SOPHOS

The Perception Barrier

An inside look at IT security issues and concerns in the U.K. public sector

Sophos Research December 2019

Introduction

The U.K.'s public sector has embarked on an ambitious journey of digital transformation, embracing mobile and online channels as well as the cloud, analytics, AI-supported decision making, and more. The aim is not just to cut costs and improve efficiency, but to deliver more inclusive and higher quality services and care.

All that technology and connectivity needs protecting, and this is not as easy as it may sound.

Legacy computer hardware, software that has not been updated, misconfiguration of connected devices and networks, vulnerable remote access systems, and human error all contribute to a landscape of opportunity for attackers. Add to this the growing complexity and precision targeting of many cyber threats and it is not surprising that staying on top of cybersecurity and protecting data and users is an uphill task for many IT teams, including those in the public sector.

To better understand the IT security challenges and concerns facing the U.K.'s public sector organisations, Sophos, a global leader in next-generation cybersecurity, commissioned independent research among public sector IT professionals, from CIOs/CISOs to frontline IT practitioners.

There is some good news. For example, the study found that the majority of respondents (79% overall) believe data security is taken more seriously in their organisation now than it was two years ago, ranging from 62% in the NHS up to 93% in education. Further, despite concerns about employee skill levels, around three-quarters of respondents overall believe their non-technical colleagues will always try to take the right steps to protect the organisation's data. These are encouraging foundations to build on for a more secure digital public sector. But there are other areas that need to be addressed, ideally as a priority and we highlight some of them in this report.

The research was conducted in Autumn 2019 and involved 784 U.K. public sector IT professionals who work primarily in either the NHS (272), education (261), or central or local government (251). The interviews were conducted online by Sapio Research.

Top findings

1. The NHS has the highest IT 'security burden' in terms of the percentage (9%) of individual users allocated to each IT security professional
2. Around half (47%) lack confidence in their IT teams' ability to spot and cope with security incidents and 57% don't believe public sector IT leaders are ready for the next generation of tech disruption
3. Around a third of public sector IT teams have limited visibility and/or control of online apps running on their networks
4. Just over half (55%) of public sector IT leaders believe their organisation's digital data is less valuable than that of the private sector
5. The majority of senior IT leaders (76%) say their organisation was affected by a ransomware incident over the past year. Only 16% of IT practitioners were aware of such an incident

6. Many IT leaders also say that there had been a large increase in both IT security incidents (45%) and actual breaches (38%) – compared to a far lower 4% and 8% respectively among IT practitioners
7. The top drivers of IT security are greater risk awareness, the demands of GDPR and media coverage of damaging data breaches, followed by a move towards the cloud, greater collaboration across the public sector and the rise of remote and flexible working
8. A quarter (26%) of respondents, including 36% of IT leaders believe that recruiting and retaining skilled IT security professionals is the biggest obstacle to delivering IT security
9. Just over a third (38%) are moving towards external managed services for IT and security

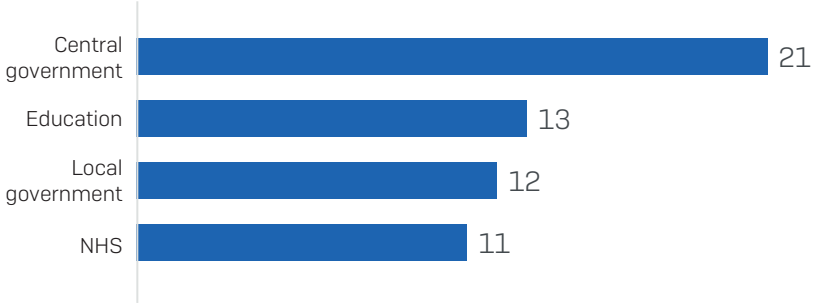
IT security challenges and concerns

The IT security burden

Respondents were asked how many people looked after IT security in their organisation, and how many IT users were supported overall. The combination of these results shows the 'IT security burden' carried by different parts of the public sector, with central government having the lowest security burden and the NHS the largest, in percentage terms.

The IT security burden for different parts of the public sector

Showing average (mean) number of staff in IT security teams



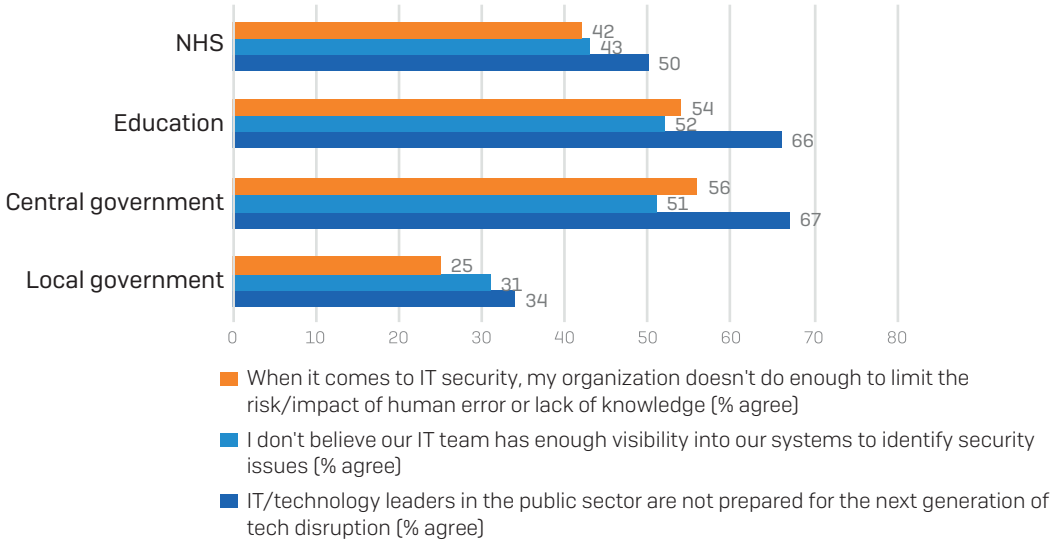
Average number of employees using respondents' IT systems	Users per IT security staff (% of users per each staff member)
4686	223 (5%)
2366	182 (8%)
4661	388 (8%)
2323	211 (9%)

Incident readiness

Around half of public sector organisations (47% overall) have doubts about their IT team's ability to identify and respond to security incidents.

This could reflect underlying concerns, also revealed in the survey, about the speed of technology evolution, a feeling that not enough is being done to protect against human error, and a belief that IT security threats against the organisation's data are on the rise.

Public sector security unreadiness



Visibility and control

One in three public sector IT teams has limited visibility (35%) of applications accessing the internet from within their organisational network, and around the same number admits to only partial control (31%) over connected apps. The risk for these organisations is that unmanaged and potentially insecure apps inside the security perimeter could be offering cyber-adversaries an unguarded route into the corporate network, from where they can move laterally, escalate privileges, and more.

The encouraging news is that over half of all respondents say they have complete visibility (52%) and control (61%).

Organisational sector	Visibility of online applications inside the network		Control of applications in use on the network	
	Complete	Partial	Complete	Partial
NHS	57%	32%	63%	28%
Education	48%	39%	59%	32%
Central government	58%	33%	67%	29%
Local government	33%	40%	45%	39%
Overall	**52%**	**35%**	**61%**	**31%**

The perception gap within IT

The survey uncovered a significant gap between the risk awareness of IT leaders like CIOs and CISOs and their frontline IT teams, regardless of the type of organisation.

Just over half (55%) of public sector IT leaders believe their organisation's digital data is less valuable than that of the private sector, despite the fact that their organisations handle highly sensitive, confidential, personal, and government information. This sits at odds with the fact that IT leaders consistently rate their organisation's threat level and risk as higher and wider than those dealing with every day IT issues.

- The majority of senior IT leaders (76%) say their organisation was affected by a ransomware incident over the past year. Only 16% of IT practitioners were aware of such an incident
- Many IT leaders also say that there had been a large increase in both IT security incidents (45%) and actual breaches (38%) – compared to a far lower 4% and 8% respectively among IT practitioners

Whether these results reflect a broader and more accurate perspective of senior roles, or an over-estimation of risk based on limited data, they reveal a lack of common understanding about what is actually happening. The end result could mean that IT security teams misinterpret and therefore fail to adequately prepare for the actual level of risk faced by the organisation.

Public sector security perception & experience

Top security concerns

Respondents were shown a list of potential challenges to IT security and asked to select the ones their organisation was most worried about. The results highlight shared concerns, such as employee skill levels, as well as the specific challenges facing each type of organisation: for example, ransomware in healthcare, the use of personal devices in education, nation state attacks targeting central government, and insecure legacy systems within local government.

The top three IT security concerns (% agree):

NHS

1. Increase in remote and flexible working: 38%
2. Employee skills: 37%
3. The risk of targeted ransomware attacks: 35%

Education

1. Increased use of freely available cloud solutions (Dropbox, Box, Google Docs etc.): 39%
2. Employee skills: 38%
3. Greater number of personal devices used for work: 37%

Central government

1. Increased use of cloud applications: 47%
2. Increased use of freely available cloud solutions (Dropbox, Box, Google Docs etc.): 42%
3. The risk of targeted attacks by nation states: 42%
4. Rising number of daily malware attacks: 41%

Local government

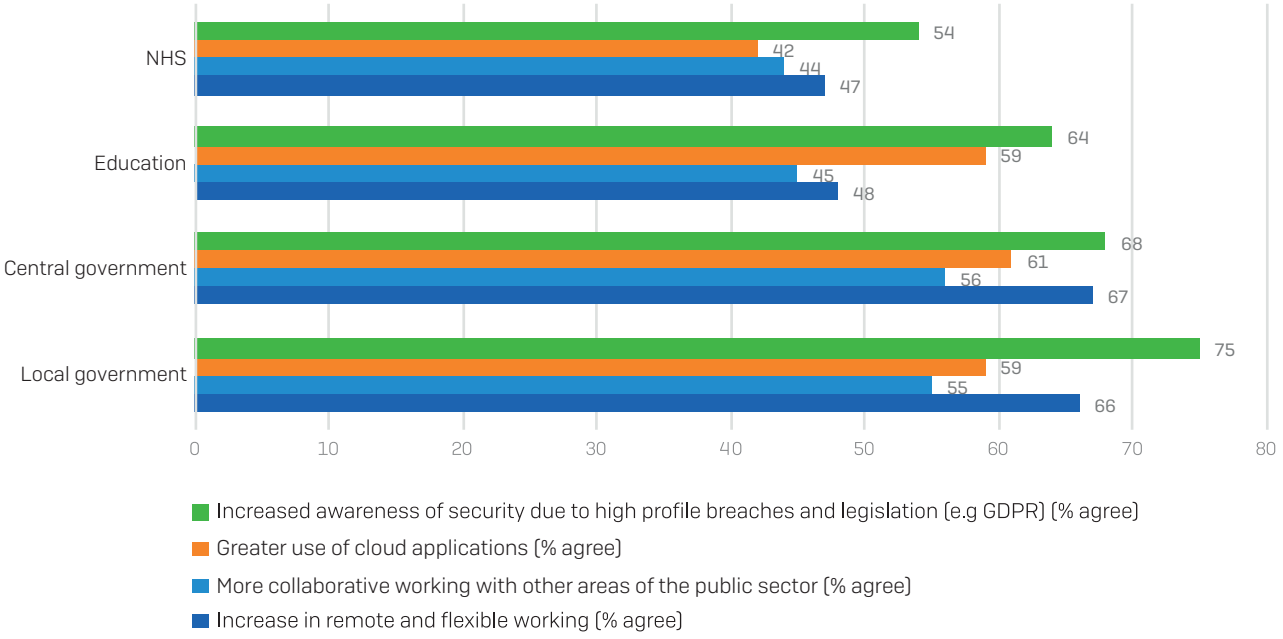
1. Continued use of legacy systems: 41%
2. Employee skills: 36%
3. Rising number of daily malware attacks: 35%

Delivering security

The top driver of IT security in the U.K. public sector is simply greater understanding of the risks and their impact, underpinned by the demands of legislation such as GDPR and media coverage of damaging data breaches.

Other significant drivers are the security needs introduced through digital transformation, including a move towards the cloud, greater collaboration across the public sector, and the rise of remote and flexible working.

Main drivers of IT security in the UK's public sector



Security success depends on people

Alongside the concerns about employee skills already mentioned, the public sector appears to be facing a challenge when it comes to attracting and keeping enough cybersecurity professionals. It is not alone in this. The latest (ISC)2 research suggests the U.K. could have around 100,000 unfilled cybersecurity jobs by 2022.

Overall, around one in four (26%) respondents, including 36% of IT leaders, believe that recruiting and retaining skilled IT security professionals is the biggest obstacle to their organisation's ability to deliver IT security. This breaks down into a third for the NHS (34%) and central government (36%), and one in six or fewer among education (13%) and local government (16%).

The way forward – outsourcing the challenge

Many of the organisations surveyed retain all their IT security in-house (41% overall, ranging from 33% for the NHS to 55% for local government), but some now look to external providers to help. Overall, 13% now use external IT security providers. External support can help to address staff shortages and offer additional expertise, flexibility and scalability – including 24/7 threat hunting. As such it can both complement and replace in-house security support.

Just over a third (38%) are moving towards managed services, ranging from 26% in education to 49% for the NHS, with a further quarter (23%) overall relying on a combination of managed services and in-house support.

Cybersecurity essentials

The following checklist is a guide for IT security teams implementing security best practice. To be effective, it should be accompanied by an ongoing program of employee security awareness training and support.

- Check that you have a full inventory of all devices connected to your network and that any security software you use on them is up to date
- Always install the latest security updates, as soon as they are released, on all the devices and servers on your network
- Have different levels of data access rights for different employees
- Keep regular backups of your most important and current data on an offline storage device as this is the best way to avoid having to pay a ransom when affected by ransomware
- Administrators should enable multi-factor authentication on any security dashboards or control panels used internally, to prevent attackers disabling security products during an attack
- Remember, there is no single silver bullet for security, and a layered, defence-in-depth security model is essential

How Sophos can help

Sophos has proven expertise in helping a wide range of public sector organisations – in education, healthcare and government – to keep employees, customers, devices and networks secure in an increasingly complex and rapidly evolving cyber threat landscape.

Alongside this, Sophos is a leader in next-generation security, offering integrated, multi-layered security solutions that are as advanced as they are easy to manage and implement.

For example, Sophos Intercept X employs a comprehensive defence-in-depth approach to endpoint protection, combining multiple leading next-gen techniques to deliver malware detection, exploit protection and built-in endpoint detection and response (EDR). Intercept X also provides accurate data on security incidents detected and blocked, avoiding the risk of misperception and misinterpretation within IT and IT security teams.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2019-12-06 WP-UK (GH)