bsi.

...making excellence a habit.™

Information and Cyber Challenges in the Public Sector

Survey 2018

Contents

Executive summary

The public sector operates in an environment driven by data. From education and healthcare to utilities and housing, data is now as integral to the success of public services as the teams and physical infrastructures through which they are deployed.

With the increase in the volume and complexity of data, however, has come an increased risk of its loss, theft or misuse through malicious attacks or mismanagement, many of which threaten citizens' privacy and security and cause serious disruption to essential services.

Recent high profile data breaches have brought these security concerns into the spotlight, with the WannaCry attack in 2017 highlighting the vulnerability of NHS data management systems, many of which were based on outdated legacy IT platforms[1].

The adoption of cloud based IT systems, though not universal, is helping to reduce this risk through robust security safeguards and sophisticated end to end data encryption.

However, the transition from on-premise or hybrid server data management to remote cloud systems poses its own security challenges.

First, around establishing best practice among staff for the management of data that may be shared with other people and organizations due to the rise in the use of collaboration tools.

Second, because of the growth of 'shadow IT' - productivity applications downloaded by staff and used on both personal and work devices, often without the knowledge and authorization of IT managers, which can create opportunities for hackers to bypass system security and access sensitive data.

In both cases, the challenge can be met with coordinated staff training and education to make sure everyone in the organization - not just IT teams - understands the risks and commits to the highest standard of Information Security Management Systems (ISMS).

Public services have an obligation to embrace the government's digital transformation agenda to make the most of the efficiencies modern cloud-based computing brings, however the pace of this uptake must never be at the expense of security for users, organizations and above all, citizens.

Methodology

This survey was compiled by BSI in conjunction with GovNewsDirect to examine the robustness of the public sector against cyber-attacks and other threats to data security. It examines preparedness in the event of a malicious attack, the extent to which security measures are already in place and organizational attitudes towards information resilience.

A broad range of public sector organizations were polled, including Central and Local Government, Healthcare, Education and Blue Light services.

Respondents were drawn from all levels across C-Suite positions, directors, senior and line managers and lead officers. There were 909 unique responses across 745 separate public sector organizations.

The results of the survey are published here to allow those who took part and others to benchmark themselves against the wider public sector and review their own systems and contingencies for data security.

[1]National Crime Agency. 'The Cyber Threat to UK Businesses. 2017-2018 Report. P.8

Background

The sheer volume of sensitive information now held and shared across networks means organizations of every kind are targets for cybercriminals wishing to disrupt critical services or profit from the monetary value of data on the dark web.

Increasingly, cyber-attacks are being mounted not just by individual malicious actors, but by nation states via proxy servers that make it all the more difficult to trace and attribute blame.

Cyber-attacks fall into three main categories:

Distributed Denial of Service (DDoS)

DDoS attacks are launched by large linked networks of computers that are used, without their owners' knowledge, to swamp websites and other networks with connection requests to a point where their capacity to operate is overwhelmed. Those behind such attacks will often demand ransom payments to withdraw them.

Ransomware

Ransomware is a harmful virus that infiltrates network systems, often via unscreened email or software downloads, and paralyses part or all of the network functions. During the WannaCry ransomware attack on NHS systems, over a third of England's NHS trusts were disrupted and more than 6,900 NHS appointments had to be cancelled.

Massive data breaches

Data breaches can be malicious - when criminals hack network systems security to steal sensitive information - or accidental, when information is leaked, lost or inadvertently placed in the public domain.

Data security regulations

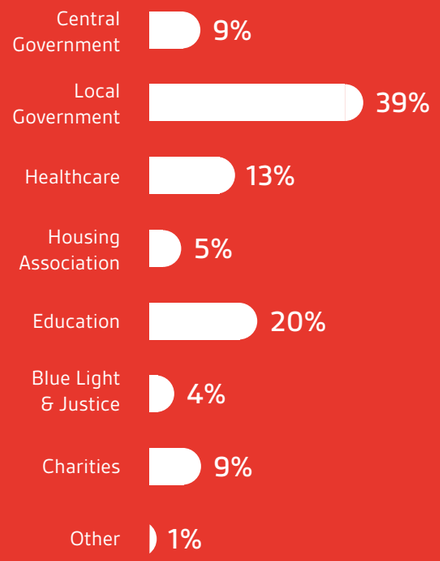
In recognition of the threat of cyber-attacks to businesses and public services, the EU has established, the Network and Information Systems (NIS) directive, which became law in the UK in May 2018.

The NIS applies primarily to organizations identified as Operators of Essential Services (OES), including Blue Light, Power and Healthcare, as well the authorities that regulate them. It also applies to certain digital service providers, including cloud computing server operators.

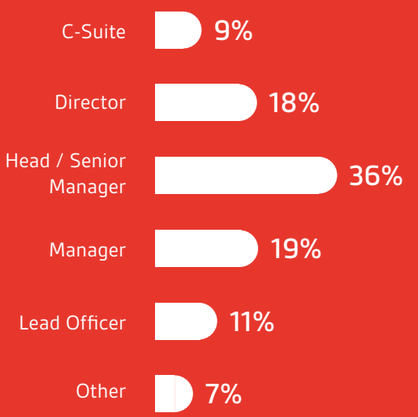
Much of the NIS is aimed at helping organizations establish best practice for data security. However, in line with the serious consequences of data security breaches, from economic and social damage right up to and including loss of life, it also sets out penalties for data security infringements on a par with, if not stricter than, the new General Data Protection Regulations (GDPR): up to €20m or 4% of turnover for private sector businesses.

909 Unique responses / 745 Unique organizations

Sector



Seniority



Findings and statistics

Does your organization have a cloud first policy?

- **22%** Yes
- **48%** No
- **24%** Partially
- **6%** Planned

What is your policy on BYOD (Bring Your Own Device)?

- **31%** Available to all staff
- **28%** Restricted to authorized staff
- **41%** Not allowed

Have you an 'Acceptable Internet Usage' policy in place?

- **85%** Yes
- **12%** Yes but could be improved
- **3%** No

Have you a 'Data Loss Prevention' policy in place for cloud services?

- **51%** Yes
- **17%** Yes but could be improved
- **32%** No

Are you aware of the security standard ISO 27001?

- **33%** Fully Aware
- **41%** Partially Aware
- **26%** Never heard of it

Over a quarter (26%) have never heard of ISO 27001

52% Have never heard of EU NIS directive

Are you prepared for the impacts of the EU NIS (Networks and Information Systems) directive?

- **37%** Yes
- **11%** No
- **52%** Never heard of EU NIS directive

Are you aware of the National Cyber Security Centre (NCSC) guidance and its impact on your business?

- **47%** Yes
- **28%** No
- **25%** Partially

Is there a preference for data residency in your organization?

- 27% **EU**
- 1% **Anywhere**
- 7% **No**
- 3% **Other comments include:**

"As long as there is some confidence in security, probably rather the UK"

"Central servers"

"No rules but policy is to maintain sovereignty"

"Our own IT estate"

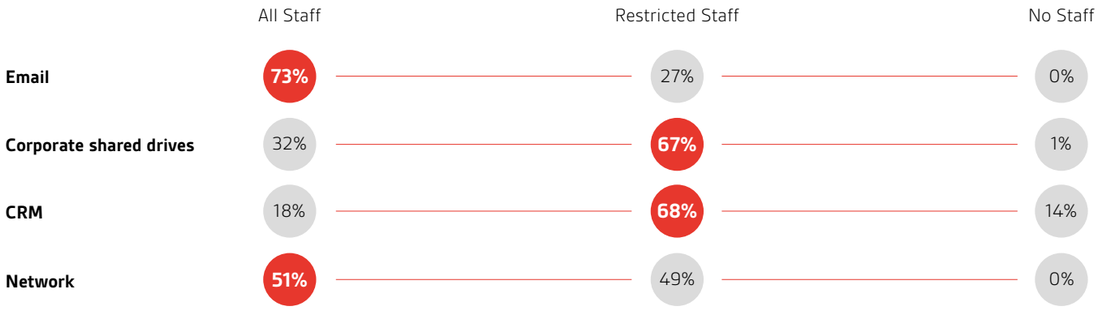
"Our own servers"

"Probably UK"

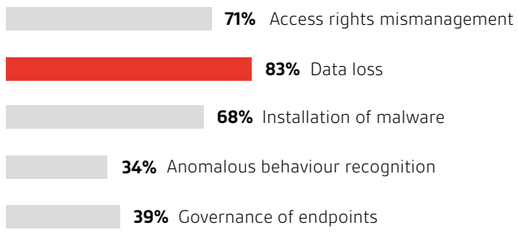
"Residency/cloud with single server isolated"

"UK and official sensitive environment"

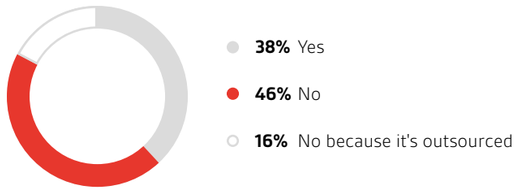
How many users in your organization have remote access to the following:



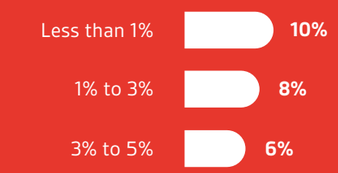
Have you considered any of the following potential risks from disgruntled employees?



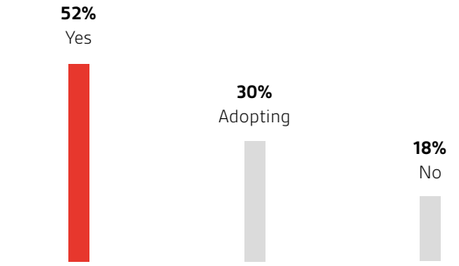
Is your organization affected by a skills shortage relating to security?



What percentage of your department's budget gets allocated to cybersecurity?

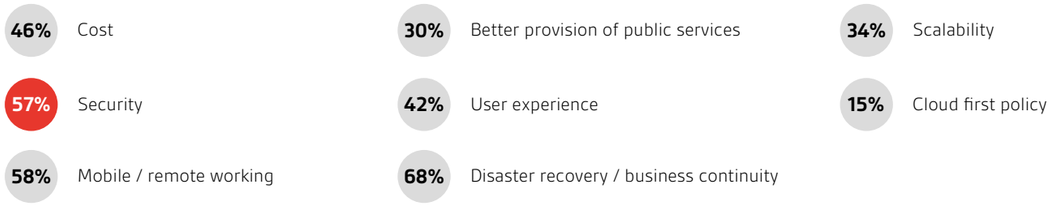


Are you using Office 365 across your organization?



57% said security is the third most important key requirement/driver for cloud adoption

What do you consider to be the key requirements/drivers for cloud adoption?



How many cloud applications are being used in your department?

38% 0 - 5

14% 5 - 10

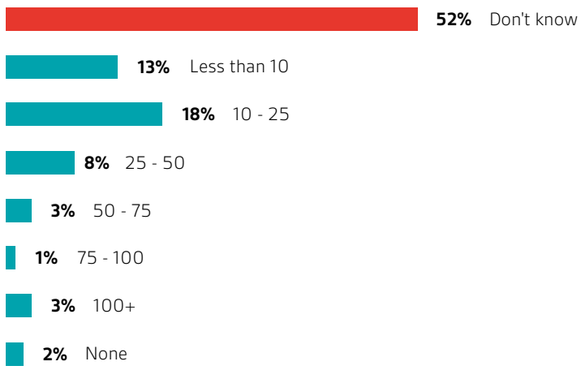
5% 10 - 15

7% 15+

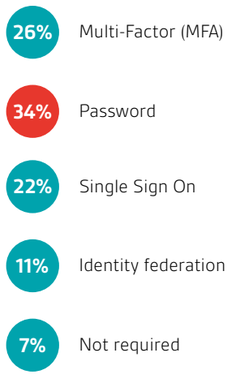
9% None

27% Don't know

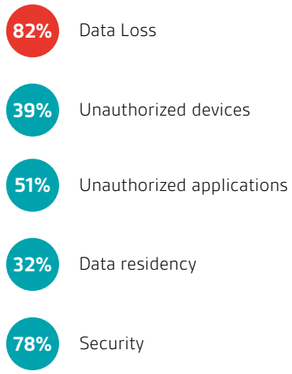
How many cloud applications are being used in your organization?



How do you manage authentication in the cloud?



Which of the following Shadow IT risks are a concern to your organization?

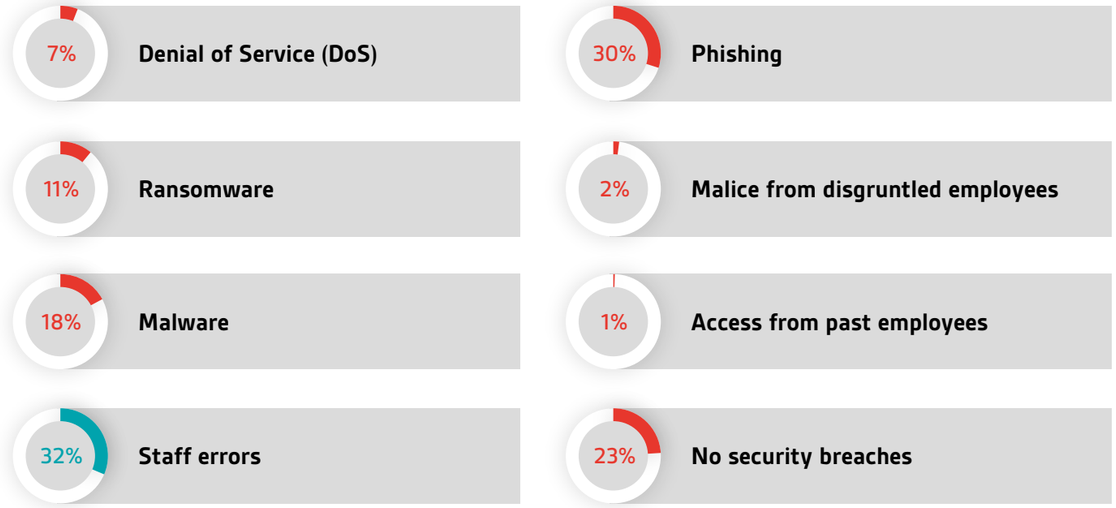


Do you know what the security limitations are around Office 365?

43% Yes

57% No

Which security breaches have you suffered in the last 12 months?



Do you have a plan/process in place to handle a security breach?

94% have a plan in place to handle data security breaches

Have you considered the security around IoT (Internet of Things)?

- **15%** Yes (we have a policy)
- **40%** No
- **31%** Partially
- **40%** Not required

How do you control third party access to your network?

- **37%** Policy
- **16%** Audit control
- **71%** Authentication
- **34%** VPN
- **14%** Not allowed

Are you aware of modern day advanced threats / botnets from the use of Artificial Intelligence (AI)?

- **59%** Yes
- **41%** No

How confident are you in accessing your applications / systems when under a cyber-attack?

- **3%** Extremely confident
- **39%** Confident
- **32%** Not Confident
- **18%** Concerned
- **8%** Extremely Concerned

Does your organization adhere to an ISMS framework?

- 42% Yes
- 9% No
- 28% Could Be Better
- 21% Never Heard of It

Survey analysis report

The survey results highlight a number of issues - some cultural, some technical, some financial - that demand closer examination by those tasked with maintaining cybersecurity in the public sector. However, across all these fronts, three consistent themes emerge:

1

The security implications of the ongoing move to adopt cloud data management systems and the move away from on-premise servers.

2

The threat posed by shadow IT in a decentralized, cloud-based model.

3

'Whose job is it anyway? - I have no need to know this is an IT issue.' The ambiguity over where the responsibility lies for adopting data security best practice across the organization.

The security implications of cloud data management

Across the whole of the public sector, different organizations are at different stages of their digital transformation journey. Among those surveyed, almost half (48%) declared they don't have a cloud first policy.

Where cybersecurity is concerned, however, there is a 'straight line' consequence for those organizations that lag behind in their adoption of cloud-based computing. Older operating systems employing on-premise or hybrid cloud data servers may be more vulnerable to attacks, have more points of entry and are easier for hackers to target and compromise.

During the WannaCry cyber-attack, there were many organizations using older operating systems for which available security patches had been issued but not applied. This underlines the importance for organizations to have up to date control and security measures in place, to ensure they are protected from the threat.

The reason parts of the public sector are still using outdated legacy IT networks is down to the pressure IT budgets have been under for many years now, and the fact that the pace of innovation in IT far exceeds the average public sector equipment replacement cycle.

Nevertheless, it is a serious point of concern for data security when some respondents note they are still using older versions of Microsoft Office.

For those organizations that have already adopted cloud-based systems, the benefits are manifold. Business continuity; remote working; scalability; cost; and of course, security in the form of robust authentication and end to end data encryption. In fact, 57% named security as the most important driver for moving to the cloud.

Those less advanced in their journey, however, may feel pressure to adopt cloud systems before they are fully prepared, as pressure from software providers and vendors are brought to bear.

One respondent commented that suppliers are "offering little choice, or pricing out on-site hosting to maximize their margins". Another stated: "we don't use cloud unless we have to, but are given little choice."

It's here that contradictions emerge. While older legacy systems may be less secure, introducing cloud data management before staff understand the implications for data security can also pose a risk.

For most of the public sector, adopting the cloud means adopting Microsoft's Office 365, with 52% of those asked already having done so.

> "We still have some legacy applications that present a greater challenge in the way they operate".

While Office 365 is certified to the highest security standards, including ISO 27001, the ubiquity of its collaboration tools, particularly SharePoint and OneDrive, can present challenges by allowing individuals and organizations with less stringent security standards access to sensitive information contained in shared documents. For example, it's been found that, on average, 17.1 percent of unencrypted files stored on OneDrive accounts can be considered 'sensitive' and that there are 204 files in each corporate Office 365 recording unencrypted passwords that are called 'passwords'.*

If the public sector is to gain long-term benefit from the advanced security features of today's advanced networks, it is imperative organizations address the human factor by training staff properly and embedding best practice when it comes to storing sensitive data in a way that makes it accessible to authorized users only.

The threat posed by shadow IT

Shadow IT refers to all IT-related activities built or deployed inside organizations without explicit approval. For organizations that have embraced cloud-based data management, the challenges of shadow IT are well understood.

As IT becomes less centralized and users gain access to a wider variety of devices, remote working tools and downloadable productivity apps that operate outside the 'official' network, the potential for data loss, leakage or malicious attacks increases.

82% said data loss was their biggest single concern over the use of shadow IT in the workplace, with 72% citing security as their main worry. With the multiple challenges that shadow IT presents, it's easy to understand why:

- Apps downloaded on personal devices from unauthorized sites can have malware embedded in their code, which can quickly spread and affect the entire network.
- Authentication on shadow IT devices and software is seldom robust, with many users setting the same password across multiple machines. All it takes is one successful phishing attack to expose that password and a determined hacker can gain access to multiple layers of sensitive data.

Neither can IT managers always control access to networks over shadow IT devices after employees move on. Because of this, data loss or theft by disgruntled employees and former employees is seen as a very real risk, with 83% of respondents stating it's their main concern where shadow IT is concerned. The perceived risk of malicious action, however, seems to be much higher than the actual risk. Only 1% said they had actually experienced it.

Yet despite the fact that most shadow IT operates outside their sphere of influence, it's still the responsibility of IT managers to ensure the security and compliance of any data employees upload to cloud services using their own devices, and any breaches under NIS regulations that happen as a result can still incur heavy fines.

Shadow IT is clearly here to stay. Its prominence in the workplace is, after all, a direct result of the flexibility and extra efficiencies that data management in the cloud offers, allowing employees to develop their own IT 'workarounds' to increase personal productivity - despite the fact that such workarounds can also have enormous consequences for data security elsewhere in the organization.

If shadow IT can't be eliminated, the next best thing is to lessen the risks it poses by making sure employees understand the correct procedures for protecting the data they handle with it.

The steady rise of BYOD in the public sector, though less marked than in the private sector, represents an opportunity to integrate shadow IT devices more formally into existing networks, and to increase the competence of those who use them through training and education to certified data security standards.

Again, as with the transition to cloud-based data management, the most significant improvements are to be gained by embedding best practice and increasing knowledge across the organization.

Ambiguity over responsibility for data security

Like the other significant challenge for data management currently occupying the public sector, GDPR, the impact of NIS regulations has exposed an ongoing confusion about exactly where the responsibility lies for ensuring information resilience within individual organizations.

Qualitative responses gathered during the survey point to a level of uncertainty and even indifference in some areas over exactly who is charged with making sure systems are safe from cyber-attack and other forms of data loss.

Typical comments include: "I have no need to know - this is an IT issue". "This is the responsibility of IT and should come out of their budget"

The fact that 52% have never heard of the EU NIS directive and over a quarter (26%) have never heard of ISO 27001 - the most significant legislative development and the most widely accepted certification for cybersecurity respectively - suggests this 'not my problem' outlook is widespread.

Certainly, those with a specific IT remit will be under close scrutiny to ensure security updates, firewalls, authentication, anti-virus software and other technical safeguards against cyber-attacks are in place.

But as already stated, such measures can only mitigate against direct attacks on the network itself.

Equally important - if not more so - than the technical safe-guards is buy-in from everybody involved in handling data, in whatever capacity, to best practice processes for protecting that information.

If that is to happen, public sector organizations must give serious consideration to ongoing programmes that guarantee standards of performance in data security.

Organizations with continuous training methodologies have experienced significant reductions in susceptibility to phishing attacks and malware infections that often accompany them. The fact that 32% of those surveyed have attributed security breaches to staff errors and 30% to phishing incidents reveals organizations strongest asset is often their weakest link.

Ultimately, information resilience in the public sector will be achieved as much through cultural change and continuous professional development as by the advances in IT counter measures to tackle the efforts of cybercriminals across the world.

BSI comment:

With today's citizens expecting fast, easy, personalized digital experiences, public organizations need platforms and systems capable of adapting to those demands and helping prevent cyber-attacks. The increase of hackers, human errors, data breaches, Bring-Your-Own-Device (BYOD) policies and the necessity to share and protect companies' information is empowering public organizations to consider digital transformation strategies.

The migration of services and data to the cloud has become a mainstream operational activity in recent years. The public sector has shown their commitment to this process as demonstrated by the large number of those surveyed who are currently using or in the process of adopting Office 365. This migration is driven by several factors with the top three being business continuity and disaster recovery, mobile and remote working, and security. Capitalizing on this movement of data to the cloud we see a large percentage of public sector users having remote access to email, file data and CRM systems.

Cybersecurity awareness is growing within the public sector. Interestingly, the ISO 27001 Information Security standard has high levels of awareness but the EU Networks and Information Systems (NIS) Directive and UK National Cyber Security Centre (NCSC) guidelines have a much lower level of awareness.

Evolving technologies and emerging threats continue to play a part within risk management. Among those surveyed, data loss was one of their key challenges. It is imperative that as data and applications move to the cloud and remote working is more freely facilitated that the data owners in conjunction with their technology leadership teams are aware of their regulatory requirements and identify the appropriate training and technical processes.

Stephen Bowes
Head of Solutions Delivery and IT
BSI Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:

Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services

Security awareness

Phishing and user awareness training, online solutions, social engineering and simulation testing

Information management and privacy

Information risk management, privacy, data protection, eDiscovery and forensics

Compliance and testing

PCI DSS services, Cyber Lab testing and product and software assessments (CC, CAS-T/CPA)

GovNewsDirect

This survey was built in partnership with GovNewsDirect. GovNewsDirect specialize in facilitating innovative and engaging partnerships between the private and public sector.

Find out more

UK
Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

IE/International
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com

bsi.

In association with... GOV NEWS DIRECT