CYBER SECURITY

ADAPT TO RAPID DIGITALISATION, NAVIGATE CHANGE AND PREPARE FOR THE FUTURE

CYBER SECURITY IN THE PUBLIC SECTOR

STRATEGY GUIDE

STRATEGY GUIDE

Softcat

WHERE IS THE PUBLIC SECTOR TODAY?

IT'S TIME TO TAKE STOCK

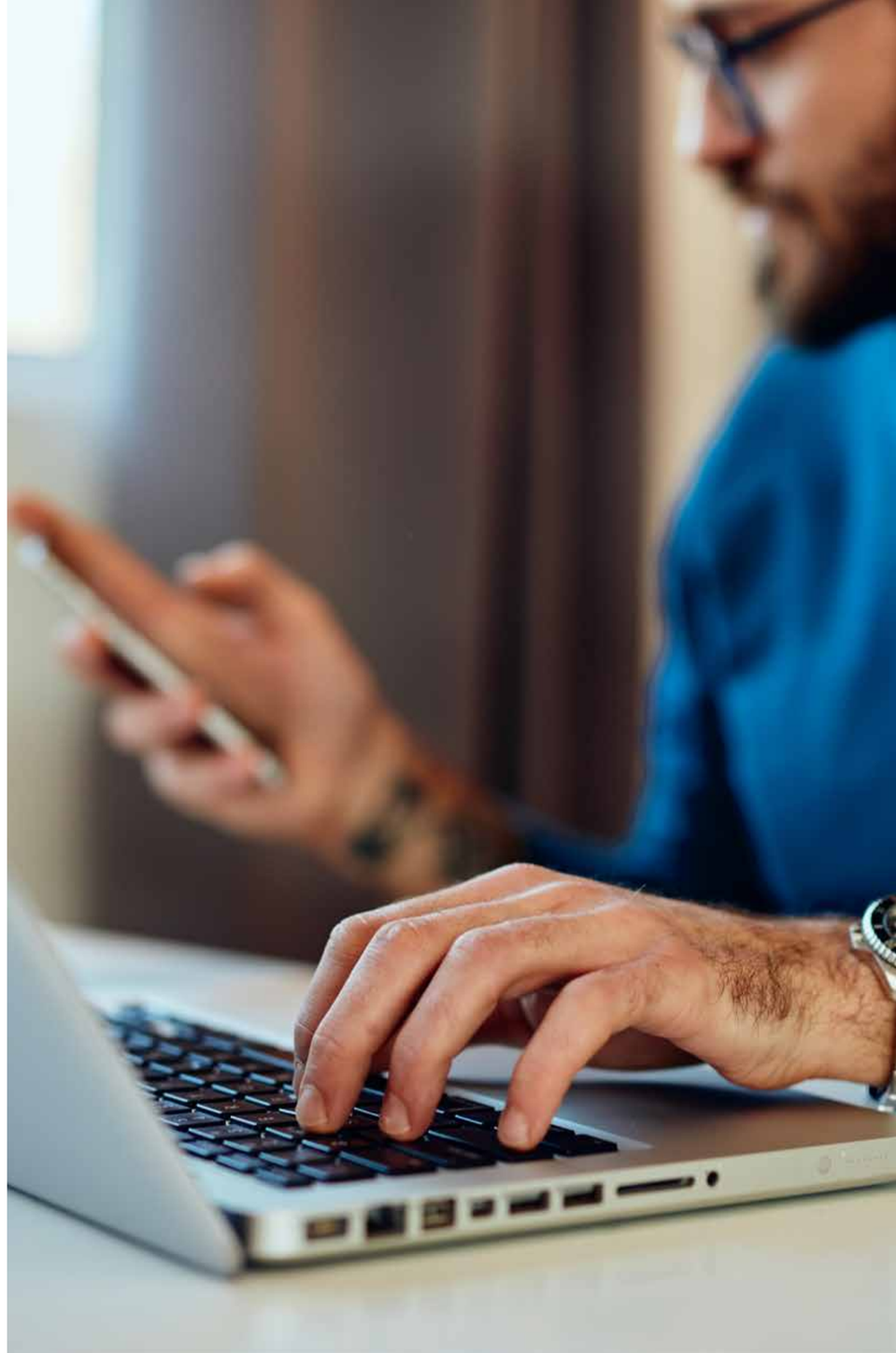
Louise Fellows
Public Sector Director

A lot has happened in a short space of time. The pandemic has accelerated digital transformation across many areas of the public sector and there's been a drive to expand remote services and enable home working.

These changes created more efficient ways of working and facilitated business continuity when it was needed most. They have also encouraged more risk averse organisations to start realising the benefits of digital transformation. However, with such rapid change, certain foundational operations, processes and practices were understandably rushed and, in some cases, missed. You could say that the house was built without some of the footings.

Technologies and solutions recently introduced provided a lifeline for citizens across the UK, but we now need to consider how secure they are. The public sector is truly human-centric, people are a priority and any data is therefore particularly sensitive and valuable. This makes cyber security even more vital to this sector and its people.

At Softcat, we're people focused too. We strive to deliver the best possible experiences to our employees, which means we're also able to provide the best possible experiences to our customers. We put people first, and with this in mind, we feel it is our duty to tell you that now is the right time to take stock and ensure your technology is underpinned by security that provides assurances for every individual at every level.



INTRODUCING OUR STRATEGY GUIDE

This guide has been created to highlight the main concerns and considerations that need to be taken into account within the public sector today – and provide you with practical advice to help overcome the challenges you face.

Our intention is to set you on a path to continued cyber security success. This 'success' will of course be different to every organisation, but our aim is to help you think about the key areas that impact everyone within the sector and tackle them accordingly.

Contributor overview

To help inform this strategy guide, we've held in-depth conversations with three of our experts to talk about the key areas that public sector organisations need to consider when building a cyber security strategy. All three offer a wealth of experience within the security space. And over the coming pages, we've shared their insight, opinion and expertise in order to help you overcome your cyber security challenges.

JAMES SEAMAN
Account Chief Technologist, Softcat

James is a senior member of the Office of the Chief Technologist Officer (OCTO) – Softcat's consultancy and advisory service. More importantly, however, he has a wealth of hands-on public sector experience, implementing several complex projects in the North of England.

ADAM LOUCA
Chief Technologist, Softcat

Adam focuses on developing, engaging and transforming Softcat's strategic customers' cyber security approach. In addition, he also runs Softcat's cyber assessment services business, which helps customers understand and improve their cyber security.

SEAN HUGGETT
GRC Consultant, Softcat

Sean specialises in governance, risk and compliance, including data protection, security risk management and ISO 27001. He has helped Softcat customers prepare for GDPR, NIS, ISO 27001 certification and other industry security standards.

EVERY SILVER LINING HAS A CLOUD

THE STORY OF ACCELERATED CHANGE

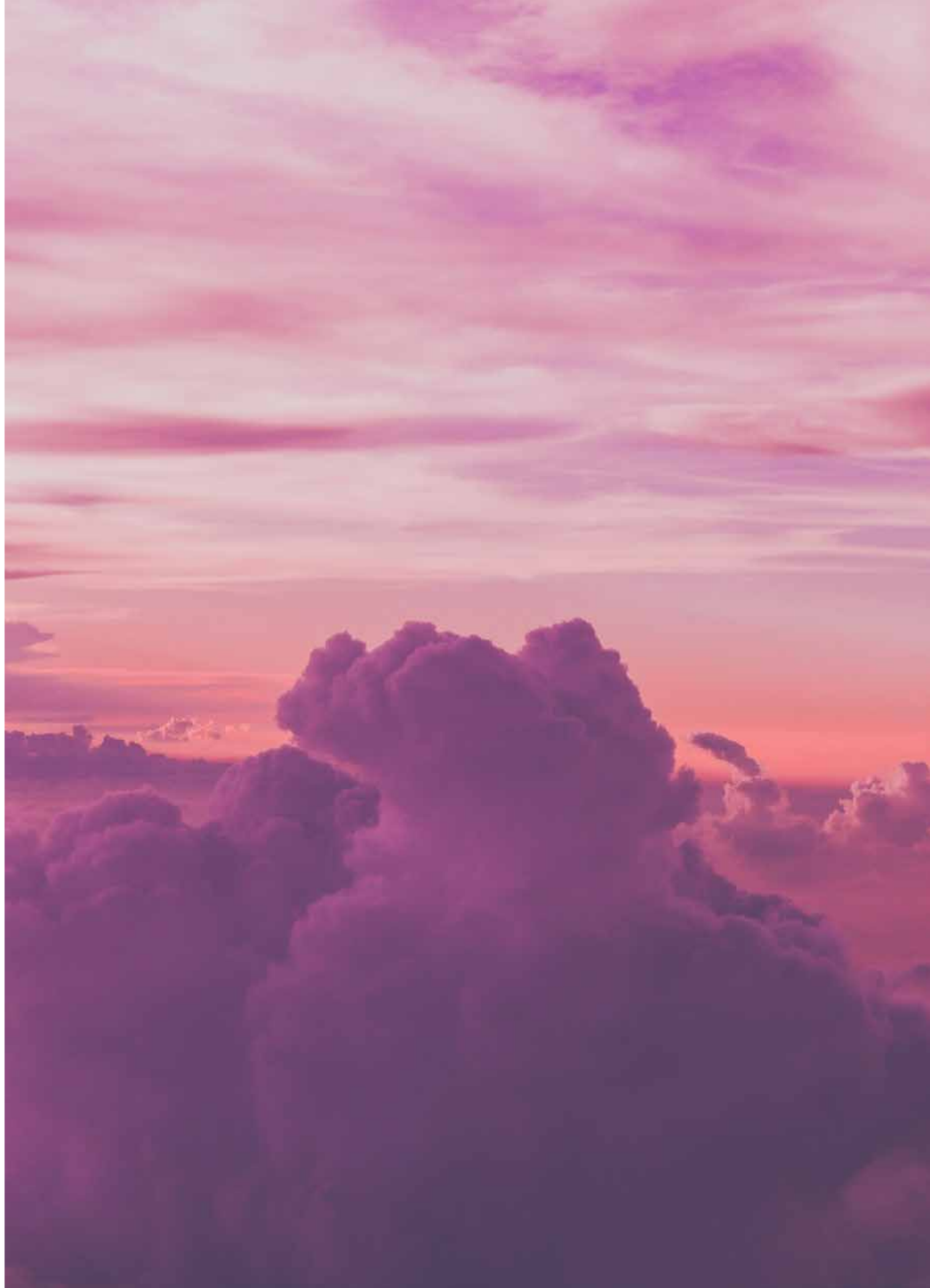
James Seaman
Account Chief Technologist, Softcat

It's easy to frame all recent change as a result of the pandemic. However, changes were afoot in the public sector long before then; the Government's Cloud-First policy was created back in 2012.

What COVID-19 did was accelerate digital transformation agendas across the sector – especially across education, local and central government and blue light services – and it's fair to say that organisations adapted well to the unprecedented period of disruption. Adoption of new technologies was largely successful, and any inertia was mainly due to people and processes as opposed to technology.

In some ways, you could say that every cloud has a silver lining. Through extremely challenging conditions, even the most change averse public sector organisations evolved and embraced modern cloud technologies to provide invaluable services to citizens across the UK.

However, you can also say that every silver lining has a cloud because many public sector organisations adopted 'new' technologies without building the correct foundations of security and governance first. Consequently, at Softcat, much of the work we're now doing is retrospectively shoring up our customers' new ways of working.



EDUCATION

Following the initial impact of the pandemic, education institutions started using collaboration tools, such as Zoom, practically overnight. With few security measures in place, meetings were being Zoombombed, there were versioning issues, and there were problems around a lack of staff knowledge in adopting the new technology.

Many technology providers forgot to consider the impact of change – both financial and operational – to employees who work in very effective ways. So, how do you empower teachers and academics to use new tools correctly? And how do you ensure remote and classroom learning becomes just one task?

I believe the answer is to implement the right change management. It's vital to educate employees and give them the tools or capability to find the most effective way to use a new solution.

HEALTHCARE

How do we deliver unconstrained clinical pathways? This is the key question in healthcare because of how human the sector is. People will always be a crucial element within healthcare, therefore within in a physical environment where the clinician is sat in the same room as the patient, technology should never be a barrier between them. Technology needs to support the physical interaction – not interfere with it.

The same applies to remote healthcare, especially if we want – or need – remote methods to become common practice. Cyber security that's in place needs to be seamless as opposed to being a hurdle to overcome. This approach underpins everything that I try to achieve with my customers – pandemic or no pandemic.

What's more, an astounding number of healthcare institutions don't backup their infrastructure, leaving them open to any type of hack or ransomware. The first line of defence is recovery, so when it comes to cyber security, it's really important to start with backup; do the basics before layering up further security.

LOCAL AUTHORITY

It would be an understatement to say that health and social care has become a key consideration for local authorities – the agenda has hijacked their priorities. With all of the focus going into dealing with the impacts of the pandemic, local authorities have faced the biggest challenges in terms of getting back to their core line of operations.

However, with the government concentrating mainly on blue light, healthcare and education services, local authorities have been somewhat forgotten about. The challenges are bigger, but the budgets are smaller. So, to consider facing cyber risks on top of everything else can feel overwhelming.

Retrospective accountancy within local authorities means departmental budgets must be spent each year. Cost avoidance is a challenge; cost saving is the goal. And investing heavily in cyber security that reaps financial rewards over several years isn't always the answer – they have to offer savings, now.

OPTIMISING INVESTMENTS

No matter which area of the public sector you're in, the ultimate goal should be to ensure IT makes everything more efficient without disrupting the human aspect. You also need to consider how to shrink your estate and make it simpler to protect the public pound. New investments should be optimised; existing 'distressed investments' made over the past few months should be turned into tactical and strategic outcomes.

We understand the pressure on CIOs today to keep everything running while educating others and meeting stringent budget requirements. So, focus on what you do best and if it isn't cyber security or asset management, then look for support. Be a savvy investor. If you know what 'good' looks like, outsource a specialist to run it for you.

At Softcat, optimising investments is what we take responsibility for. We consolidate. We optimise. We ensure value is derived or added. And we have the customers, experience and expertise to ensure you make the right decisions. Rather than adding to the complexity, our duty of care is to make sure you decommission the things you don't need before implementing anything new. We offer true advisory, which, to our knowledge, is unique in the reseller market.

PUTTING PEOPLE FIRST IN THE PUBLIC SECTOR

DRIVING IMPROVED BUSINESS OUTCOMES

Adam Louca
Chief Technologist, Softcat

The public sector is, by definition, a people-based business. It is therefore crucial to ensure that the balance of technical input and human output is right; technology has to play a supporting role, empowering people to achieve better outcomes.

However, in recent times, many public sector organisations have understandably invested heavily in digital technology – enabled by additional government funding in an attempt to overcome the impacts of COVID-19. This injection of funding has given organisations access to complicated and advanced public sector tools, especially in the cyber security arena. Unfortunately though, many are now struggling to realise the true value of their distressed investments, and that's where I'm currently providing support to customers.

VALUE REALISATION IS VITAL

Traditionally underfunded public sector organisations have suddenly been able to invest in the best technology they can buy – but they're unable to work out how to operationalise the technology and implement it effectively. There's little wonder. With the budget of a large enterprise, but the internal resourcing of an SME, it's very hard to bridge the gap and realise any value.

The work I'm doing at the moment with customers is to break up the bigger problems into modular components that are small enough to enable meaningful progress. This means I can help to deliver a capability package that moves things forward. Along with the critical cultural change that's required to facilitate change, and the support for internal IT teams, my aim is to strip things back to make them more manageable.

SPENDING IN THE RIGHT PLACES

For public sector organisations fortunate enough to have received additional funding, the challenge quickly becomes a lack of time and resources to deliver new investments. For the organisations without funding, the challenge is to do better with less. And for all organisations, the hardest thing is to spend less on technology and invest more in internal teams.

In my opinion, countless public sector organisations would benefit from building up their internal capabilities – investing in skills and education in order to make the most of the right technology solution. Training and resources should be an area of focus; just imagine the progress you could make by spending more of your budget on upskilling employees as opposed to just upgrading IT equipment?

Generally, however, my best advice is to prioritise. You can't do everything all at once, so which areas of the business matter most to you? It's worth considering the investments that make sense at any time: get your user identities in order; decide who has access to what; define who should work remotely and how. Take a pragmatic approach and focus on the areas that will always hold the most value – no matter what happens in the world around you.

NAVIGATING A COMPLEX LANDSCAPE

By their very nature, public sector organisations have an even more complex supply chain than many enterprises given the amount and type of data they have – internally, externally and across the third sector. They also often lack standardised processes due to their lack of resources. Therefore, it's important to get the right data to the right people by providing appropriate access.

A good example of this can be seen within the Police force. After responding to a domestic violence case, the Police may want to share data with a women's refuge, but they might not be able to due to restrictions on sharing between third parties. In this instance, someone needs to be in place to make a common-sense decision and consider a risk-based approach where necessary. They need mechanisms to by-pass bureaucracies.

This is why, at Softcat, we provide an external assurance as a corporate organisation – taking responsibility for some of the risk associated with navigating a complex landscape. The public sector is essentially a patchwork of standards and regulations, but its organisations need to share information between them in order to put people first. Therefore, we find ways to help public sector organisations make things work, move forward and make better decisions.

BEING PROACTIVE AND POSITIVE

Unlike within an enterprise setting, the risk of doing nothing is huge within the public sector. It could be the difference between someone getting fed or not; or missing out on the support they need. So, it's important to be proactive towards digital change and positive about the impact it can have on your organisation.

The key is to co-ordinate a multi-agency approach – and to not let technology get in the way of collaboration. It's all about knowing when to act in a person's best interests to intervene and sidestep any restrictions.

OUR APPROACH

At Softcat, we have three key questions that we aim to help customers answer: How do you get the most out of the technology? How do you create leaders of tomorrow? And how do you ensure that security doesn't become a barrier?

We can provide informed support in this area because we are highly accredited to work within the public sector. We are one of only a handful of suppliers to have passed the requirements of the SPS Cyber Security Framework; we work across 50+ frameworks within the public sector; and our credibility is based on our wealth of experience.

We offer security programme leadership; strategic guidance; commercial support; and governance risk and compliance consultancy – helping customers to build out their own unique processes.

What's more, with an award-winning internal culture and a commitment to developing people, we can happily share our experience with public sector organisations to help them grow. In other words, when it comes to the public sector, we're good at putting the public first.

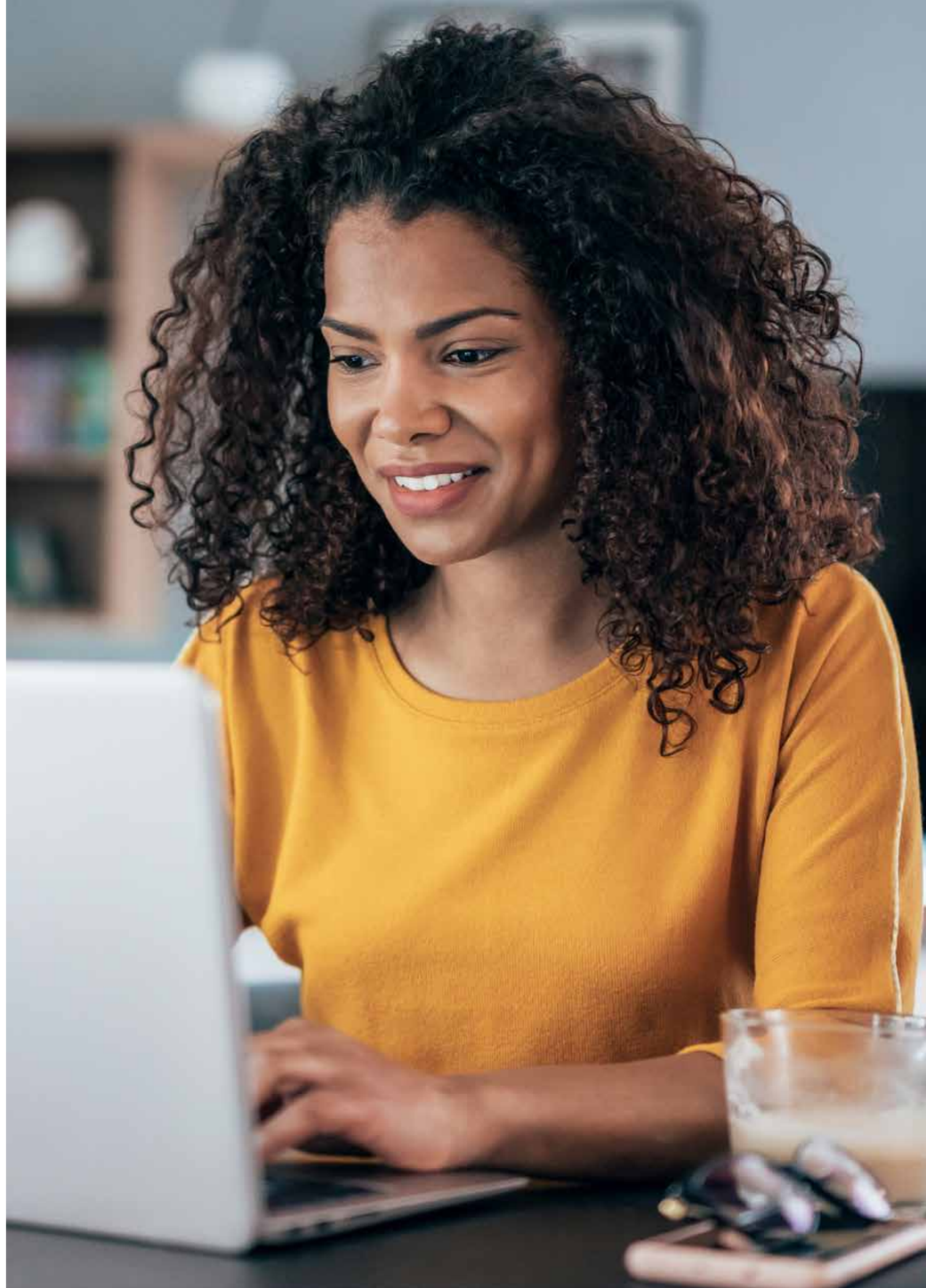
SAME GAME, DIFFERENT RULES

DEALING WITH THE CHALLENGES OF A UNIQUE SECTOR

SEAN HUGGETT
GRC Consultant, Softcat

Whether it's political change, economic shift or environmental issues, major global events are something we all have to face and overcome. However, it's fair to say that in the public sector, a different set of rules apply to how situations are dealt with.

Within a people-orientated environment, public sector organisations have to deal with a diverse variety of challenges – and make the most of a different range of opportunities than many other sectors. Despite common preconceptions, it's an exciting and surprising sector that impacts all of our lives.



THE HUMAN SECTOR

While the world adapts to increasingly remote ways of working, there are certain areas of the public sector that will always rely on the human aspect – much more than areas of the private sector. In healthcare, for example, a doctor will always need to see a patient face-to-face. And while technology can support the interaction, making the process more efficient and providing the right information at the right time, the human aspect will always be critical.

There are differences around cyber security, too. Things like GDPR, legislation and wellbeing laws are taken incredibly seriously in the public sector due to the higher risks associated with people and data. Councils, for instance, must provide access to a very different type of information than organisations within the private sector; the support sought by individuals with highly sensitive personal circumstances is clearly very different to the support sought by those who have been overcharged for a product.

However, this means there's a huge opportunity for public sector organisations to forge ahead and set cyber security standards that will benefit people everywhere. The surrounding laws and regulations are more stringent than many of those in the private sector, but that means we have the chance to make cyber security even better.

WHERE DO WE GO FROM HERE?

The big question at the moment is undoubtedly around COVID-19 and where the public sector will go next. Will organisations be empowered to invest in technology, or will they have to cut corners? Those in higher education, for example, were doing really interesting things with technology before the pandemic, so how will they adapt to current conditions and continue?

In healthcare, GP surgeries can now work together to form Primary Care Networks with the objective of achieving economies of scale, pooling resources and providing targeted, proactive healthcare and support for their patients. In education, schools are joining forces to share best practice. Will we be overwhelmed with the siloed containers of technology that therefore need to communicate with each other, or find ways to optimise shrinking budgets and reduce risk?

Even within the organisations who have been granted additional funding, the nature of public sector budgeting means that investments made aren't always in the best interests of sustainable transformation. It's easier to place an asset on the balance sheet that will provide an immediate tangible benefit, as opposed to trying to justify an intangible consultancy fee that promises to provide efficiencies and savings down the line. So, how can we attain buy-in for security leadership services or transformation support?

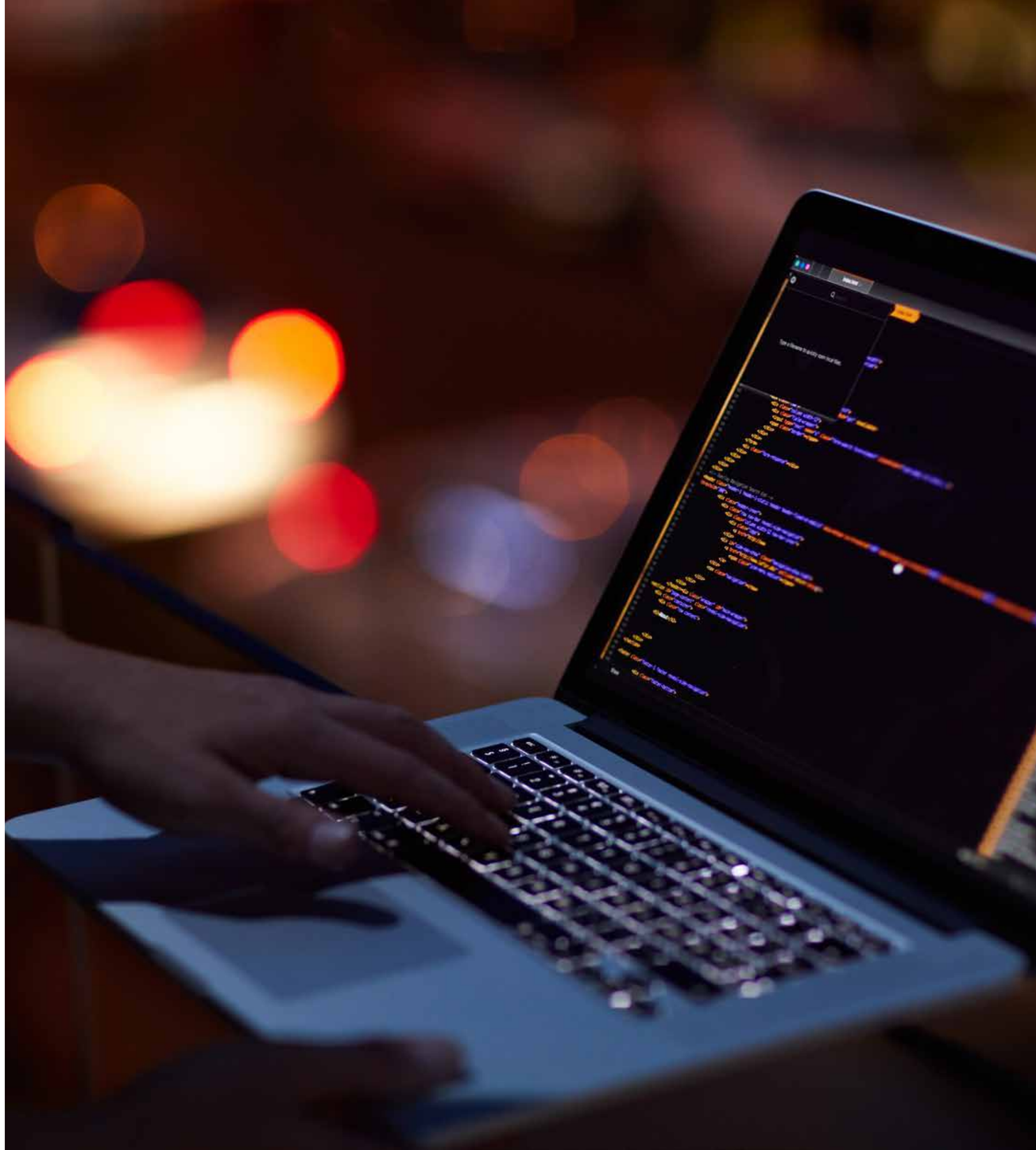
TAKE ONE STEP AT A TIME

With so much change in the world, it's important to realise that you can't do everything at once; you can't secure everything within the public sector at the same time. So, you need to prioritise. Carry out threat assessments to find out what the most immediate threats are. Identify your vulnerabilities and prioritise around them. Ensure the ongoing proactive management of risk, rather than the reactive management of incidents.

At Softcat, we help public sector organisations to build a strategic framework; identifying and prioritising their security plan. We ensure they break down bigger issues and work through smaller problems – making progress quicker and improving their security posture.

From our very first customer engagement, we take a view from the outside in – assessing the security landscape without the burden of having to firefight issues as many public sector organisations currently have to. We call upon our broad network of experts and specialists where necessary to help develop a plan and implement it. And we show them what 'good' looks like to keep them on track in times of change.

Our combination of in-depth experience and knowledge of the public sector, with our inherently human approach, means that we have well-established relationships within the public sector – and we offer the assurance of understanding all the relevant governance, legislation and audits associated with public sector practices.



Attend to the priorities of today; prepare for the tests of tomorrow

Start your journey to improved cyber security

When it comes to adapting to rapid digitalisation, navigating change and preparing for an unpredictable future, the public sector has its own set of unique challenges to overcome. So, here are the key pieces of advice to take away from the conversations we've had with three of our public sector experts:

- **Put people first** and consider prioritising cyber hygiene, vulnerability management and end point management. Incorporate flexibility because your priorities may change depending on the needs of the government or wider landscape.
- **Ensure that technology supports physical interaction** and doesn't interfere with it. The human aspect within the public sector is all-important, so the ultimate goal has to be to make sure IT becomes invisible while making everything more efficient.
- **Consider how to simplify your technology estate** to help protect the public pound. Both new and existing investments should be optimised and turned into tactical and strategic outcomes.
- **Focus on what you do best** and if it isn't cyber security or asset management, then look for support. Recognise what 'good' looks like and outsource a specialist to run it for you.
- **Break up the bigger problems** into modular components that are small enough to enable meaningful progress. Strip things back to make them more manageable. Build a strategic framework that enables you to create a security plan.
- **Prioritise the areas of that matter most to you** and remember you can't do everything all at once. It's worth considering the investments that make sense at any time – no matter what's going on in the world around you.
- **Create your own ecosystem** of trusted partners and employ a digital-first business model. Form digitally integrated relationships with the people in your supply chain to enable short-term business continuity and realise long-term business benefits.
- **Build up your internal capabilities** and invest in skills and education to make the most of your technology solutions. Try to spend more of your budget on upskilling employees as opposed to just upgrading IT equipment.
- **Implement the right change management** because transformation can only occur when everyone's on-board. It's vital to educate employees and give them the tools or capability to find the most effective way to use a new solution.

If you're interested in the many ways in which Softcat can support your public sector organisation, don't hesitate to get in touch. We'd love to learn about your current setup, and advise how best to improve upon it.

Email: **CyberServices@Softcat.com**
Or speak to your Account Manager today.

Softcat