stotles.

The £22b future of the UK's cyber security

Opportunities for public sector suppliers

August 2022

Contents

Introduction

An introduction

Former CEO of the National Cyber Security Centre, Ciaran Martin said **“a major cyber attack on the United Kingdom is a matter of ‘when, not if’”**.

The need for greater cyber security is inextricably linked to the growing trend of technological advancement across the globe. Cyber threats on a personal, enterprise, and, government level continue to increase.

So, what do increased threats toward government organisations mean for cyber solution suppliers working with the public sector?

This report aims to prove the magnitude of opportunities emerging for cyber security and IT suppliers to work with government organisations over the next decade.

The objective

Using research gathered from Stotles into the current and future cyber security landscape, this report helps you, our reader, accomplish the following:

- Understand and build reliable knowledge of the public sector cyber security market
- Pinpoint areas of the market that present potential opportunities for your business
- Equip yourself with concrete methods and tools for gaining insights and creating real opportunities with public sector organisations

The agenda

The report follows a zoom-out, zoom-in approach, detailing:

- An overview of the evolving cyber security landscape in the public sector
- Concrete methods to proactively create opportunities
- Examples from the Stotles platform of deep insights and opportunities suppliers can use to grow their business, such as, (a) finding existing open contracts, (b) monitoring notable purchasing frameworks, (c) understanding active buyer organisations, (d) sourcing important decision-makers, and (e) following noteworthy suppliers in the space.

The end goal

Ultimately, this report aims to provide you with foundational knowledge, actionable insights, and useful methods that market-leading cyber suppliers use to find, create, qualify and engage opportunities with the public sector. So, let’s get started!

ⓘ **Note:** The contents within this report are subject to change as government cyber security strategies evolve.

The current UK cyber security landscape

stotles.

An overview on the cyber market

A quick skim through the Center for Strategic & International Studies report on Significant Cyber Incidents against government agencies shows a concerning rise in cyber attacks against global powers in the last year alone.

Cybersecurity Ventures predicts the cost of cybercrime to grow by **15% YoY over the next 5 years, totalling $10.5t USD annually by 2025, up from £3t USD in 2015**.

According to a cyber security insights report released by AT&T, this rise in costs represents a monumental transfer of economic wealth. Across the globe, governments are scrambling to ensure tighter cyber security measures to protect their organisations from devastating breaches.

Thankfully, the UK has not seen another cyber incident the scale of the May 2017 WannaCry attack on the NHS. However, central government organisations, local councils and individual politicians continue to be targeted by cyber criminals.

The fallout from a 2020 ransomeware attack cost Hackney Council over £10m to rectify, according to an audit covered in the Hackney Gazzette. The EU Agency for Cybersecurity (ENISA) has described the current age as the "golden era of ransomware", reporting a 150% rise in ransomware attacks between April 2020 to 2021.

Increased cyber threats mean increased demand for cyber solutions. Increased demand means more opportunities for suppliers to work with the public sector. The following sections of this report outline how you can effectively pre-engage with these emerging opportunities and grow your business with the public sector.

> **40% of the cyber incidents managed by the National Cyber Security Centre between September 2020 and August 2021 were aimed at the public sector.**

The market opportunity

According to Fortune Business Insights report "Cyber Security Market 2022-2029", the global cyber security market size is expected to grow 13.4% (CAGR) over the next 8 years, reaching **£305bn by 2029, up from £113bn in 2021**.

The DCMS Annual Cyber Sector Report tracks the performance of the UK's cyber security industry and reported the sector contributed **£5.3 billion to the UK economy in 2021, rising from £4 billion in 2020**.

We're only scratching the surface of the cyber security market in 2022. The future opportunities for suppliers to grow alongside various public sector initiatives is massive.

Monumental government-led cyber initiatives

Increased need for cyber security means increased support from government

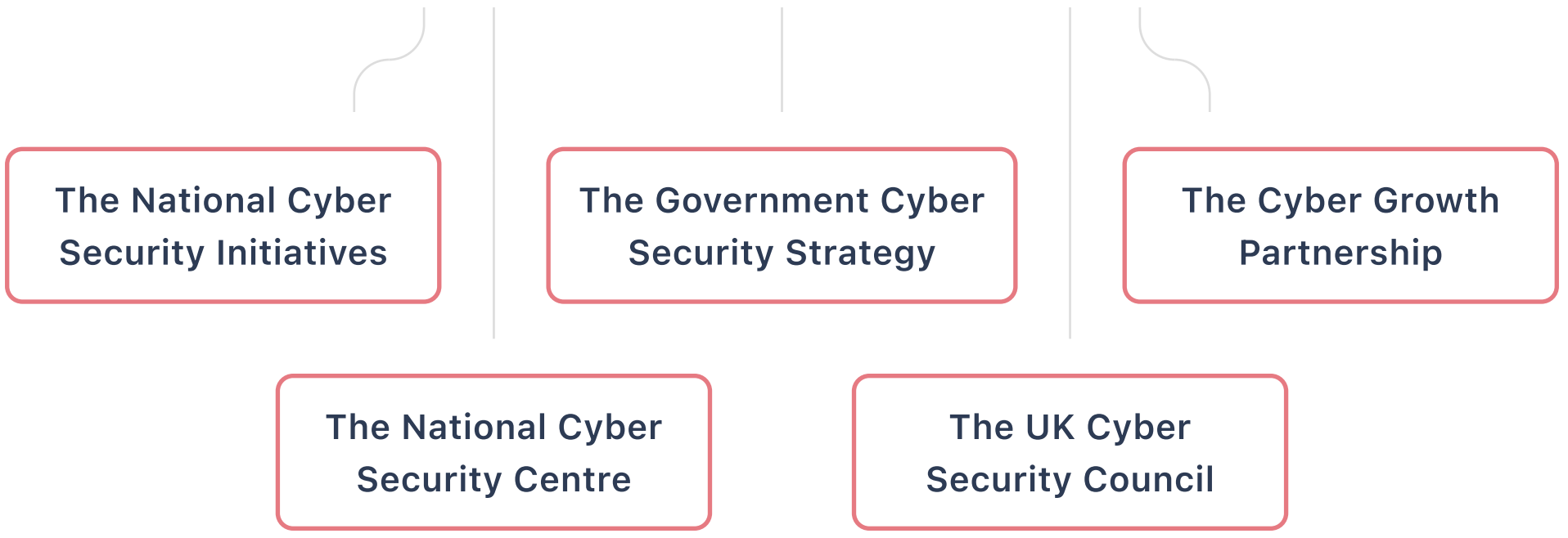
In response to the unprecedented globalisation of the last two decades and the shift to a digital online existence emerging post-COVID19, the UK government has instituted new strategies to tackle the insecure state of the nation's cyber security. These strategies have big implications for government suppliers.

The National Cyber Security Strategy

In January, the new National Cyber Strategy was published, taking over from the previous National Cyber Strategy of 2016, which laid out the UK's aim to be a global leader in cyber.

The strategy sets out the three-year plan to "*ensure the UK remains confident, capable and resilient*", and that government organisations "*continue to adapt, innovate and invest*" in protecting the nation's cyber space.

The following section of this report explores how the UK's National Strategy impacts the public sector's cyber security needs.



Government Cyber Security Strategy

On January 25th 2022, the government launched its first cyber strategy report, named 'Government Cyber Security Strategy - Building a Cyber Resilient Public Sector'. The report outlines the UK public sector's plans to successfully combat and thrive against growing cyber threats over the next 8 years, or until 2030.

The strategy's vision:

The strategy outlines a vision to *"ensure that core government functions are resilient to cyber-attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030."*

Two key pillars emerge from the strategy:

Pillar 1: Build a strong foundation of organisational cyber security resilience

This pillar calls upon every government organisation to build a resilient and impenetrable cyber security system. In other words, organisations must have complete visibility over their entire cyber ecosystem — from IT assets held, to the handling, storage and sharing of data. The pillar implies that improved cyber visibility enables sufficient risk assessment at any given time.

As part of this pillar, government organisations must adopt the National Cyber Security Centre's (NCSC) **Cyber Assessment Framework** (CAF).

The CAF aligns government organisations under a set of industry-standard cyber-resilience protocols. These protocols are underpinned by 39 contributing outcomes, each with a set of indicators and good practice (IGPs) attached that are used to create sector-specific CAF profiles, which provide appropriate and proportionate cyber security measures.

Organisations' assessments of cyber-resilience within the CAF will be verified by independent auditors, ensuring each government body is deemed secure by a third party. The need for third party involvement represents a big opportunity for cyber security auditors and suppliers who can help with verification. To ensure you're aware of these opportunities as they arise, sign up to Stotles.

> **Stotles tip**
>
> The opportunity for suppliers to get involved lies in the cyber solutions needed to achieve the 'contributing outcomes' listed in the third column on the next page.

Cyber Assessment Framework's objectives, principles, and contributing outcomes

OBJECTIVE	PRINCIPLE	CONTRIBUTING OUTCOME
Managing security risk	Governance	Board direction
		Roles and responsibilities
		Decision making
	Risk management	Risk management process
		Assurance
	Asset management	Asset management
	Supply chain	Supply chain
Protecting against cyber attack	Service protection policies	Policy and process development
		Policy and process implementation
	Identity and access control	Identity and verification, authentication, and authorisation
		Device management
		Privileged user management
		Identity and access management (IdAM)
	Data security	Understanding data
		Data in transit
		Stored data
		Mobile data
		Media / equipment sanitisation
System security	System security	**Secure by design**
		Secure configuration
		Secure management
		Vulnerability management
	Resilient networks and systems	Resilience preparation
		Design for resilience
		Backups
	Staff awareness and training	Cyber security culture
		Cyber security training
Detecting cyber security events	Security monitoring	Monitoring coverage
		Securing logs
		Generating alerts
		Identifying security incidents
		Monitoring tools and skills
	Protective security event discovery	System abnormalities for attack detection
		Proactive attack discovery
Minimising the impact of cyber security incidents	Response and recovery planning	Response plan
		Response and recovery capability
		Testing and exercising
	Lessons learned	**Incident root cause analysis**
		Using incidents to drive improvements

Pillar 2: Defend as one

The second pillar aims to better connect government organisations - enabling more effective sharing of data, expertise and capabilities.

A key component of this pillar is the creation of the Government Cyber Coordination Centre (GCCC). The purpose of the GCCC is to "*foster partnerships and share cyber security data and threat intelligence rapidly to identify, investigate and coordinate the response to incidents on public sector systems*", supporting the notion that a more collaborative government means a tighter cybersphere.

The government states a legitimate belief that without robust visibility across every government IT, digital and data asset, cyber security risks go unmanaged on a broad scale.

Five objectives of action

Under the two pillars, the strategy outlines five main objectives. These objectives introduce the five pathways government organisations must follow to ensure the **aims of the strategy are met by 2030**.

OBJECTIVE	DESCRIPTION
Government will manage cyber security risks	Organisations will need to uphold effective risk management processes, governance and accountability to identify cyber threats at organisational and cross-government levels. Cyber security assurance will provide organisations with the visibility necessary over their entire cybersphere to allow for effective decision making. This objective also calls out the importance of long-standing private sector partnerships to enhance the longevity of cyber initiatives.

Stotles tip

Suppliers whose services include **data visualisation**, **data transformation, cyber security consulting** and **secure digitisation of IT infrastructure** will be called upon in Objective 1.

Government will protect against cyber attacks	Organisations will need to adopt proportionate security measures, with centrally developed systems that can protect at scale. Accordingly, organisations must be 'secure by design' and ensure cyber security measures are embedded and appropriately configured across the tech-stack used, and ensure they are continuously developed and updated.

Stotles tip

We predict the need for **artificial intelligence** and **post-quantum cryptography** solutions being necessary for Objective 2.

Government will detect cyber security events	Organisations will need to ensure there is comprehensive monitoring of systems, networks and services to foresee cyber threats before they become incidents. Cross-collaboration and visibility across government organisations will be necessary to ensure a shared detection capability.

Stotles tip

Objective 3 will require suppliers who provide **SOC, 'monitoring & observability tools'** and **Managed Detection and Response MDR** Solutions.

Government will minimise the impact of cyber security incidents

Organisations must respond to cyber security incidents swiftly and enable rapid responsiveness at scale.

Systems and assets affected by cyber incidents need to be assessed as soon as possible, and business as usual must resume as quickly as possible, with minimal disruption.

Cyber Incident Response Providers will be called upon in these situations. The NCSC recommends government organisations work with **Cyber Incident Response** (CIR) certified companies.

Stotles tip

To ensure you are in the running for Objective 4 opportunities, you must certify your company as CIR by submitting this application form.

Government will develop the right cyber security skills, knowledge and culture

Government must continue to develop the country's cyber security workforce, not just in the form of technical cyber security experts, but also in all professions that must effectively incorporate cyber security as part of their practices.

Stotles tip

Suppliers who provide **cyber security training**, **education**, and **development** will be necessary to achieve Objective 5.

Initiatives under each of these objectives have varying prioritisation of go-to-market action, grouped as follows:

- **Immediate transformational initiatives** that must be completed immediately to "*unlock disproportionate benefits across the strategy's outcomes*", meaning immediate need for cyber solutions are known and in-market.
- **Short-to-medium term initiatives** that will be outlined during the first spending review period, meaning upcoming opportunities for cyber solutions are imminent.
- **Medium-to-long term initiatives** that are not yet funded and won't be delivered during the first spending review, meaning long-term opportunities for cyber suppliers to prepare for.
- **Long-term initiatives** at varying stages of development that will be reviewed to ensure alignment against the aim of the strategy (not during the first spending review period).

Supplier opportunity: Cyber Growth Partnership

The Cyber Growth Partnership (CGP) is a joint venture between industry, academia and government organisations, led by techUK. The purpose of the CGP is to "*boost the UK's global market position in cyber security product and services.*"

Under the CGP, a Cyber Security Suppliers' scheme has been developed. The scheme offers an opportunity for cyber suppliers who work with the government to lean on their relationships and leverage government logos when applying for future opportunities.

Cyber Cluster Collaboration

Within the CGP, in conjunction with Department for Digital Culture Media and Sport, and in support of the National Cyber Strategy's goal of continuing to adapt, innovate and invest, a Cyber Cluster Collaboration has been formed.

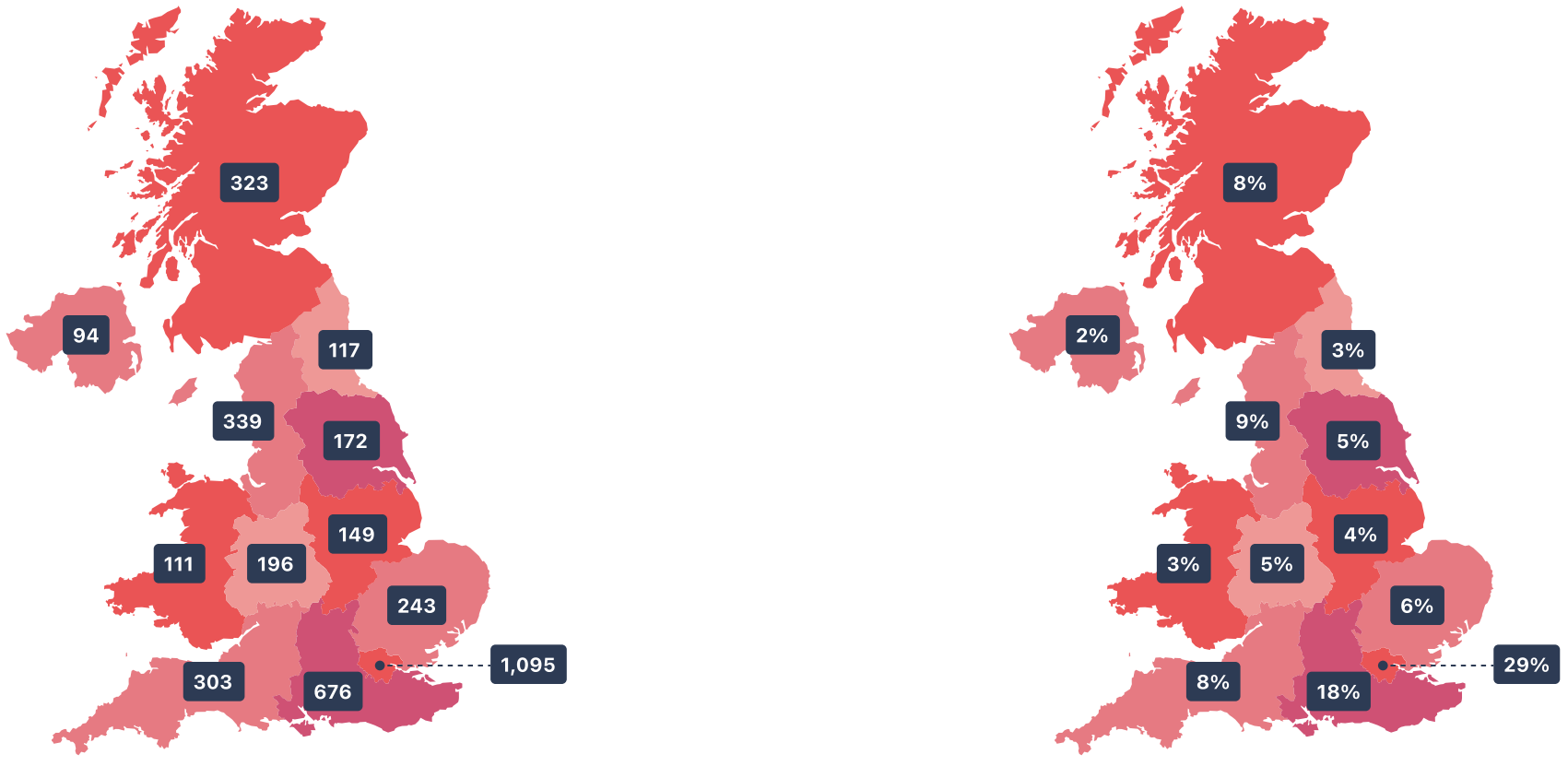
This involves a network of 20 regional clusters of cyber businesses, employers and local organisations to ensure cyber growth is distributed across the nation. The table below showcases the clusters that have been formed and the main contact at each.

CLUSTER NAME	CLUSTER WEBSITE	KEY CONTACT
Bristol and Bath Cyber	bristolandbathcyber.com	tim@lujam.com
Cyber Wales: Capture the Flag	cyberwales.net/clusters/ctf	leanned@cyberwales.net
Critical National Infrastructure in Wales Cyber Cluster	cyberwales.net/clusters/cni	richardr@cyberwales.net
CyberNorth	dynamonortheast.co.uk/clusters/cyber-resilience	phil@guerrillaworking.com
CyNam (Cyber Cheltenham)	cynam.org	info@cynam.org
Education in Wales Cyber Security Cluster	cyberwales.net/clusters/education	kerryb@cyberwales.net
IP Wales Cyber Cluster	cyberwales.net/clusters/ipwales	kerryb@cyberwales.net
MENA Cyber Security Cluster	cyberwales.net/clusters/uae	faheem@cyberwales.net
Midlands Cyber	midlandscyber.com	info@midlandscyber.co.uk
NI Cyber Cluster	nicyber.tech	j.millar@qub.ac.uk
Norfolk and Suffolk Cyber Security Cluster	nscsc.org.uk	contact@nscsc.org.uk
North Wales Cyber Security Cluster	cyberwales.net/clusters/north	jasond@cyberwales.net
North West Cyber Security Cluster	nwcsc.org.uk	vicechair@nwcsc.org.uk
Oxford Cyber Security Cluster	oxcyber.uk/cx	ed.dorling@whitehelm.com
ScotlandIS Cyber	scotlandis.com/scotlandis-cyber	cyber@scotlandis.com
South Wales Cyber Security Cluster	cyberwales.net/clusters/south	johnd@cyberwales.net
South West Cyber Security Cluster	southwestcsc.org	info@southwestcsc.org
Women in Cyber Wales Cluster	cyberwales.net/clusters/womenincyber	clare.johnson@southwales.ac.uk
Yorkshire Cyber Security Cluster	ycsc.org.uk	email@ycsc.org.uk

At the time of writing this report, more than half of the UK's cyber security firms are registered in London and the South East. The map below displays the distribution of registered cyber suppliers across the UK. The clusters aim to aid with this redistribution and allow for more regional opportunities.

Active cyber security offices by region

Source: Perspective Economics (n=3,818)



The creation of the National Cyber Security Centre (NCSC)

The NCSC is a government agency acting as the technical authority for cyber incidents across the UK.

Several cyber initiatives were dissolved into the NCSC to provide a unified national response to cyber threats. These include:

- Government Communications Headquarters' (GCHQ) National Technical Authority for Information Assurance (CESG), the former provider of advise on how organisations protect their network and IT systems from threats
- Computer Emergency Response Team UK, the former computer security incident team
- Cybersecurity Capability Assessment, previously responsible for providing cyber threat assessments to UK government departments
- All cyber functions once part of the Centre for the Protection of the National Infrastructure (CPNI)

The UK Cyber Security Council

The council acts as the expert voice of the cyber security profession in the UK. Its focus is to seek alignment for qualifications and certifications in the sector, and to set the standard for Charted Cyber Security Professionals.

For more information on how to ensure your qualifications are recognised, visit this website.

In this section, we've dissected the government-led cyber security strategies worth knowing about, so suppliers can properly position themselves for major upcoming opportunities.

The next section of the report outlines major funding allocations and initiatives driven by these strategies.

Cyber security budgets across central, local and healthcare organisations

A funding overview: Spending is big, and it's growing

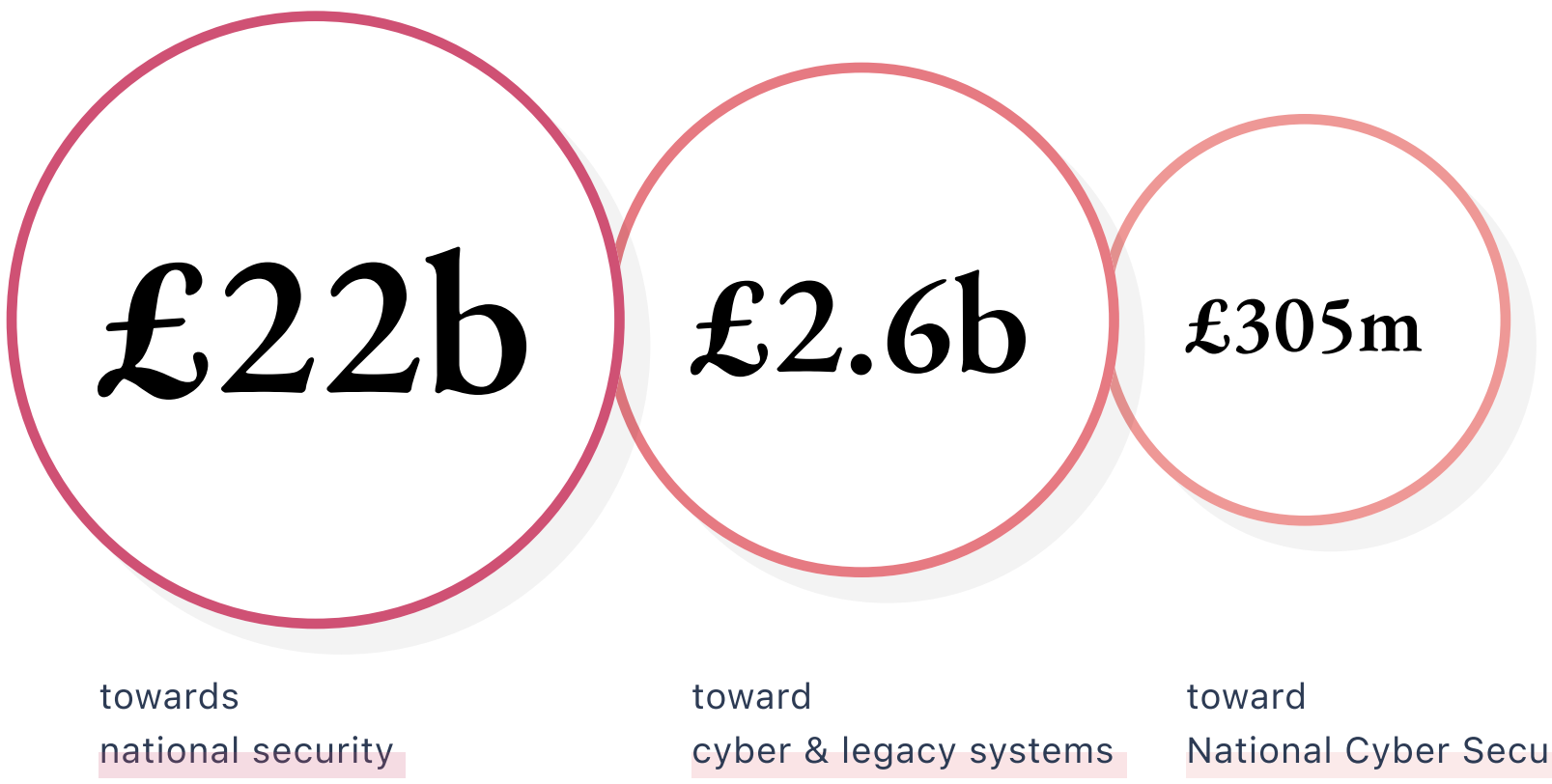
This next section of the report unpacks some of the key budgets and funding allocations currently at play in the public sector cyber security sphere. The aim is to highlight the monumental financial opportunities emerging for cyber security suppliers working with the government in the coming years.

Key public sector cyber funding

The National Cyber Security Strategy has committed **£22b to research, development, and technology** for the UK's national security over the coming years.

Specifically, the government stated in the 2021 Spending Review that it will be investing **£2.6b into cyber and legacy IT systems** over the next three years. This amount far exceeds the £1.9b over a five year period committed in the previous strategy, and we expect spending to increase as cyber threats continue to grow.

For example, the National Cyber Security Strategy outlined a **£114m increase** in the National Cyber Security Programme funding, bringing the total funding of the 2021-22 programme to **£305m**. According to the Integrated Review of Security, Defence, Development and Foreign Policy, the additional investment enables the UK to stay at the forefront of global action to secure a safe digital future and successfully adopt new technology to drive resilience and economic growth.



towards
national security

toward
cyber & legacy systems

toward
National Cyber Security Programme

Spotlight on local government funding

The Strategy allocated an additional **£37.8m to local authorities** to address technology needed to omit cyber security risks.

When combined with the local authority allocation published in the 2020 Spending review, total funding available to local governments is **over £85m**.

Additionally, the Local Government Association has been awarded £1m from the National Cyber Security Programme, enabling local government officers in England to undertake a professionally certified course, as part of a sector-wide skills uplift.

These funding initiatives imply opportunities for suppliers to serve local governments with services, such as cyber security training and solutions.

Spotlight on healthcare funding

The Department of Health and Social Care released a document on the 29th of June 2022 titled 'A plan for digital and social care'.

The report focuses on the digital transformation needed for NHS organisations to meet the challenges of *"2048, not 1948, when it was first established."*

The report stipulates that by March 2025, constituent organisations of an Integrated Care System must have **increased cyber security capabilities, resilience, clinical safety and accessibility**.

Additional key points for cyber suppliers seeking to sell to healthcare buyers:

- Over the next 3 years, **£150m has been provided to enable digital transformation**, including the need for cyber security and resilience solutions and a pledge to 'buy better tech'.
- This winter, the DHSC will publish a Cyber Security Strategy for Health and Social Care to guide NHS organisations on how to build cyber resilience.
  - The report will provide details on DHSC's plan to enhance national protections of the NHS Security Operations Centre, including security monitoring, threat intelligence and national incident response co-ordination.
  - Cyber consultants will be called upon to work alongside local NHS and social care organisations to help manage cyber risks and ensure they are compliant with nationally mandated cyber standards by 2025.

Other notable funding insights

Spotlight on HM Revenues and Customs funding

As mentioned in the Autumn and Spending Review 2021, a priority for government organisations is improving the digital privacy and resiliency of internal IT systems.

According to Think Digital Partners, HM Revenue and Customs is one of the most frequently attacked organisations and considered first-in-line for technological advancements to ensure cyber safety.

In response to this threat, and as part of the Government Cyber Security Strategy, the government has allocated an additional **£468m over the next three years, on top of the £98m allocated in 2021-2022 to HMRC**. The aim of this funding is to help HMRC modernise its IT systems and transform the way the organisation procures IT services to create for more opportunities for smaller businesses.

Using Stotles data, the below table shows a snapshot of five suppliers with which HMRC has engaged on cyber security initiatives in the past 5 years. Understanding the current buyer-supplier ecosystem allows you to identify partner channel opportunities and your competitive landscape.

5 cyber suppliers working with HMRC 2017-2022.

Signal	Supplier Name	No. of Awards	Example contract won
Cloud migration, Cloud security	IBM	11	Cyber Tactical Remediation Delivery Partner
Threat intelligence, Cyber security	Computacenter	7	Threat Intelligence Narrative Reporting
Security architecture, VMware	Capgemini UK	16	HMRC Container Platform Delivery and Support 2022
CHECK, Penetration teseting	Finyx Consulting	13	HMRC Cyber GSeC Consulting
Cloud security, IAM	Equal Experts UK	30	BDEC G-Cloud Support Services

Stotles tip

Stotles tracks key buyer-supplier relationships across the public sector. Successful suppliers map these relationships to understand partner channel opportunities and competitor movement. For insights into supplier relationships of government organisations that matter to you, sign up to Stotles.

Budgets are being allocated to cyber security initiatives across public sector, most notably in central government, local government and healthcare. These flows of funding present huge opportunities for suppliers.

£22m for cyber security in developing countries

The Foreign Secretary, Dominic Raab, announced **£22m of new investment** to build cyber security resilience across the world

- This is a joint venture with Interpol to set up new cyber operations hubs in developing nations
- The initiative will target countries in Africa, the Commonwealth and Indo-Pacific

The next section of this report outlines the actionable steps cyber suppliers can take to create opportunities and win work with the public sector.

By looking at historical data of the typical path to procurement, suppliers can identify certain buying signals helping them get in-the-know and in the conversation for opportunities faster and earlier.

Concrete methods to create opportunities

Concrete ways suppliers can create opportunities and win cyber security contracts

Increased demand for cyber security suppliers and growing budgets for cyber initiatives have resulted in far greater supplier competition.

The major question on the minds of successful suppliers is how to get ahead of tenders and involved with buyer organisations before the competition.

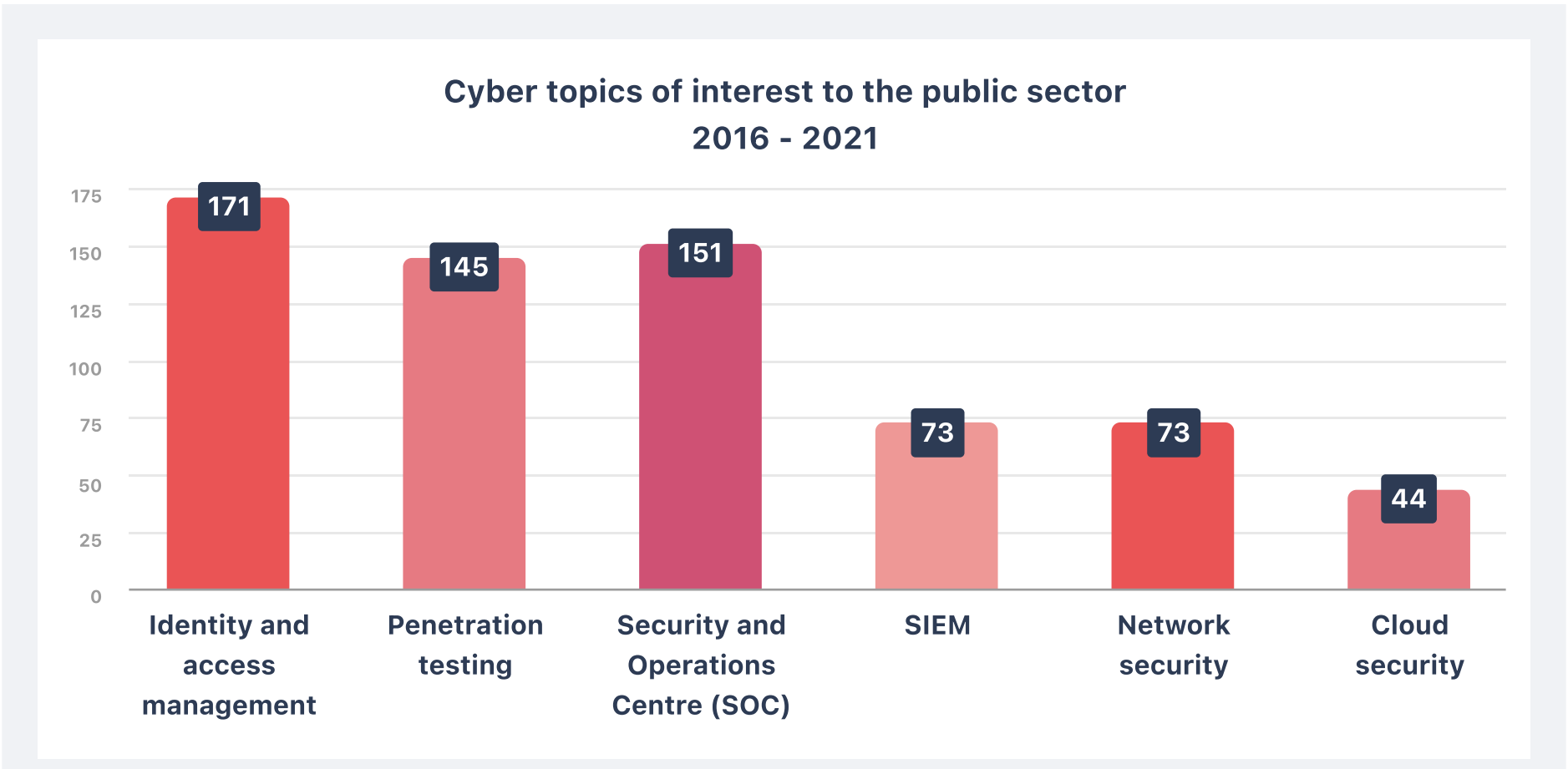
Using Stotles data, this section outlines different methods suppliers can use to to proactively track market signals and create more public sector opportunities. We look at trends in keywords, key purchasing routes and upcoming contract expiries to equip you with legitimate avenues for proactively engaging with the market.

Method 1: Track cyber keyword trends

Tracking keywords is an essential first step towards generating more public sector opportunities. By proactively tracking market signals you can understand what the public sector is asking for and where the opportunities may lie.

We've analyzed various keyword topics relating to cyber security in titles and descriptions of contract data between 2016 and 2021, picking a sample of the most popular terms to indicate key areas of cyber procurement.

Most notably, we found 171 references to 'Identity and access management' solutions, indicating the significant demand that the public sector has had for these solutions and their importance in government cyber security strategies.



Stotles tip

Cyber suppliers can set up custom views based on a multitude of cyber-related keywords that track open, upcoming and awarded contracts in the space. To set up your feed with these custom views for free, sign up to Stotles.

Method 2: Look for buyers starting digital transformation programmes

To understand at which point in the cycle a cyber solution is needed, it's helpful to look at historical data surrounding activity that precedes cyber security specific contracts.

Using Stotles data, we are able to uncover typical procurement activity by buyers before they release cyber security opportunities. In general, tracking signals of digital transformation can lead to uncovering upcoming cyber security opportunities.

The example below follows the University of Sheffield's path to procuring Endpoint Detection & Response (EDR) and Next-Gen Antivirus (NGAV) software as part of their cyber security tech stack.

EVENT #1
January 2021

In January 2021, the university was hiring for digital transformation consultants under this '**Interims for Digital Transformation, Business Change and BAU**' contract.

The contract was awarded to Real Staffing Group and was valued at £750,000 GBP.

EVENT #2
March 2021

Two months later, in March 2021, the university awarded Bloom Procurement Services the right to run a digital transformation and legacy system contract, named 'Data Migration Services for Interim Module Management in SLP'.

The contract called for data migration services from legacy systems to the Univeristy's new systems.

The contract lasted less than four months and had a value of £62,000 GBP.

Awarded

2883/MH Data Migration Services for Interim Module Management in SLP

University of Sheffield

Supplier(s) awarded	Value	Signals
Bloom Procurement Services Ltd	62,000 GBP	Legacy systems

Timeline

Award date	Contract start *	Contract end *
2021-03-22 a year ago	2021-03-25 a year ago	2021-07-02 a year ago

EVENT #3
January 2021

Three months after that, in June 2021, we saw the shift to requiring specific cyber security solutions occur via the release of this Endpoint Detection & Response (EDR) and Next-Gen Antivirus (NGAV) Software and Associated Services contract.

In the last month of the previous data migration contract, the university awarded Softcat PLC the above contract via the Software Products and Associated Services Framework.

This contract has a value of approximately £350,000 GBP and spans over three years.

● Awarded

2924/HP - Endpoint Detection & Response (**EDR**) and Next-Gen Antivirus (NGAV) Software and Associated Services

University of Sheffield

Supplier(s) awarded	Value	Signals
Softcat PLC	347,887 GBP	Cybersecurity EDR

Timeline

Contract start *	Award date	Contract end *
2021-06-09 a year ago	2021-06-09 a year ago	2024-06-08 in 2 years

The aim of this example is to show that early signals of digital transformation can act as indicators of downstream cyber security opportunities.

This type of analysis can be repeated across different signals. For example, if you provide ISO certifications, it is a good idea to track when government organisations complete cyber security audits, as it often precedes needing a certification.

To keep track of recently awarded digital transformation contracts and predict buyers who may require cyber security services, see this feed of digital transformation awards or sign up to Stotles.

Method 3: Monitor expiring cyber contracts

Another way suppliers can create more opportunities is by monitoring upcoming expiring contracts.

Given the extensive need for ongoing cyber security services, much of government procurement of cyber services happens on a recurring basis. Keeping track of upcoming contract expiries means suppliers can prepare ahead of time to win potential contract renewals.

Below are several examples of major cyber contracts expiring in the next 6 months that suppliers can use as a basis for focusing on which buyer relationships you want to build.

DLUHC CHECK Penetration Services

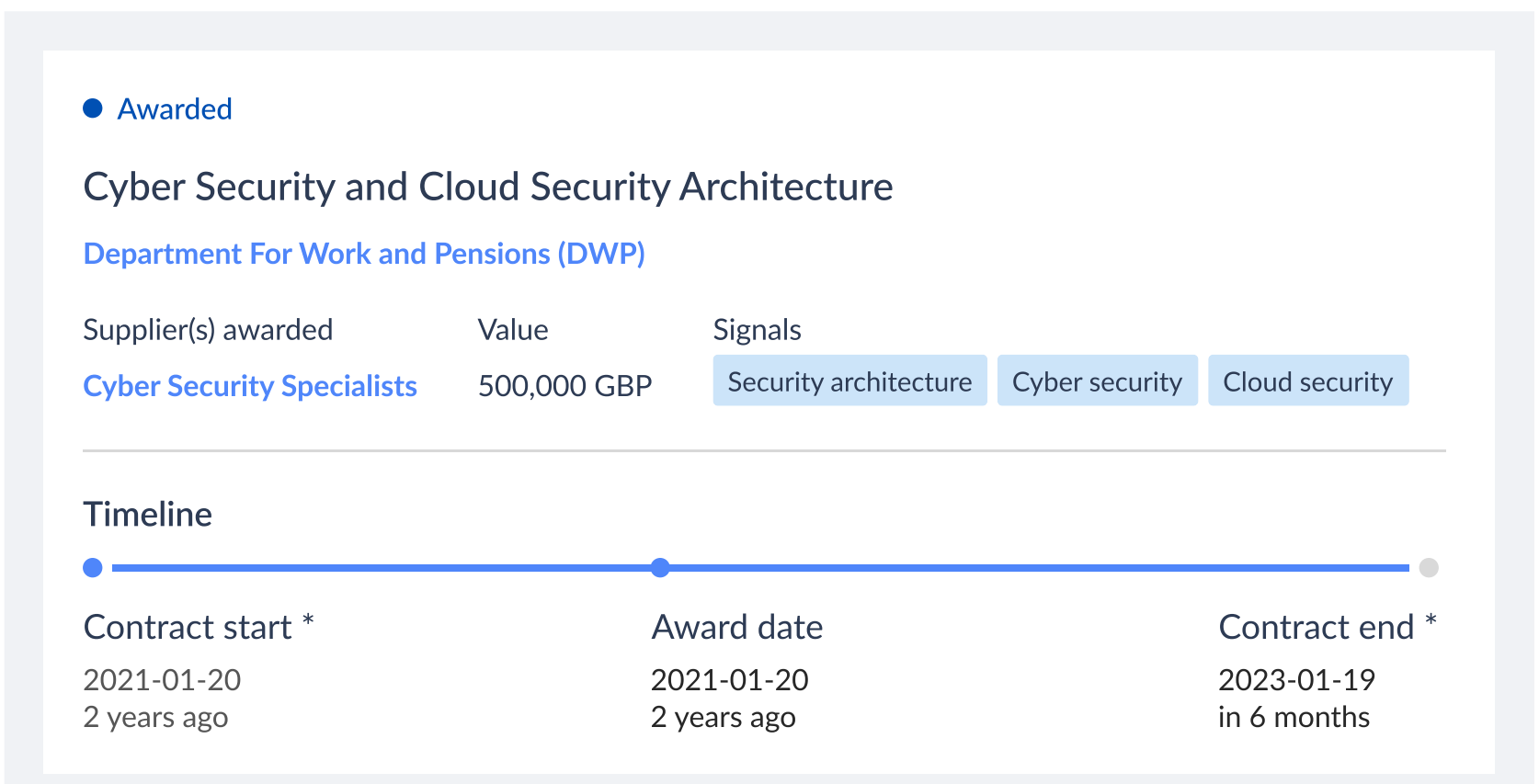
The Department for Levelling Up, Housing and Communities (DLUHC) awarded Arcturus Security Limited the below contract on CHECK penetration testing services across their organisation. This contract ends in January, 2023.

- For a more in-depth look at DLUHC's procurement activity, view their Stotles buyer profile

Cyber Security and Cloud Security Architecture

Cyber Security Specialists were awarded this Cyber Security and Cloud Security Architecture contract from the Department For Work and Pensions (DWP). This particular contract ends in 7 months (at the time of releasing this report).

- For a more in-depth look at DWP's procurement activity, view their Stotles buyer profile



CISO Penetration Testing Provision

UK Health Security Agency awarded NCC Group Security Services this CISO penetration testing contract to provide a range of cyber security related solutions. This contract ends in August, 2022.

- For a more in-depth look at UK Health Security Services' buyer activity, view their Stotles buyer profile
- For a more in-depth look at NCC Group's supplier activity, view their Stotles supplier profile

● Awarded

CISO Penetration Testing Provision

UK Health Security Agency

Supplier(s) awarded	Value	Signals
NCC Group Security Services Ltd	55,000 GBP	CHECK, "IT health", Threat intelligence, Cyber security, Penetration testing

Timeline

Award date	Contract start *	Contract end *
2022-05-31	2022-06-01	2022-08-30
2 months ago	2 months ago	in 27 days

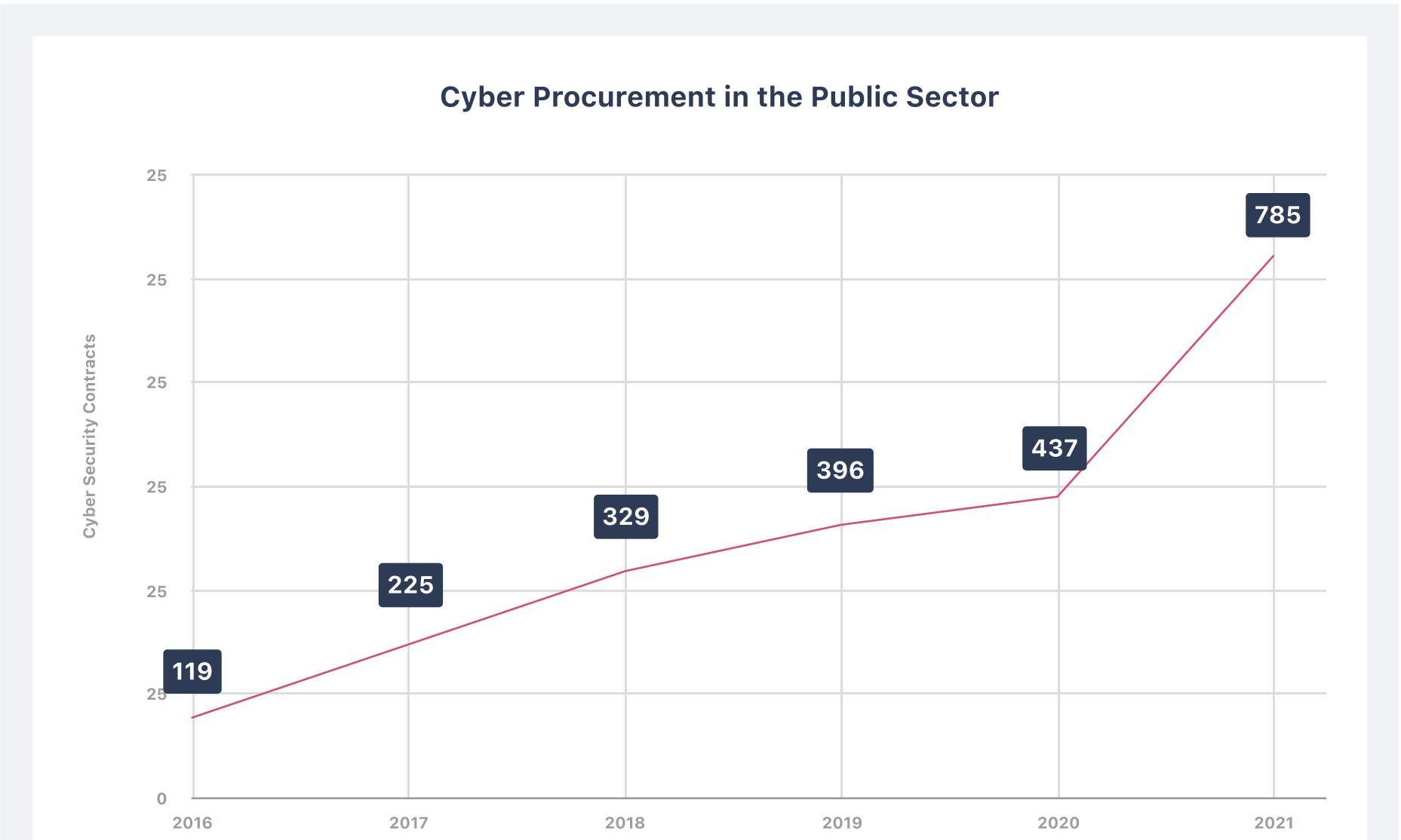
This section of the report aims to equip cyber suppliers with methods that help you proactively engage with government buyers before they go to public tender. By tracking cyber-related keywords, typical early signals of cyber spending (eg: digital transformation) and monitoring upcoming contract expiries, you can adopt a more proactive sales and marketing approach to find your next opportunity before it goes to tender.

Noteworthy purchasing frameworks and open contracts

stotles.

Cyber procurement across the public sector

We can confidently say it is the most prosperous time for cyber suppliers to work with the government. The below chart shows the increase in publicly reported cyber security award activity across the entire public sector between 2016 and 2021.



But, where are these awards happening? By analysing the procurement methods leveraged by public sector buyers, suppliers can better position themselves to win more work. The following section provides insight into live open opportunities and major frameworks across government organisations worthy of suppliers' attention (at the time of writing this report). It also highlights the ways that leading suppliers use Stotles to find opportunities and framework agreements in the market, using a range of examples of real cyber security procurement.

Live and upcoming open contracts

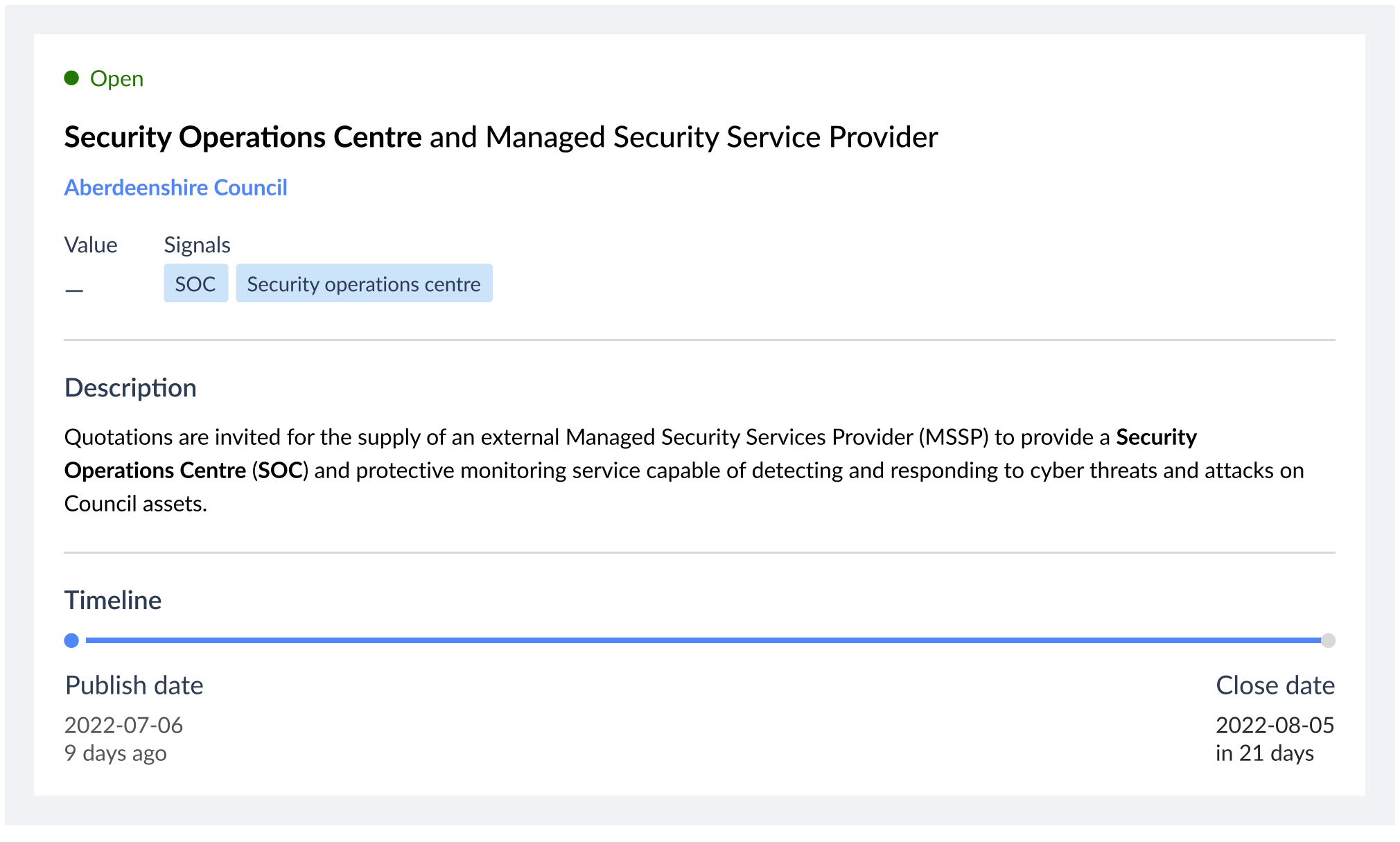
Below is a list of open tenders currently live and available for cyber supplier bidding. Chasing tenders is not the business development strategy successful suppliers use, but being aware of open tenders is necessary to ensure you're aware of what's going on in the market.

To keep track of open opportunities, bookmark this Stotles Cyber Opportunities Feed, or sign up to Stotles for free today.

Example 1: Security Operations Centre and Managed Security Service Provider

Aberdeenshire Council is looking for a supplier to provide a SOC and protective monitoring service to detect and respond to cyber attacks on council assets.

For a more in-depth look at Aberdeenshire's procurement activity, view their Stotles buyer profile



Example 2: SentinelOne EDR Licences

The Department of Agriculture, Food and the Marine is looking for an Endpoint Detection and Response (EDR) supplier to improve its cyber security posture and assure they are compliant with security standards.

● Open

SentinelOne EDR Licences

Department of Agriculture, Food and the Marine

Value	Signals
–	Detection and response, Cybersecurity, EDR

Description

In line with this strategy, DAFM will be migrating some IT services to the Office of the Government Chief Information Officer (OGCIO) to be delivered under their Build to Share (BTS) Managed Desktop Service.

Timeline

Publish date	Close date
2022-07-29 4 days ago	2022-08-22 in 20 days

Example 3: Cyber Security Criticalities Assessment Service

The Home Office is seeking a supplier to design, develop, deliver and refine a Criticalities assessment process to be used within the Assurance Process across the Home Office.

● Open

Cyber Security Criticalities Assessment Service

Home Office

Value	Signals
400,000 GBP	Cyber security

Description

The Home Office is seeking a service provider to Design, Develop, Deliver and Refine a Criticalities assessment process for the Home Office, considering the business impact of Home Office Assets, intended to deliver a corporate cyber security criticalities assessment to be used within the Assurance Process across the Home Office.

Timeline

Publish date	Close date
2022-07-28 6 days ago	2022-08-11 in 8 days

Key frameworks and dynamic purchasing systems

Many cyber security initiatives are purchased through framework agreements as part of larger technology and digital programmes. For suppliers, knowing the right cyber and digital frameworks utilised by buyers is an important gateway to winning work.

IT Infrastructure 2022

Locala Community Partnerships CIC has released this prior information notice (PIN) for an upcoming framework which requires an independent supplier to provide security operations centre solutions.

- This PIN was released on 5th of May 2022 and has an estimate framework value of £10m.

Pre-tender

IT Infrastructure 2022

Locala Community Partnerships CIC

Value

10,000,000 GBP

Signals

Security operations centre

Description

Lot 1 - 1st, 2nd and 3rd line support services. Lot 2 - Network Management Services.
Lot 3 - **Security Operations Centre**. Lot 4 - Cloud Management Print Services.

Timeline

Publish date

2022-05-05

Cyber Security Services 3 Dynamic Purchasing System (DPS)

Cyber Security Services 3 is £153m flexible commercial agreement run by Crown Commercial Services. The DPS is available to, and used by, central, local, third party government organisations and charities to procure for cyber security solutions.

● Open

Cyber Security Services 3 DPS

Crown Commercial Service

Value	Signals
153,000,000	Cyber security

Description

Crown Commercial Service (CCS) is setting up a dynamic purchasing system for a period of 36 months and is inviting bidders to request to participate for the Cyber Services 3 DPS.

Timeline

Publish date	Close date
2020-01-14 3 years ago	2023-02-11 in 7 months

Below are two examples of cyber security contracts awarded through this DPS:

- HM Land Registry (HMLR) awarded NTA Monitor this Penetration Testing Services contract in June 2022, valued at £1.53m.
- This Cyber Incident Response Retainer and Advisory Service contract, valued at £450k was awarded to Deloitte by Ulster University in March 2022.

GCloud 13 Framework

GCloud 13 is one of Crown Commercial Services' major digital frameworks. Lot 2 of the framework is dedicated to Cloud Software, with cyber security software falling under this category.

Suppliers involved in GCloud13 have not yet been selected or published at this time, but once they are, they will be visible in Stotles, which can help suppliers not on the GCloud 13 framework identify potential partners and resellers with which they can begin building relationships.

● Closed

G-Cloud 13

Crown Commercial Service

Value	Signals
4,000,000,000 GBP	Cyber security

Description

The maximum initial duration of any call-off contract that may be placed by an eligible contracting authorities is 36 months with one extension allowed, up to 12 months. G-Cloud services, available via the digital platform, will require frequent procurement refreshes to bring on new suppliers and services.

Timeline

Publish date	Close date
2022-03-08 5 months ago	2022-05-18 2 months ago

Below are two examples of cyber security contracts awarded through the previous iteration of this framework, G-Cloud 12:

- This Threat Led Cyber Security Transformational Change for PLASMA contract was awarded to BAE Systems Applied Intelligence Ltd by NHS Blood and Transplant.
- National Employment Savings Trust (NEST) awarded Deloitte this Provision of incident response support and remediation resource contract in January 2022, valued at £50k.

Stotles tip

There are many routes of purchasing used by government buyers. Staying on top of new key frameworks is vital in eliminating the risks of (a) being blocked from proper routes to market, and (b) missing opportunities.

Our framework intelligence can help you monitor new framework movements and track key buyers' activities via frameworks across the market. To better understand major upcoming cyber frameworks and how to leverage them, chat to our team.

NIS Directive = Billions in cyber funding across Europe

For readers who supply outside of the UK in the EU region, the Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cyber security.

NIS Directive 2 aims to elevate the level of cyber security for entities in critical sectors of the EU economy and society by categorising entities as 'essential' and 'important'.

Funding for the current period (2021-2027) will happen through various initiatives, including:

- European Defence Fund (EDF): **€7.9b** toward the European Defence Fund
- Digital Europe Programme: Cyber security budget of **€269m** until the end of 2022
- Horizon Europe Project: **€67.3m** added to the cyber security budget in 2022

This section of the report has featured a sample of the many existing procurement contracts, notable purchasing frameworks and dynamic purchasing systems being used to purchase cyber security solutions and services. As the need for cyber security solutions continues to grow across every digital initiative, we expect significant increases in volume of cyber security tenders and frameworks to hit the market.

Major government buying activity to track

Key government buyer movements to watch

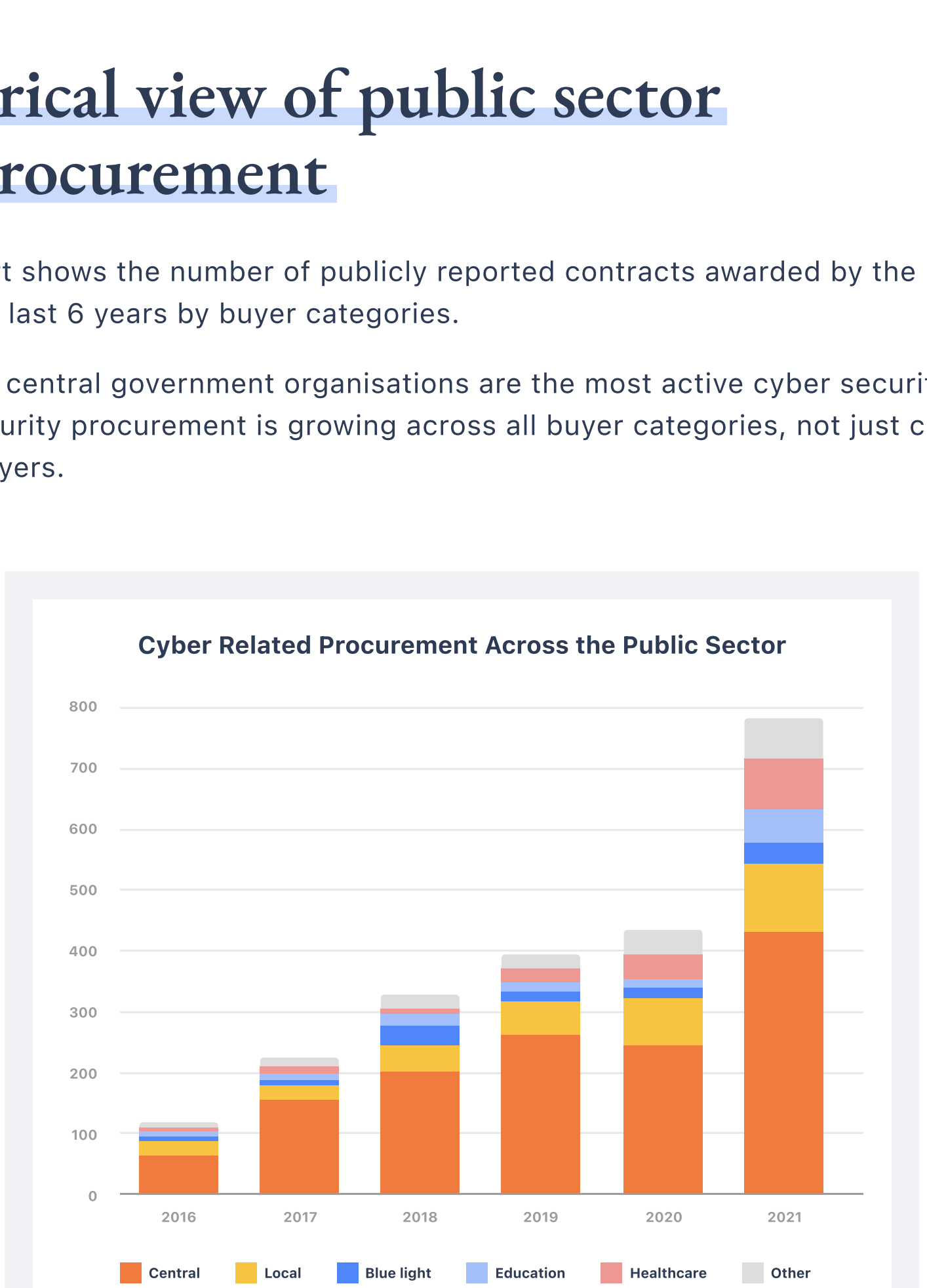
As the need for cyber security services continues to multiply across government organisations, the market's leading suppliers are spending more time monitoring and acting on buyer activities.

Using Stotles data, this section analyses the historical cyber security purchasing activity of government organisations. First, we'll assess the high-level trends exhibited across all buyers of cyber security services and solutions in the public sector. Then, we'll dig into central and local government cyber procurement activities. In doing so, we'll lean on two buyers showing significant activity in the cyber security space: a central government organisation (HMRC) and a local council (Kent County Council).

A historical view of public sector cyber procurement

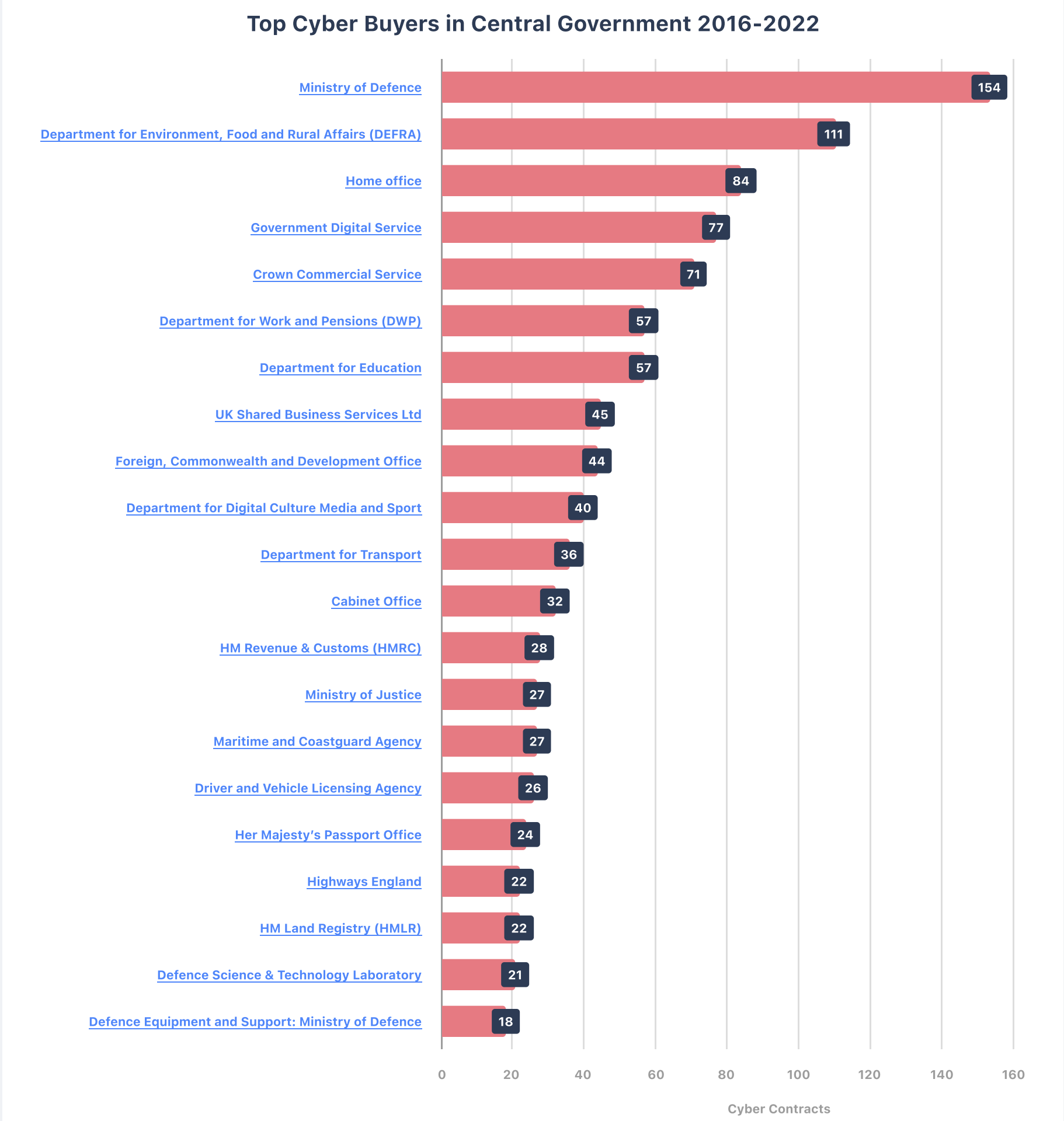
The below chart shows the number of publicly reported contracts awarded by the UK's public sector over the last 6 years by buyer categories.

Unsurprisingly, central government organisations are the most active cyber security buyers. That said, cyber security procurement is growing across all buyer categories, not just central government buyers.



Cyber security purchasing in central government

The chart below illustrates the cyber security procurement activity of central government organisations based on publicly reported contracts, over the last 7 years.



Stotles tip

Once you've identified active buyers in your market, you can prioritise where to focus your efforts. Stotles buyer profiles give suppliers an in-depth view of procurement activity, key supplier relationships and access to decision-maker contact details. To find out more, sign up to Stotles.

Central government buyer spotlight: HM Revenue and Customs

HMRC has been awarded over £500m to modernise their IT solutions and ensure their cyber security systems are as secure as possible.

In section four of this report we illustrated some of the key relationships HMRC has with cyber security suppliers. Now, we can unearth deeper insights into their movements using Stotles' buyer profiles, including a summary of their procurement activity, a spotlight on their upcoming contract expiries and examples of key decision-maker contact details.

Using this buyer profile, suppliers can gain deep insights that help you create the most informed outreach plan, identify the right people, develop the best outreach messaging, and engage at the right time.

A summary of HMRCs procurement activity

HM Revenue & Customs (HMRC)

London, United Kingdom | Central / Non-ministerial department | www.gov.uk/.../hm-revenue-customs

NUMBER OF EMPLOYEES
20000+

ANNUAL SPEND
Over £1B

Upcoming contract expiries | In the next 1 year | See expiries matching my settings

Number of contracts and frameworks awarded
137

Total contract and framework value
£483,640,578.5 GBP

Average contract and framework value
£3,556,181 GBP

% of contract and framework value awarded to SMEs
25.5%

IT services: consulting, software development, Internet and support
50
£131,531,987

Business services: law, marketing, consulting, recruitment, printing and security
19
£258,639,317

Research and development services and related consultancy services
17
£2,890,000

Software package and information systems
15
£23,725,904

Furniture (incl. office furniture), furnishings, domestic appliances, ...
10
£231,302,811

Upcoming contract expiries

The below graphic highlights HMRC's upcoming cyber security contract expirations. By tracking upcoming contract expiries, suppliers can keep an eye on potential renewals ahead of time and begin to pursue a relationship with the buyer.

Signals	Title	Expiry date	Value
Vulnerability assessment, Cyber security	Tenable Vulnerability Assessment Scanning Tool	2023-09-02	£259k
Cyber security, IT health	Auxiliary Transition Resource Tender	2024-07-03	£29.6m
Security assessment, Penetration testing	Cyber Security Services	2023-03-14	£1m

Key decision maker contact details

Stotles buyer profiles offer contact information of key decision makers within buyer organisations. Below is a glimpse into some of the key decision-makers within HMRC suppliers can build a tailored outreach approach for.

Decision-makers Procurement

Filter by: Seniority Function

Chief Officer

First Permanent Secretary and Chief Executive
Jim Harra
[redacted]

Second Perm Secretary
Angela MacDonald
[redacted]

C-level & Execs

Chief Finance Officer
Justin Holiday
[redacted]

Director General Transformation
Joanna Rowland
[redacted]

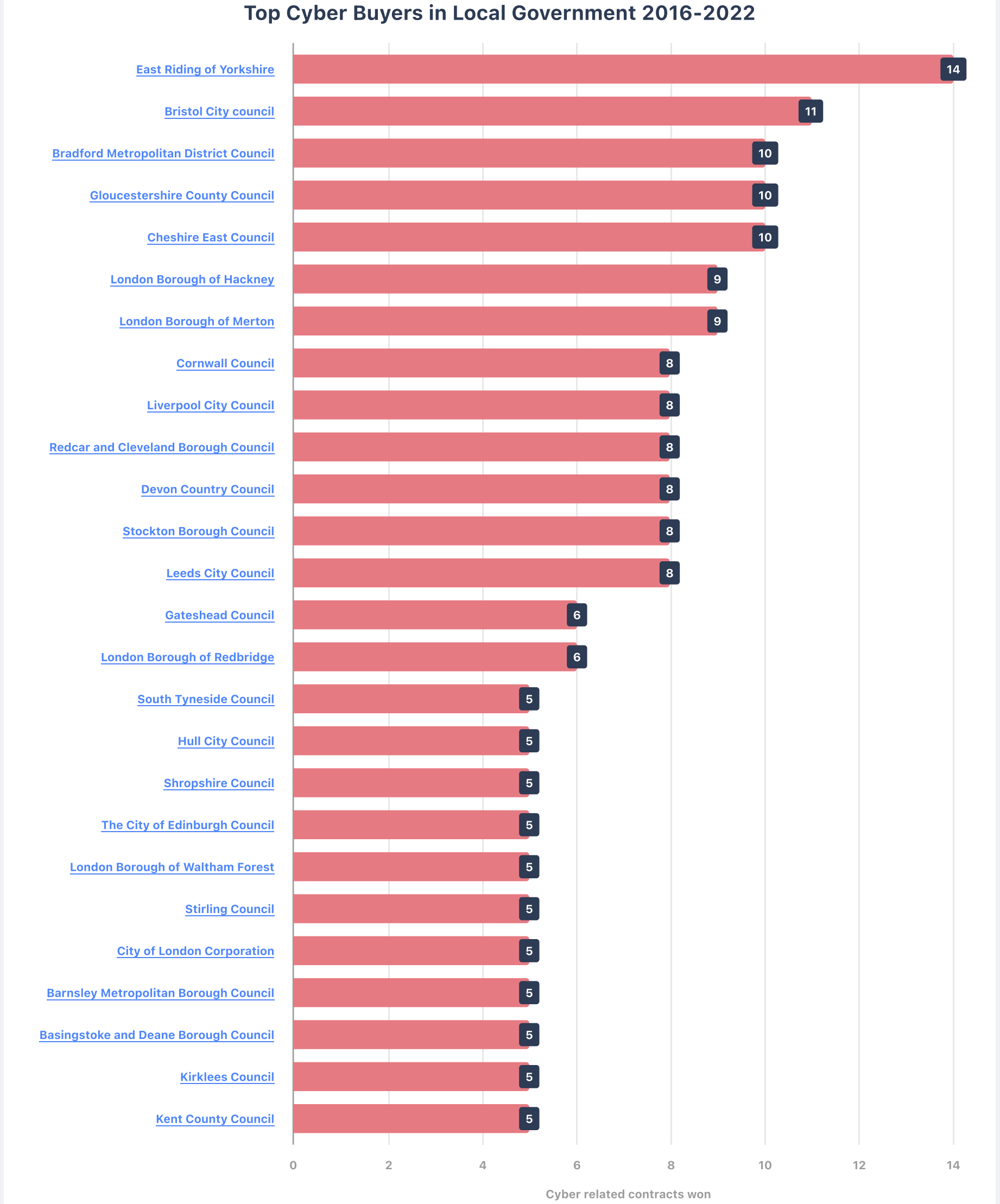
Stotles tip

The top suppliers track upcoming contract expiries to get ahead of future opportunities, then locate decision maker contacts within buyer organisations. After gathering this data, suppliers create tailored account plans and begin to build relationships.

Cyber security purchasing in local government

The graph below shows the cyber security procurement activity of local government organisations based on publicly reported contracts, over the last 7 years.

Whilst East Riding of Yorkshire has been the most active overall, Cornwall Council and The City of Edinburgh Council have been the most active this year.



Local government buyer spotlight: Kent County Council

As mentioned at the beginning of this section of the report, cyber security procurement by local councils continues to increase. We've spotlighted Kent City Council as an example of one local authority procuring for cyber security solutions.

A summary of Kent County Council procurement activity

Kent County Council

Maidstone, United Kingdom Local / Local authority www.kent.gov.uk

NUMBER OF EMPLOYEES
20000+

ANNUAL SPEND
Over £1B

Summary Contacts Procurement activity Suppliers

Upcoming contract expiries In the next 1 year See expiries matching my settings

Number of contracts and frameworks awarded
86

Total contract and framework value
£327,536,401.4 GBP

Average contract and framework value
£4,199,185 GBP

% of contract and framework value awarded to SMEs
20.9%

Education and training services
9
£497,018

Construction work
8
£231,302,811

Business services: law, marketing, consulting, recruitment, printing and security
8
£2,733,973

IT services: consulting, software development, Internet and support
8
£678,840

Software package and information systems
6
£1,367,049.4

Upcoming contract expiries

In November 2021, Kent City Council awarded Boxxe Limited a contract named SIEM Log Event Management System to monitor their security posture using log files. This contract is set to expire on October 31, 2022.

● Awarded

SS14144 - SIEM Log Event Management System

Kent County Council

Supplier(s) awarded	Value	Signals
boxxe Limited	17,550 GBP	SIEM

Description

SS14144 - SIEM Log Event Management System provision & support (Logpoint)

Timeline

Publish date	Award date	Contract start *	Contract end *
2021-10-05 9 months ago	2021-10-05 9 months ago	2021-11-01 9 months ago	2022-10-31 in 4 months

Key decision maker contact details

We've extracted some of the key decision maker contacts within Kent City Council for suppliers to use in their outreach approach.

Decision-makers | Procurement

Filter by: Seniority ∨ Function ∨

Chief Officer

Corporate Director Strategic & Services
David Cockburn
[redacted]

C-level & Execs

Corporate Director - Finance
Zena Cooke
[redacted]

Head of Financial Operations
Catherine Head
[redacted]

Director of Infrastructure
Rebecca Spore
[redacted]

Stotles tip

Stotles buyer profiles help suppliers unlock insights which inform a faster, more relevant outreach approach. To access key details on the buyers that matter to you, sign up to Stotles.

This section of the report illustrates the noteworthy cyber security procurement activity across a range of government buyer organisations. Suppliers who have a clear understanding of the buyers who are active in the space can prioritise their sales efforts, locate decision maker contact details and build the most informed account plans to win public sector work.

Key cyber security suppliers leading the charge

stotles.

Key suppliers dominating the cyber security space

As the public sector demand for cyber security solutions has increased, so too has the number of cyber security suppliers in the market. Many successful suppliers take a channel partner route into the public sector. Understanding the key suppliers already working withing the government can provide gateways, or “warm ins”, into buying organisations, which can lead to downstream sales opportunities.

This section of the report showcases the top cyber suppliers working with the public sector, and concrete methods of using supplier intelligence to gain more traction in the market.

A look at the top 10 most active cyber security suppliers

The bar chart below displays the top suppliers active with government buyers, and how many reported contract awards they have received over the last 5 years.

The prevalence of VARs in the above graph indicates the importance of having strong partner channels in this space.

Stotles tip

Understanding the top players in the public sector cyberspace gives you complete visibility over the market. You can track competitor movement and identify partner channel opportunities for your business. For a deeper dive into supplier movement, sign up to Stotles.

Opportunities for cyber security SMEs

The suppliers winning the largest number of contracts tend to be large enterprise corporations and value-added resellers (which indicates the importance of having strong partner channels in this space), not SMEs. However, numerous opportunities and initiatives exist to enable SME involvement in public sector cyber market. The following section shines a light on how SMEs can get involved through local councils.

In February 2022, the Department for Levelling Up, Housing and Communities released their white paper titled, 'Levelling Up the United Kingdom'. A major component of this paper focused on local authorities reforming their procurement practices to better support small, local businesses.

The White Paper notes the government will introduce laws to "*make it easier for small businesses and social enterprises across the country to bid for and win public contracts*".

This shift toward supporting SMEs taps into the growing importance of 'social value' factors for suppliers. Social value factors refer to how buyer organisations can award contracts to suppliers that support local communities and disadvantaged groups.

The below example showcases an instance where a local authority awarded a pivotal cyber security contract to a local SME in London.

Stotles tip

We expect more local authorities to continue to procure for cyber solutions via local supplier solutions as budgets increase. To ensure you're aware of SME opportunities in your area, sign up to Stotles.

Cyberscout Limited <> London Borough of Hackney spotlight

In the introduction of this report, we touched upon a recent ransomeware attack against London Borough of Hackney's data. In response to this attack, the borough had to respond swiftly to the incident.

London-based SME Cyberscout was awarded the Cyber Security Response Services contract for the provision of cyber attack data mitigation, including call handling and credit monitoring services.

Cyberscout Limited

Country	Region	SME
United Kingdom	London	No

Top buyers supplied

Contracts awarded	Buyer	Latest activity	Country
1	London Borough of Hacnkey	2021-10-29	United Kingdom

Contracts won

Award date	Title	Expiry date	Country	Value
2021-02-19	Cyber Security Response Services	2022-05-10	United Kingdom	£50,000 GBP

This section of the report showcases insights Stotles provides on supplier movement so you can identify key partner channel opportunities and competitor activity.

Tracking supplier ecosystems allows you to gain in-depth understanding over the market, relevant to your partners and competitors. To access a briefing on key buyer-supplier relationships that matter to you, sign up to Stotles.

Summary

Summary

This report explores the magnitude of opportunities available for cyber security suppliers in the public sector.

The specific examples used throughout the report showcase the refinement and relevancy that is possible with Stotles. All of the data relating to specific funding, open opportunities, frameworks, buyer organisations and supplier relationships can be uncovered for opportunities relevant to your business.

To find out more about how Stotles can drive sales productivity for your team, contact our team at team@stotles.com or sign up to the free version of our platform at www.stotles.com.

The release of this report supports our mission to unlock the potential of businesses and government working better, together.

More on Stotles

We combine millions of UK & EU buying signals and opportunities into one view, tailored to you. Our aim is to help suppliers:

Find early signals

Get notified about public sector opportunities via curated **prospecting reports** and **live feed** **notifications**

Understand buyer behaviour

Gain a deeper understanding of buyer activity and trends with **account briefings** and **buyer profiles**

Locate important prospects

Directly reach the people that matter with **decision-maker contact details** and discovery

Inform targeted outreach

Develop a compelling outreach strategy with **persona briefings** and **buyer profiles**

Analyse competitor landscape

Identify key incumbent suppliers and explore future opportunities with **upcoming contract expiries** and **supplier profiles**

Map partner ecosystems

Discover alternative routes to market with **partner mappings** and **briefings**

Resources

Government resources

We relied on these government resources to inform this report. Suppliers should monitor these resources for potential updates throughout 2022.

Autumn Budget and Spending Review 2021

Read article

Cyber Exchange: Cyber Clusters

Read article

Cyber Incident Response: Certified Suppliers

Read article

Cyber Security Sectoral Analysis 2022

Read article

Cyber Security Supplier to Government Scheme

Read article

Government Cyber Security Strategy

Read article

Levelling Up the United Kingdom

Read article

National Cyber Strategy

Read article

Integrated review of Security, Defence, Development and Foreign Policy

Read article

News sources

In conjunction with the Stotles platform and the resources linked throughout the report, we relied on information from the below sources:

A timeline of significant cyber incidents

Read article

Global cyber security market value predictions

Read article

UK pledges £2.6bn to improve its own government cyber practices

Read article

UK pledges £22m to support cyber capacities in vulnerable countries

Read article

WannaCry cyber attacks and the NHS

Read article

£10m cost to Hackney Council post cyber attack

Read article

Cyber security breaches survey 2022

Read article

Global cyber security market statistics

Read article

Promoting economic growth in the UK's cyber security sector

Read article

UK's Critical National Infrastructure report

Read article

UK cyber security council to oversee cyber certified professional scheme

Read article

Cyber security: Technology trends

Read article

Appendix

stotles.

Appendix