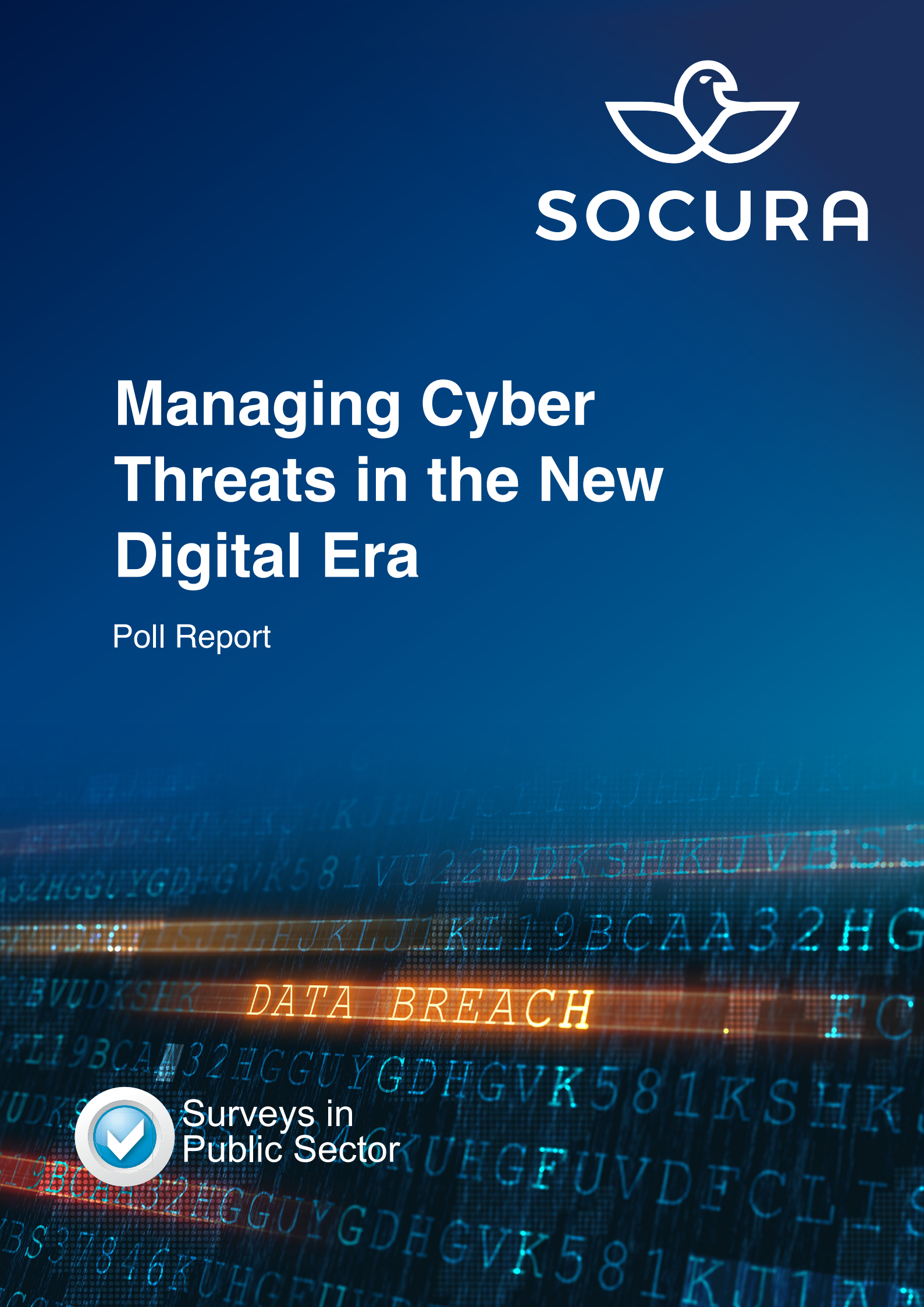
SOCURA

Managing Cyber Threats in the New Digital Era

Poll Report



Surveys in Public Sector

Contents

Introduction

According to the Cyber Security Breaches Survey 2022[1], two in five businesses (39%) report having experienced cyber security breaches or attacks in the last 12 months. Of the 39%, around one in five (21%) identified a more sophisticated attack type such as a denial of service, malware, or ransomware attack. Among the businesses that identify breaches or attacks, nearly a third (31%) estimate they were attacked at least once a week. The most common threat vector was phishing attempts (83%).

In addition, the National Cyber Strategy[2], recently released by the UK government, revealed the extent to which public sector organisations are being targeted by cyber criminals. Billions are being invested in cyber and IT to boost the public sector's resilience and protect the information that so many rely on.

To find out how public sector organisations are trying to protect their critical information, and what plans they have in place to prevent and contain cyber breaches in the future, Socura has partnered with public sector researchers, Surveys in Public Sector, to conduct a quick poll considering:

- **The key challenges for organisations to manage cyber security**
- **The precautionary measures organisations have implemented to help prevent and contain cyber breaches**
- **The approach of security work performed via internal and/or external expertise**

1. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
2. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

About Socura

Socura aims to help make the digital world a safer place; changing the way organisations think about cyber security through a dynamic, innovative and human approach. Their forward-thinking services help organisations to not only detect advanced threats and targeted attacks, but contain them too.

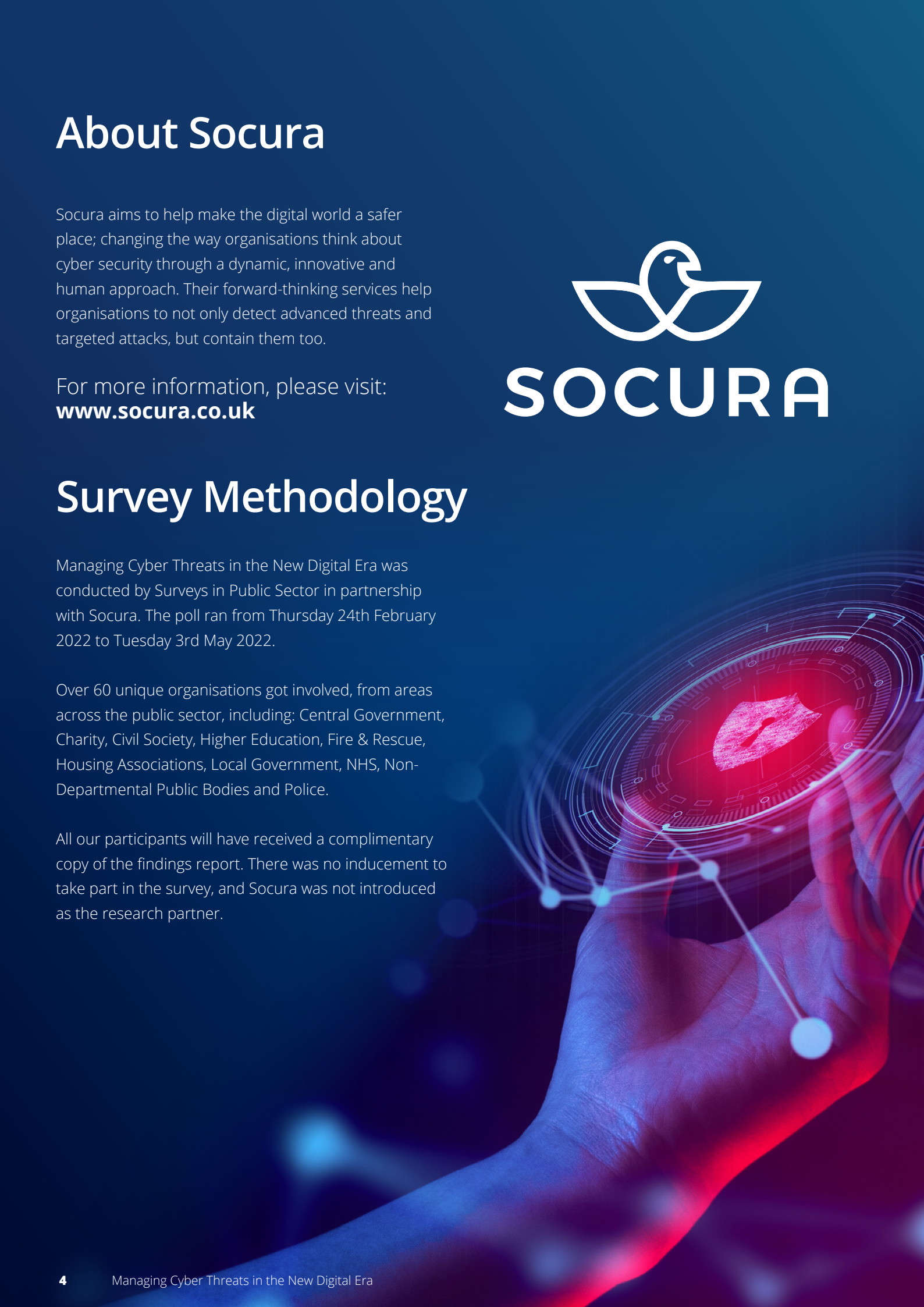
For more information, please visit:
www.socura.co.uk

Survey Methodology

Managing Cyber Threats in the New Digital Era was conducted by Surveys in Public Sector in partnership with Socura. The poll ran from Thursday 24th February 2022 to Tuesday 3rd May 2022.

Over 60 unique organisations got involved, from areas across the public sector, including: Central Government, Charity, Civil Society, Higher Education, Fire & Rescue, Housing Associations, Local Government, NHS, Non-Departmental Public Bodies and Police.

All our participants will have received a complimentary copy of the findings report. There was no inducement to take part in the survey, and Socura was not introduced as the research partner.



Key Findings

Key challenges persist in managing cyber security across the public sector

To begin with, we asked our participants to identify the greatest challenges when managing cyber security within their organisations. While responses were broad, the 'complexity of cyber threats and the need to 'keep up' with new developments' (53%) came out on top.

With increasingly sophisticated cyber threats, it is perhaps unsurprising to see that challenges also arose in 'managing vulnerabilities from legacy systems and software' (51%) and the 'ability to detect and respond to malicious threats (e.g. hacking, phishing, viruses)' (35%).

'Lack of or insufficient education for users about threats' (46%) was also viewed as one of key challenges. With diversified malicious threats and limited internal resources, it is perhaps difficult to ensure staff keep up-to-date with threats that they have to be aware of.

Moreover, our participants pointed out their concern around 'the ability to recruit skilled and experienced staff', with 35% citing 'budgetary constraints' to spending on cyber security as a potential issue.

All of which suggests that whilst the public sector recognises the need to keep up with, and protect their organisations from, ever-changing cyber threats, they are still some way from realising this due to the technical and non-technical constraints that need to be addressed.

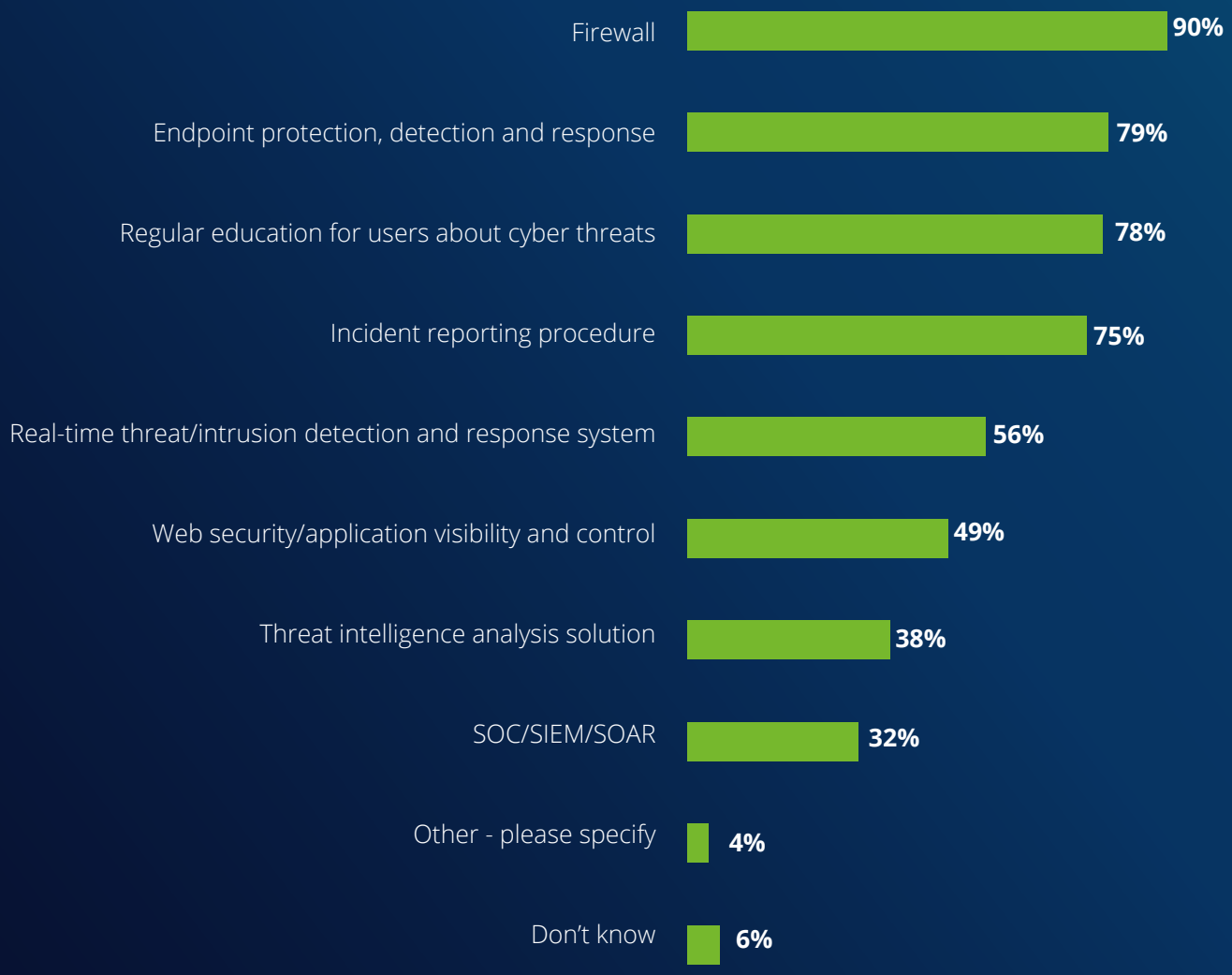
Precautionary measures being implemented and to be considered

To gain a more complete picture of the public sector's current approach to the prevention and containment of cyber breaches, we asked participants what precautionary measures their organisations have put in place. Unsurprisingly, firewall was the fundamental measure.

The prevailing hybrid and remote working trend may be fuelling some of the security concerns, particularly around device proliferation. However, it is encouraging to see that 79% of participants said that their organisation had introduced 'endpoint protection, detection and response' to tackle the emerging security risk.

Moreover, public sector organisations widely recognised the importance in educating users regularly about cyber threats (78%) as well as implementing 'incident reporting procedures' (75%) internally.

FIGURE 1: Which precautionary measures have already been put in place within your organisation?



When asked about the precautionary measures that could bring the most benefit to their organisations, but have yet to be put in place, participants highlighted a variety of measures including 'real-time threat/intrusion detection and response system' (50%), 'SOC/SIEM/SOAR' (24%) and 'threat intelligence analysis solution' (21%).

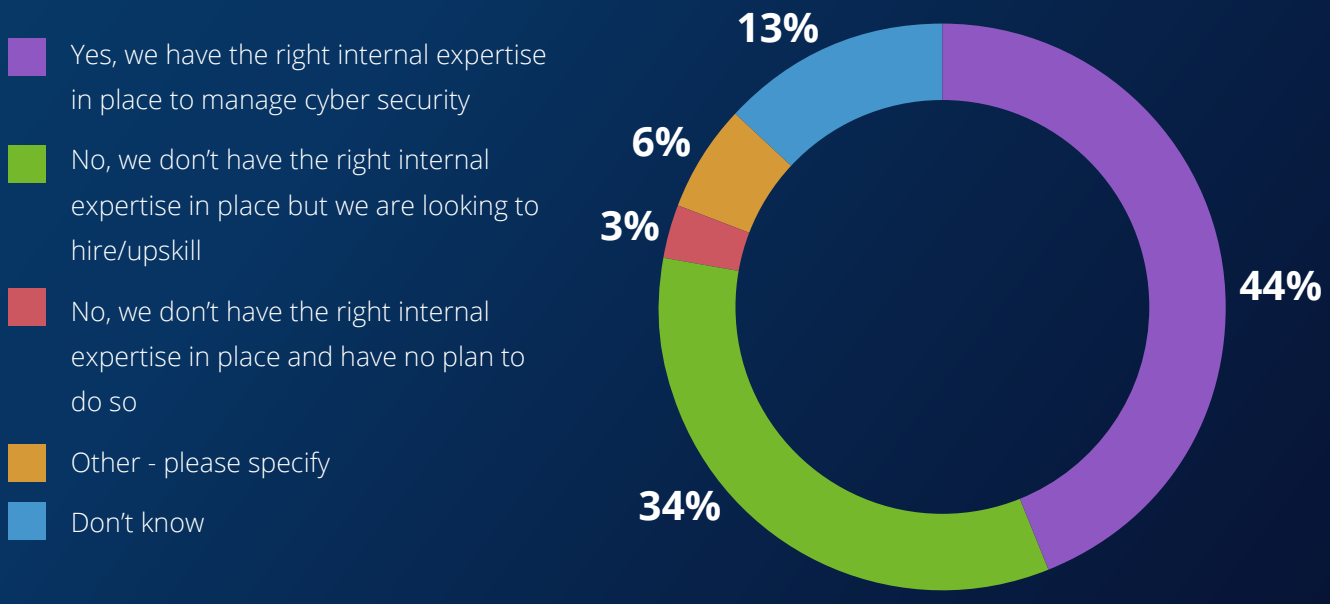
Our participants also reiterated the need to introduce 'regular education for users about cyber threats' (40%).

In broad terms, these findings fall in step with our expectations and indicate that the public sector takes every possible step to manage cyber security in all its forms, albeit to varying degrees.

Greater collaboration between in-house and external expertise could address core challenges

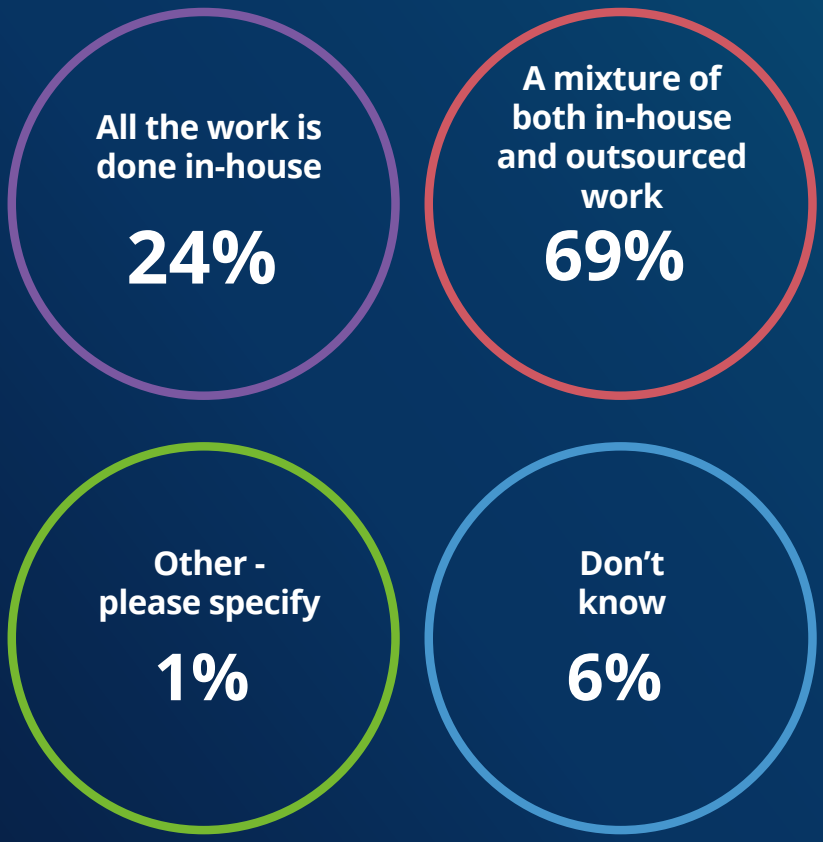
As part of our research, we asked participants whether their organisations have the right internal expertise in place to manage cyber security; 43% don't believe that their organisation has the right internal expertise in place. On this point, one respondent commented: "Nobody has the right expertise really - it's just a case of mitigating to a reasonable extent." However, it is encouraging that 34% are looking to hire/upskill their internal cyber security expertise moving forward.

FIGURE 2: Do you feel your organisation has the right internal expertise in place to manage cyber security?



Given the limited internal resources and the complexity of cyber threats, it is perhaps unsurprising that there is a need to rely on, or partner with, outsourced expertise. In total, 69% of participants said that their organisations are taking 'a mixture of both in-house and outsourced work' to protect business critical information and minimise security risks.

FIGURE 3: Which of the following best represents your organisation's current approach to protecting business critical information and minimising security risks?



Conclusion

It's over five years since the WannaCry ransomware campaign caused serious disruption to public sector systems and just over a year since the Irish HSE suffered a major ransomware attack[3].Today, the findings highlighted in this report demonstrate that the public sector C-suite is better prepared for such a threat, but the goal posts have also moved somewhat. An explosion in remote working endpoints and new technology investments brought about by the pandemic has created fresh security challenges and visibility gaps. At the same time, malicious actors have responded with more sophisticated targeted threats, while long-standing issues around public sector funding remain. The world in which we all work has changed and now, so must we.

It's encouraging to hear that many public sector organisations have come a long way with their cyber security posture under incredibly challenging conditions. The best practices that comprise good IT hygiene, like prompt patching and effective anti-virus are far more commonplace than they were five years ago. But adversaries have also been honing their skills and adapting their tactics with ample support from a vast cyber crime economy. Advanced Persistent Threat (APT) techniques, once the preserve of a limited few, are being widely adopted in "human-operated" ransomware campaigns such as the attack on the Irish HSE.

The public sector is certainly not alone in experiencing these challenges. Many organisations struggle to gain full visibility and control of their IT assets, especially in a new era of mass remote working. They're also impacted by an ever-expanding digital infrastructure to attack, security tool sprawl, the growing expertise of attackers and cyber security skills shortages. But having experienced disruption on a mass scale back in May 2017 and more recently in 2021, the public sector knows first-hand the operational, reputational, and financial damage that a serious cyberattack can have. So where do public sector leaders go from here? What steps do they need to take to prevent ransomware attacks and drive vital digital change?

A commitment to best practices as outlined in Cyber Essentials Plus and the Data Security and Protection Toolkit (DSPT) is important to provide a baseline of good security practice to keep threats at bay. Prompt patching, anti-malware on end-user devices, regular end-user training, network segmentation, strict user access controls and more can often be enough to repel commodity threats. However, the threat from sophisticated cyber crime groups, hackers-for-hire and occasionally even nation state actors means that IT security leaders must go one step further in their efforts. That requires going beyond prevention alone, to also focus on swift detection and response.

3. https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack

Acknowledgements

The research team at Surveys in Public Sector would like to take this opportunity to thank all of those who were able to take part in our poll, particularly those who found the time to offer additional insights through their comments.

We would also like to thank our survey partner, Socura, for their assistance in compiling the questions, scrutinising the responses and analysing the results.

To contact the Surveys in Public Sector team:

Email: enquiries@surveyspublicsector.org
Tel: 0845 094 8567
Address: FAO Surveys in Public Sector,
Pacific House, Pacific Way, Digital Park,
Salford Quays M50 1DR

Surveys in Public Sector

Survey Partner

SOCURA