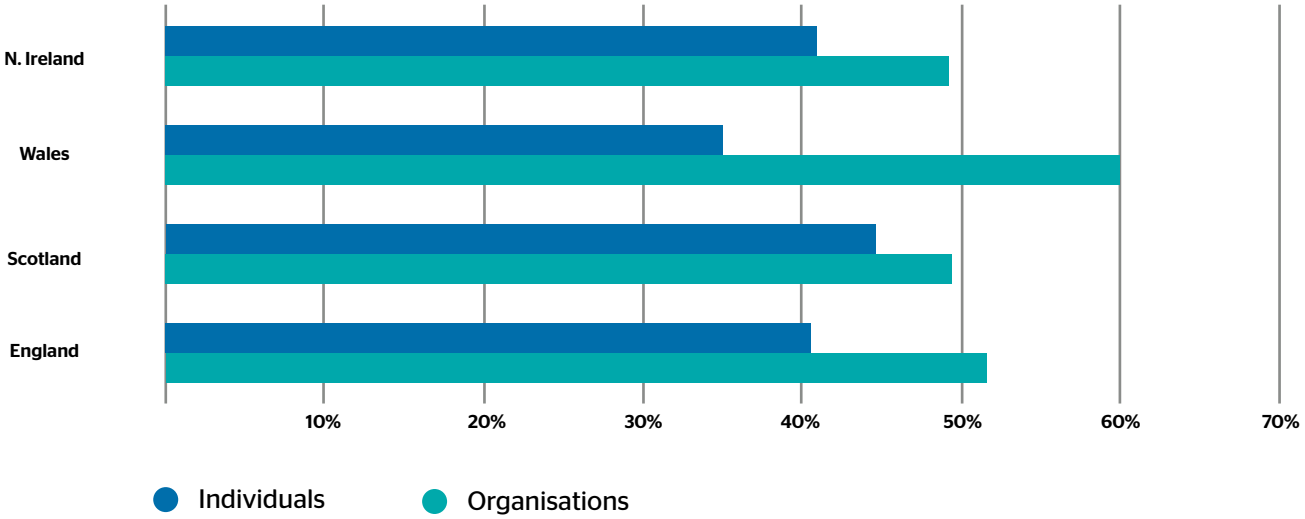
Consumers who do not take practical steps to protect themselves from cyber threats



Whether the level of risk felt has increased compared to 12 months ago



Who is responsible for keeping personal data safe?



Public trust in organisations

Over a third (37%) of Welsh respondents say their trust in organisations has decreased in the last two years, the biggest loss in any region. In comparison, 30% in Northern Ireland and 26% in the East of England say their trust had decreased.

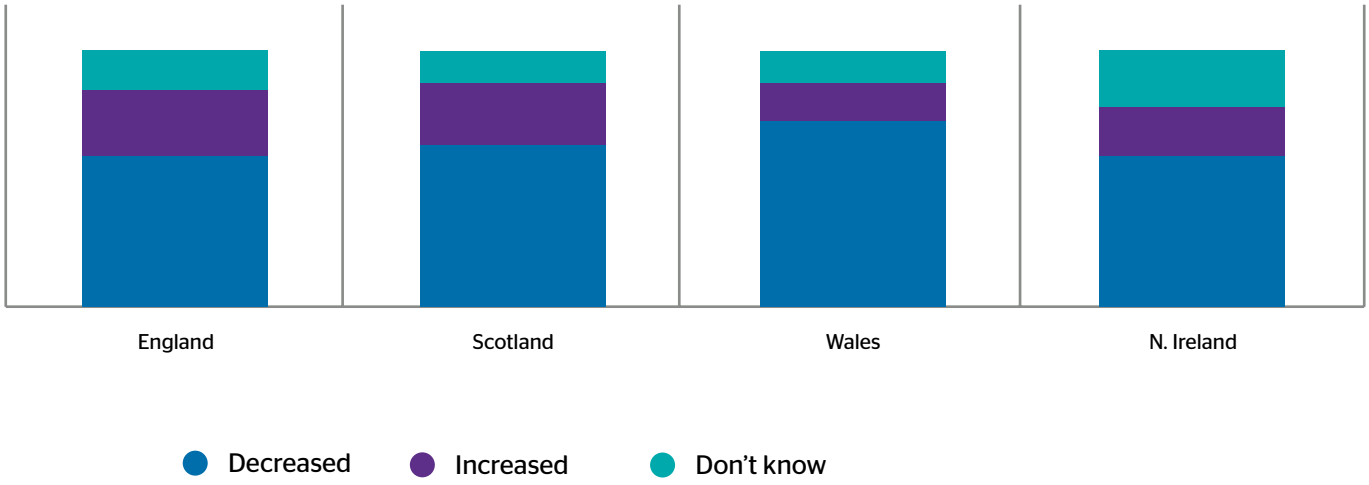
63% of Welsh people believe that advances in technology have made it more difficult for organisations to keep up with cyber criminals, more than any other region.

Interestingly, over a quarter (26%) of Londoners believe their trust level in organisations has increased in terms of their ability to protect them from a cyber attack, the biggest growth in any region.

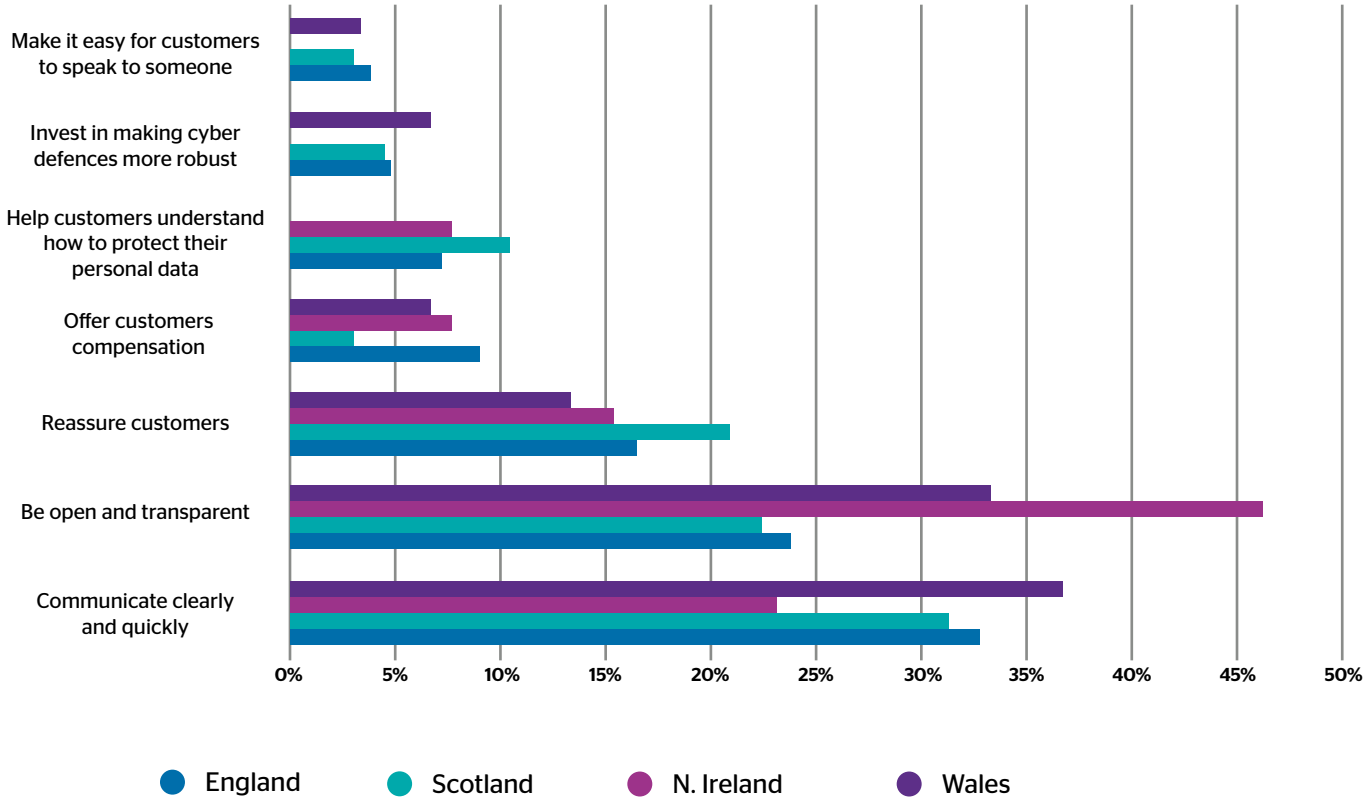
Most regions agree that the most important thing for an organisation to do to regain trust after a cyber attack is to communicate what happened and its effect on them. Similarly, 32% of Londoners, and people in Yorkshire (29%), the South West (25%) and Northern Ireland (46%) think the most important thing is to be open and transparent.

Over a fifth (22%) of respondents in the North East say there is nothing an organisation could do to regain trust after a cyber attack (the biggest percentage across all regions).

The level of trust in organisations to protect themselves from a cyber attack



Most important thing for an organisation to do after a cyber attack



Customer choice and experience

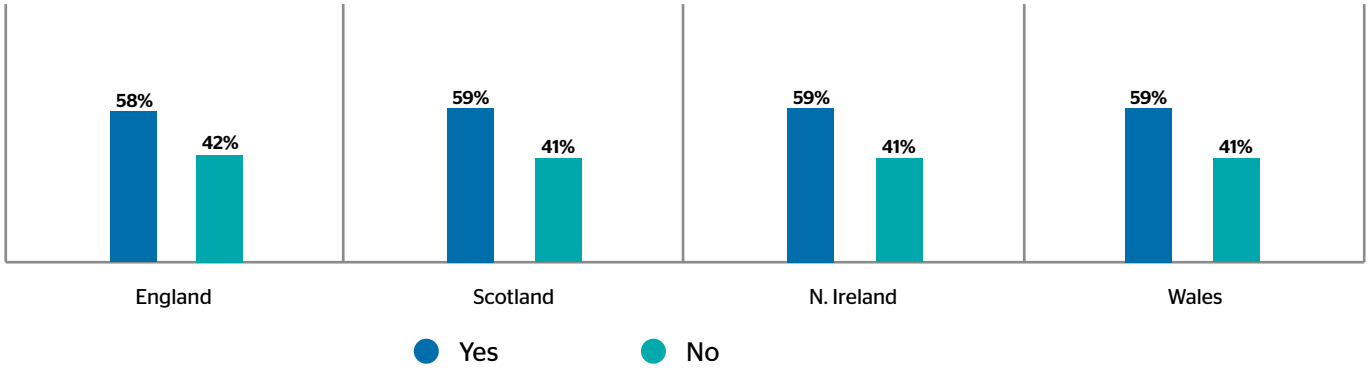
When looking at the deciding factor when choosing an organisation or a service, two thirds (66%) of Londoners say that cyber security is a deciding factor, compared to only 52% of people in Yorkshire (the biggest difference across the regions).

Looking at what's needed to help fight cyber crime, people across all regions are willing to try data encryption to secure their data, with Londoners leading the way in being most willing, with three quarters feeling this way.

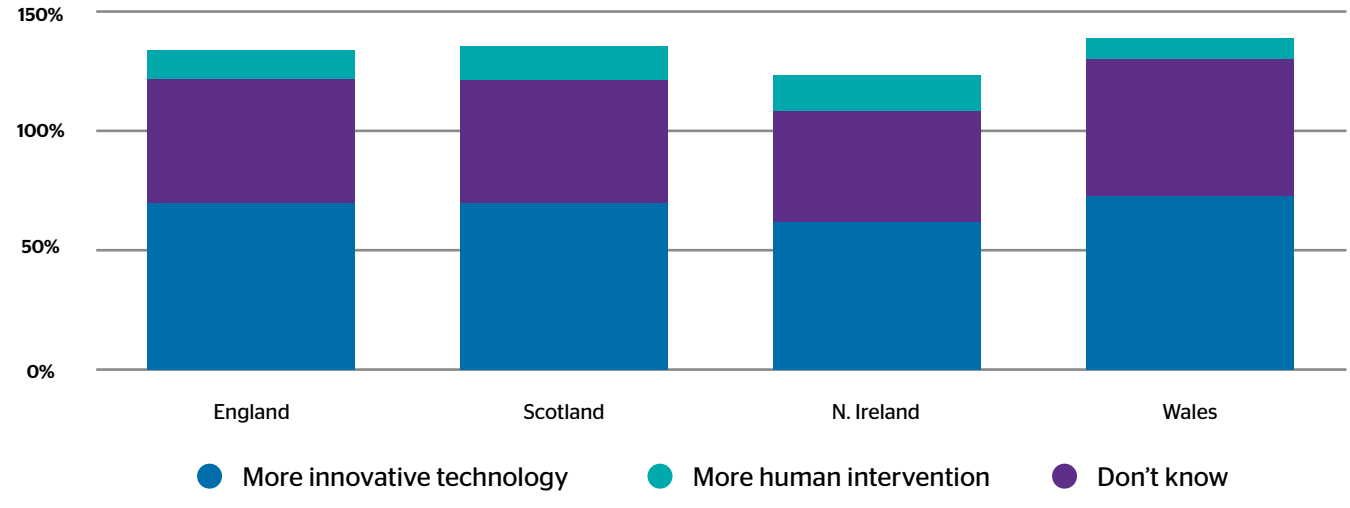
Looking at what's needed to help fight cyber crime, 78% of respondents in the North East believe more innovative technology is required, compared to 62% in Northern Ireland (the biggest gap between regions). 59% of Londoners believe in more human intervention, compared to 44% in the North East (the biggest gap between regions).

Looking at password managers, Londoners again lead the way with being most willing, with 61% happy to use this technology. Interestingly over a quarter (27%) of Scots are not willing at all to adopt it. Londoners also lead the way with being most willing to adopt iris scanning (64%), token-based identification (59%) and behaviour-metrics, which measure typing rhythm or voice (52%).

Is an organisation's cyber capability a deciding factor in whether customers would deal with them?

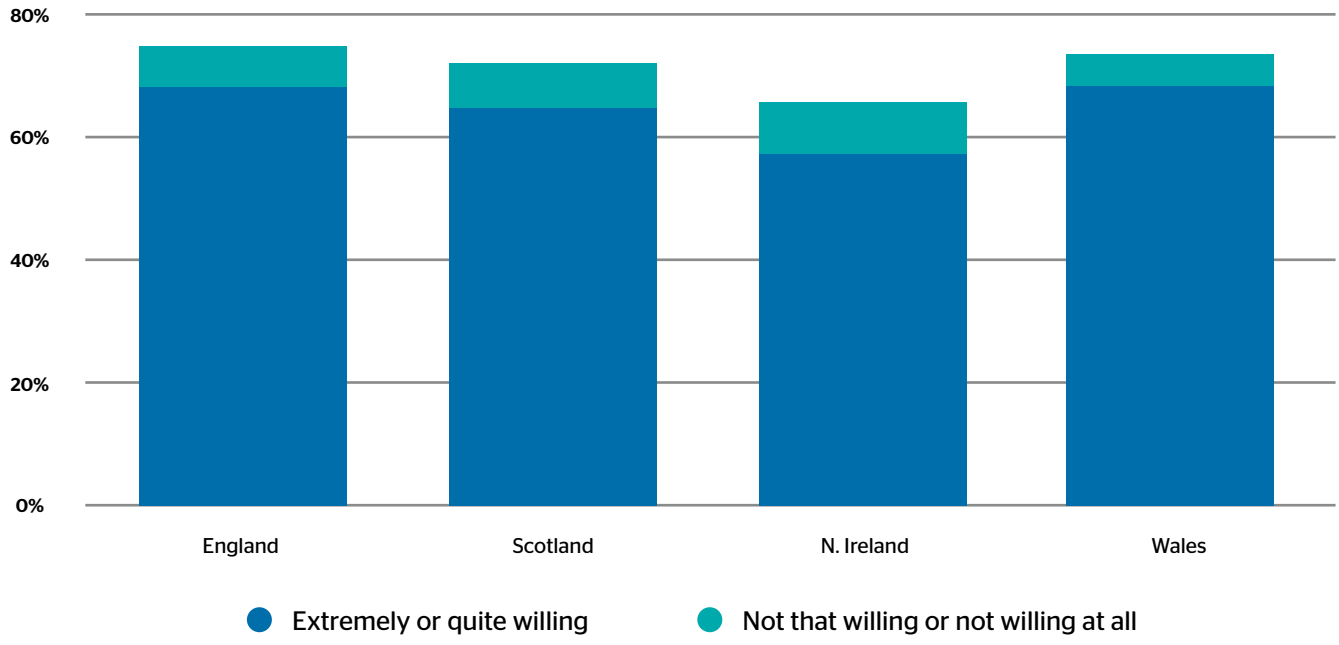


What's needed to fight cyber crime?*

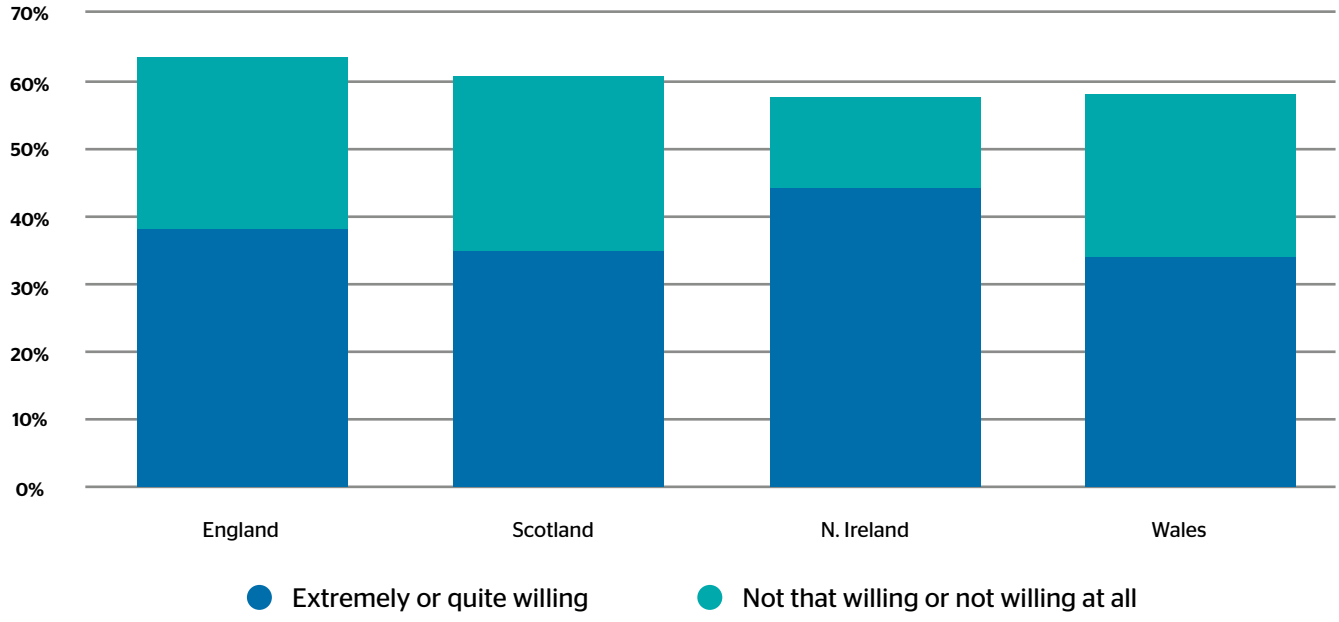


* Respondents could pick more than one answer

Data encryption adoption



Behaviometrics adoption



Recommendations

The overall conclusion that can be drawn from this research is that as people become more engaged with cyber security, organisations who approach it in the right way can use it to differentiate themselves from their competitors, enhance their customer relationships and achieve their digital ambitions. In the digital age, cyber trust is a valuable currency.

Based on the findings of this research, here are five steps for any public or private sector organisation to take in order to win and retain their customers' cyber trust.

1. Be customer-centric

Going digital creates a step change in the way you interact with customers, and as a public or private organisation asking your customers to use digital channels, you should demonstrate to them that you take cyber security seriously, especially given the risks to your reputation and bottom line.

No technology or security strategy will be successful if the experience of customers is poor. These days customers are ready to walk away from private sector companies or stop using the digital channels that public sector organisations promote. Getting cyber security right can deliver a step change in customer loyalty that will drive your digital ambitions.

2. Be proportionate

With the introduction of GDPR, cyber security is as much a corporate risk issue as it is a marketing and consumer one. While there is a wide spectrum of investment options, it's not enough just to spend money on the latest technology, and the very best security may well not be affordable. The right cyber security strategy is about an assessment of cost constraints, risk appetite and sensitivity of information, with measures that are fit for purpose in the context of the business and threat environment.

Atos works with organisations on the National Cyber Security Centre's 10 Steps to Cyber Security to identify where and how to invest in end-to-end security, from monitoring and analytics to find anomalies to ID and access management processes. Whatever the area of investment, we always advocate the use of encryption to make sure data can't be used if it is stolen.

3. Be transparent

While customer trust used to be given unquestioningly and for free, today you have to earn it. And a major way to do that is to actively and regularly communicate about cyber security and what you are doing.

Using cyber security as a differentiator is the way to earn and retain trust and recover it in the event of an incident. If data is stolen, customers expect a swift and comprehensive response, and they expect to know you've learned your lesson and made the necessary investments to avoid more problems in future.

4. Invest in user experience

Stand out user experiences are about speed, ease and clear benefits to the user and cyber security is no exception. You need to design seamless, responsive user experiences that incorporate enough security to keep data safe and customers reassured while not being so cumbersome they de-incentivise users.

For example, customers will welcome a multi-layered sign-on that is smooth and quick. But this requires specialist user experience design expertise along with prototyping and testing to incorporate components such as biometrics.

5. Educate your customers

Lack of best practice around choosing passwords and using public networks creates a very real risk. Working at informing, enabling and supporting customers to be more active partners in cyber security is important. In addition, making this integral to your wider customer engagement plans and the user experience design process is key.

GDPR is important here. The new regulation is not just a compliance checklist. It presents an opportunity to engage with your customers about what you've done to protect their data and how you will continue to respond.

What Next?

As this report has revealed, UK organisations need to continue to innovate to protect themselves, their customers and their data as the cyber security landscape evolves. If you'd like to talk to Atos about any aspect of these findings or about the challenges your organisation faces, please get in touch.

For more information:
ukwebenquiries@atos.net

Find out more about us:
atos.net/cyber-research-uk

Methodology

The research for Atos was undertaken between the 10th and 14th November 2017 through Chime Tech using Censuswide.

Sample: 3,065 general consumers.

Research type: online questionnaire.

Censuswide abides by and employs members of the Market Research Society, which is based on the ESOMAR principles.

About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 73 countries and annual revenue of around € 13 billion.

European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, the Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

Find out more about us
atos.net
ascent.atos.net

Let's start a discussion together