

PROBRAND

THE PUBLIC & PRIVATE SECTOR ONLINE SERVICES AUDIT:

Websites and online services
perceived to offer biggest data
security and GDPR risk.

INTRODUCTION

From registering with a local council, paying rent, to accessing our tax records there is not much that can't be done online in today's digital age. Even our personal health records can be instantly accessed with a few clicks.

This is the case in both the public and private sector, and there are now very few services available on the traditional high street that cannot be accessed more easily on the web.

However, recent high profile cyber-attacks like the ransomware incident in the NHS and the customer data breach at mobile network provider, Three, has put privacy and data security in the spotlight for providers of online services.

And the forthcoming European General Data Protection Regulations (GDPR), which involve the biggest changes to Europe's data protection rules in two decades, mean that there is even greater attention being given to how even the smallest companies are recording, storing and processing users' data.

What's more, greater fines and further regulation requirements - including appointing data protection officers in businesses of 250 staff or more, and obtaining a positive opt-in from users in

order to be able to process their data - mean there is even more pressure being placed on large organisations to adhere to the new data protection guidelines.

As the trend for organisations to take and deliver services online intensifies in line with consumer web behaviour, data security, user experience and quality of service are all being brought into sharp focus. Following significant progress in the private sector, of particular interest is the mandate from government into the public sector to digitise services and go 'paperless' by 2020.

This report reflects on market research commissioned by IT provider Probrand and carried out by Usurv, examining end user attitudes to the current state of online services provided by both private and public sector organisations with particular reference to:

- Safety and security
- User experience
- Efficiency and quality

About PROBRAND

Probrand provides IT products, managed IT services and solutions to over 3,500 private and public sector organisations. The business helps customers procure IT more efficiently, and deliver IT services that run and transform business operations.

Unlike traditional service providers and eshops, Probrand blends a ground-breaking digital marketplace that takes

the hassle out of IT procurement, with sector and technical experts, a best-of-breed IT services & solutions portfolio and market leading partner accreditations. Four key components defining a progressive technology services provider and an approach that delivers the best choice and outcome for customers.

Highlights

- **49%** of people are wary of sharing their data on public sector websites, compared to 40% who are wary of sharing their information on private sector websites
- **81%** of people are concerned about the security of their data held on local council websites
- **86%** of people are concerned about the safety of their data held by the NHS
- More than one in five people (**21%**) think public sector websites are difficult to navigate
- More than a quarter (**26%**) think there are too many gateways to accessing services on public sector websites
- Less than half of people (**47%**) would rate the ease of use of public sector websites as “good”
- **21%** of people think all public sector websites are failing to provide good online services
- Most people (**28%**) think retailers offer the best online customer experience
- **84%** of people have used technology to access public sector services (e.g. HMRC, local government website, etc)
- **50%** of people have accessed private sector services (e.g. mobile phone provider, household utility, etc) using some kind of technology

Public sector raises most concern on data security issues

Ahead of the enforcement of GDPR, which is due to happen in May 2018, the security of the public data held by businesses has become a major topic of discussion in organisations up and down the country, as they seek to understand and ensure they are meeting the new data storage regulations by the time this legislation comes into force.

For many, this will involve major overhauls of existing systems, as they seek to stabilise their processes and information storage procedures.

Worryingly, this research has identified that there are a number of concerns amongst the public about the storage of their data by organisations - and in particular, the data revealed that more people are concerned about sharing their personal information (such as their address, date of birth, ID numbers and payment details) with public sector websites than with those operated by private sector providers.

Nearly half (49%) of people say they are wary about sharing this type of information online with a public organisation like a council - although a significant number (40%) have the same reservations when sharing details with a private business like a retailer.

This is particularly concerning given the information submitted to public sector organisations - such as the police, the NHS and HMRC - will often be more sensitive in nature than those provided to private companies.

Public sector websites are also losing out when it comes to the safety of information stored on their servers, with 49% of people saying they are more concerned about sharing their information with a public sector site than a private website (42%).

However, this could possibly be due to the types of data being stored on the different websites, with the information stored on a public sector website more likely to be sensitive than the information held on a private server.

Recent headlines about high profile cyberattacks on both public and private sector websites are also raising concerns among consumers about the security of their information.

For example, 34% of patients say the recent NHS ransomware attack has made them more concerned about the safety of their private medical records, while 29% of customers are more concerned about the information stored by private businesses after the cyberattack against mobile network provider, Three.

These findings highlight a very real appetite for a greater amount of regulation around the storage of public data, and shows just how educated and aware the public are about the risks posed by insecure systems.

Matt Royle, Marketing Director at Probrand, commented:

“Data security is consistently one of the main concerns people have about sharing personal information online. Clearly the private sector is just ahead of the public sector when it comes to the public’s reservations about sharing and storing data – although that may be because we share more sensitive and personal information on public websites, such as those of local councils, HMRC or the NHS.

These fears are not helped when organisations fall victim to cyberattacks and doubts are subsequently raised about these organisations’ security systems. The public’s confidence in the security of these types of sites are clearly affected by these headlines.”

New General Data Protection Regulation could ease concerns

Some of these concerns could be due to the increased spotlight being given to public data storage by businesses within the media, ahead of GDPR coming into force.

While it is hoped that GDPR will increase the standards of data storage across all industries should improve - and with it, increase the level of public confidence in online services - the ongoing public debate around GDPR ahead of it being implemented has raised concerns about just how out of date existing data protection legislation.

Current data protection legislation was implemented 25 years ago, and in the time since technology and the volume of data businesses collect has surged rapidly. What's more, the public is not ignorant to just how many current business practises and technologies will not be covered by this law.

However, the new legislation will not only take into account more contemporary technologies affecting the changing data collection landscape, and should see a step change in how businesses process and handle data, with organisations being held more accountable for handling and holding personal information. It also gives users further rights to access data companies store about them.

Under the new GDPR directive, “destruction, loss, alteration, unauthorised disclosure of, or access to” data must be reported to the data protection regulator. The Information Commissioner’s Office and those affected must also be told about a data breach within three days of it being detected – a step which will help organisations seek assistance following a high profile breach.

GDPR also requires greater disclosure from companies with more than 250 employees – including providing information on why the data is being collected, processed, how long it is being stored for and what protection is in place to safeguard it.

Companies that regularly handle and process data will also have to invest in a designated member of staff, a Data Protection Officer (DPO) to oversee the processing of the data and reports to senior staff on compliance of the new legislation, making GDPR a boardroom level issue if problems occur.

Organisations will also be unable to collection information unknowingly, with opt-in boxes and disclaimers needing to be clearly displayed and positive consent needed before data is collected and processed.

Businesses and organisations will not only be required to demonstrate how they are meeting the strict data storage rules this will set out, but will also be subject to increased fines for security breaches.

Companies which do not comply with GDPR, who are found to be in breach of it, or whose systems are breached and public data lost, could be forced to pay fines up to £20 million - or 4% of a firm's global turnover - whichever is greater.

Businesses wanting to avoid these fines will need to ensure they have the correct systems, data encryptions, security processes and firewalls in place in order to prove their compliance with GDPR, ahead of the legislation coming into force in May 2018.

NHS data security gives biggest cause of concern

Maybe not surprisingly given recent headlines, people are most concerned about sharing their personal information with the NHS, with just 13% saying they harbour no concerns about this at all.

When it comes to the types of public sector online services that people are most concerned about sharing their data with, the NHS again comes out on top, with 34% of people saying they are “very concerned” about providing their data to this organisation’s online services.

This is well ahead of the 27% who are “very concerned” about sharing information online with HMRC.

Websites for schools and those dealing with education give people the least cause for concern with 41% saying they are “not concerned at all” about sharing information with primary school websites, compared to the 9% who reported being “very concerned” about doing this.

38% of people harbour no concern about sharing information online with a secondary school and 36% say the same about a website for a further education institution like a college or university.

While they don’t give people the same level of concern as NHS websites, the public does have some reservations about sharing information with the local council websites. 49% say they would be “very concerned” or “moderately concerned” about providing information to these types of platform.

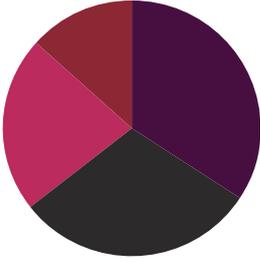
As such, there is a serious need for the NHS and HMRC to educate and reassure users on the security of their systems in ways that they can understand - in order to ensure widespread take up of technology services being provided by both organisations.

Matt Royle, Marketing Director at Probrand, commented;

“Concerns about sharing information online can be fostered by a number of issues, whether it’s the nature of the information we are giving up, the perceived security of the information we are sharing, or the likelihood of the organisation being targeted in a cyberattack.

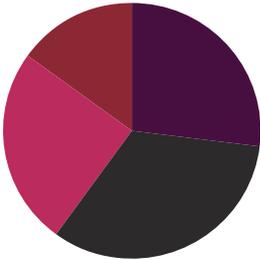
Recent headlines have caused concerns about the safety of our information stored by the NHS in particular. These concerns are likely increased due to the very sensitive nature of the data held by this organisation. While all online services have a responsibility to keep our information safe, some organisations – whether public sector or private – are always going to be under more pressure or scrutiny than others, and some of those are unfortunately currently coming up short.”

Which organisations are people most concerned about sharing their information with online?



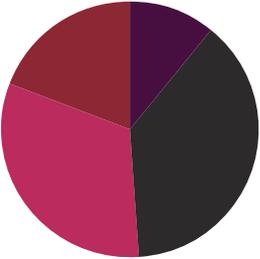
NHS

Very concerned – 34%
Moderately concerned – 30%
Concerned – 22%
Not concerned at all – 13%



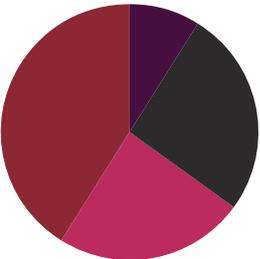
HMRC

Very concerned – 27%
Moderately concerned – 33%
Concerned – 25%
Not concerned at all – 15%



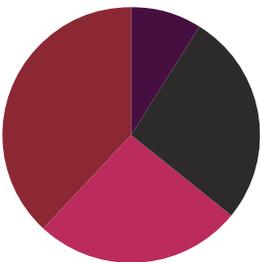
Local council

Very concerned – 11%
Moderately concerned – 38%
Concerned – 32%
Not concerned at all – 19%



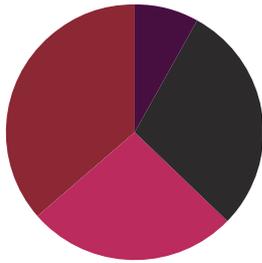
Primary education

Very concerned – 9%
Moderately concerned – 26%
Concerned – 24%
Not concerned at all – 41%



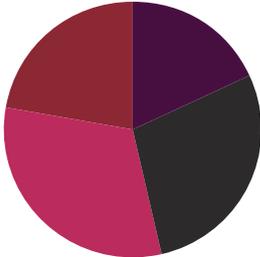
Secondary education

Very concerned – 9%
Moderately concerned – 27%
Concerned – 26%
Not concerned at all – 38%



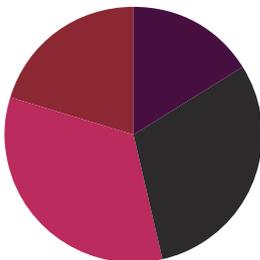
Further education

Very concerned – 8%
Moderately concerned – 29%
Concerned – 26%
Not concerned at all – 36%



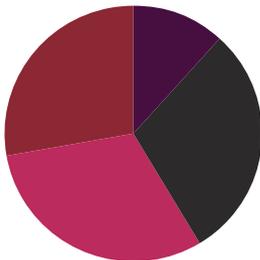
Police force

Very concerned – 18%
Moderately concerned – 28%
Concerned – 31%
Not concerned at all – 22%



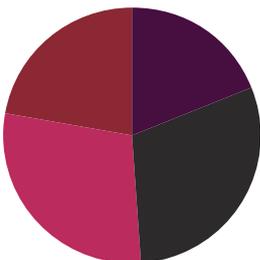
DVLA

Very concerned – 16%
Moderately concerned – 30%
Concerned – 33%
Not concerned at all – 20%



TV licensing

Very concerned – 12%
Moderately concerned – 30%
Concerned – 31%
Not concerned at all – 28%



Social services

Very concerned – 19%
Moderately concerned – 30%
Concerned – 29%
Not concerned at all – 22%

Public sector websites are failing the usability test

The websites of public sector organisations like councils, the police and the health service are failing usability tests with members of the public, with just 43% of users saying they find these platforms easy to navigate.

Only 29% of users think these websites are well designed, while just 36% say they are happy with the current user experience of public sector websites.

These figures should sound a warning to public sector organisations as 84% of people say they have used a website to try and access public sector services recently.

When it comes to why people struggle to use public sector websites, more than a quarter (26%) think there are too many gateways to accessing information online while 19% think the user experience needs improving.

In fact, less than half (47%) of people think these websites are actually easy to use with 24% rating them simply as “fair” and more than one in 10 (12%) saying public sector websites are poor in this area.

Users are also largely unimpressed with the design of these websites with just more than half (51%) describing them as either excellent or good, with the rest of users describing the design of public websites as fair (33%), poor (13%) or very bad (2%).

Finding the navigation of public sector websites difficult is not a issue - 18% of 18-24 year olds experience problems, which is the same figure as those aged 55-64.

One in five (20%) users aged 25-34 and 35-44 admit to finding these websites hard to get around while those aged 45-54 have the most trouble with 22% having problems navigating public sector websites.

Matt Royle, Marketing Director at Probrand, commented;

“Given the number of users who now try to find information about public services online, it is concerning that these organisations do not appear to be offering a good service to the public.

Local councils, the NHS and HMRC hold important information and it is the responsibility of these organisations to make this information as accessible and easy to find as possible. It is central to the government’s initiative to go paperless via a programme of digital transformation”

Public vs private sector websites

The data also found that public sector websites are failing to match their counterparts in the private sector in design and ease of use.

While 61% of people describe the ease of use of public organisations' websites as "excellent" or "good", nearly three quarters (73%) think the same of sites belonging to private sector organisations.

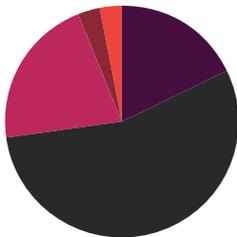
When it comes to website design, 70% of people would describe the sites of private businesses as excellent or good,

compared to 51% who would describe public sector websites the same way.

Even when it comes to providing an informative website, the private sector comes out on top - although in this area the public sector almost matches it.

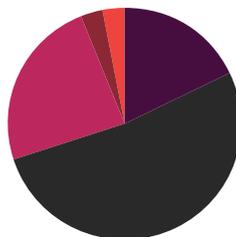
While 73% of people say private businesses' websites are "excellent" or "good" when it comes to being informative, 71% think public businesses are excellent or good for providing informative websites.

Public sector



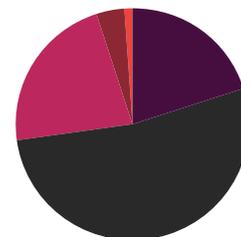
Ease of use

Excellent - 14%
Good - 47%
Fair - 24%
Poor - 12%
Very bad - 3%



Design

Excellent - 12%
Good - 39%
Fair - 33%
Poor - 13%
Very bad - 2%

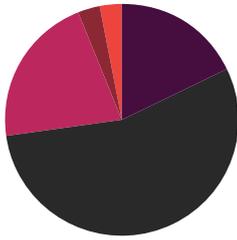


Informative

Excellent - 20%
Good - 51%
Fair - 21%
Poor - 6%
Very bad - 1%

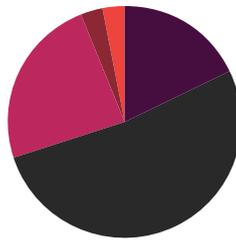


Private sector



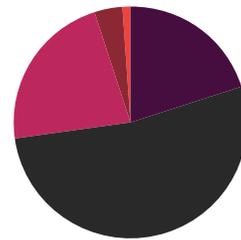
Ease of use

Excellent - 18%
Good - 55%
Fair - 21%
Poor - 3%
Very bad - 3%



Design

Excellent - 18%
Good - 52%
Fair - 24%
Poor - 3%
Very bad - 3%



Informative

Excellent - 20%
Good - 53%
Fair - 22%
Poor - 4%
Very bad - 1%

■ Excellent ■ Good ■ Fair ■ Poor ■ Very bad

Conclusion

According to the market research, the British public perceives the websites of the NHS and HMRC websites to be least secure, and these organisations must take steps to protect data, then educate and reassure users that their websites are in fact secure and meet the forthcoming GDPR requirements.

This unease in online services and website security is driven by both high profile data breaches, recent headlines about cyberattacks and the coverage of new GDPR legislation set to come into force in the next six months, which has highlighted just how out of date the current data protection laws are. What's more, internet users are now much more educated and are aware which websites protect them and their data against potential breaches.

Some of the public's concerns around the security of the information held about them by organisations are founded - it is believed that some 39% of websites are not HTTPS encrypted.

It is probable, however, that concerns about data security are relative to the types of information being shared, the historical security of data and the likelihood of a particular website or organisation being targeted.

Regardless, companies and organisations from both sectors should be concerned by this ahead of the GDPR's implementation in May 2018.

Both private and public sector organisations must ensure their websites and online platforms adhere to GDPR, are safe for users and are HTTPS encrypted to prevent data loss and breaches.

Non-compliance will see fines for security breaches increase from £500,000 to up to up to £20 million or 4% of a firm's global turnover - whichever is greater - with the repercussions carrying the potential to bankrupt a business.

The research also revealed public sector websites are currently failing to offer users good experiences, and - for the most part - are considered poorly designed and difficult to navigate.

Websites of public sector organisations are also failing to match those of the private sector in all aspects of usability, design and quality of information, suggesting the public sector is failing to give enough attention to the online needs of its users.

Considering how many people now use online services to access information from public sector organisations like councils, the NHS or HMRC, this is a concerning fact - particularly given how likely it is that online services are only going to become more popular.

In fact, the government's own 'paperless' initiative designed to push through digital ways of working by 2020, includes better websites, digital apps, forms and automated processes, and is central to serving the public better and raising efficiency standards inside public sector organisations. This research indicates there is some way to go before reaching that objective.

PROBRAND

Contact Us

Birmingham

Alpha Tower 11th Floor
Suffolk St Queensway
Birmingham B1 1T

Manchester

Suite 3b Paragon House
48 Seymour Grove
Old Trafford
Manchester M16 0LN

General enquiries

0121 605 1000