trowers & hamlins

CYBERSECURITY

The cyber landscape of the Public Sector

Contents

> *"Public sector spending is yet to provide sufficient focus on cyber security and the risks of not doing so are becoming increasingly more clear. Not only must organisations and authorities invest in their own defences, failing to include cyber resilience as part of their procurement requirements may result in suppliers being the gateway for cybercriminals. Given a public organisations role in society, and the nature of the information held, failure to invest in the necessary infrastructure could have catastrophic effects to the local area and an already unstable national economy. Local authorities can take some simple steps to improve resilience with minimal spend, but ultimately any spend will be less than that caused by any cyber-related incident and local leaders should take note."*

Prashant Pillai, Associate Dean for Research and Knowledge Exchange, University of Wolverhampton.

Introduction

Digitisation of public services over recent decades has moved at such a pace that cybersecurity has often failed to maintain the same momentum.

Such juxtaposition has resulted in ill-prepared and misinformed organisations – including Central and Local Government, housing associations and NHS trusts – being unable to, or mistakenly deciding not to, maintain the necessary protections to operate cyber-secure operations. Furthermore, it is clear that this issue is prevalent in the procurement of services and supply chains, and no matter how much individual public bodies prioritise cybersecurity, their resilience is only as good as their networks.

While we take a look at some of these issues in this white paper, there is unfortunately no one size fits all solution. What we are proposing is that whilst the Government appears to be putting a huge focus on cybersecurity – and rightly so – it should take into consideration the difficulties of different sized public bodies, their procurement activities, and acknowledge the quantity of education which is required to reduce cybercrime. A survey undertaken by the DCMS highlighted that people and culture were more of a weak link than the technology, although there was an increased vulnerability at all levels. At present, the message is not getting across.

Central and Local Government and the wider public sector will be required to take bold steps in order to ensure there is a concerted effort for society to change its intrinsic behaviours. The reality being everyone will need to play a role should any meaningful impact be made, led by the public sector's example.

We have discussed the issues addressed in this paper with industry leaders, including local and central government, in addition to reviewing some real-life examples to provide detailed first-hand accounts of the current climate.

We are especially grateful to all contributors to this paper during its formulation and are hopeful that progress can be made to educate all organisations of the benefits of cybersecurity.

Amardeep Gill
Partner
agill@trowers.com
+44 (0)121 214 8838

Background

An increase in cybersecurity threats has been widely and consistently reported as public bodies continue to digitise, even more so since the beginning of the COVID-19 pandemic. Experts predicted that cybercrime would thrive on new vulnerabilities emphasised by remote working conditions, and this has sadly become a reality.

The annual Cybersecurity Breaches Survey published by the government in the Spring found that 39 per cent of UK businesses and public organisations had experienced a cyber-attack in the previous 12 months. Around one in five of those were the victim of a sophisticated attack such as a denial of service, malware or ransomware attack, while the most common threat came from phishing attempts. Of those reporting incidents, 31 per cent said they were being attacked at least once a week. Cybersecurity is an issue which is clearly prevalent.

What is currently being done to combat these worrying statistics?

The Government is doing a great deal to address cybersecurity concerns and has published its National Cyber Strategy 2022. This strategy sets out 5 pillars of focus, namely:

- UK Cyber Ecosystem – this pillar highlights that for the strategy to succeed, the UK needs the right people, with the right knowledge to work together and build a compliance culture and support the UK cyber sector to grow;
- Cyber Resilience – this pillar focuses on understanding the risk, securing systems and being able to respond and recover;
- Technology Advantage – this pillar acknowledges that technology is required to be better designed and deployed to provide heightened security and economic advantage;
- Global Leadership – this pillar recognises the importance of a collective stance and the cooperation of all nations to provide better protections; and
- Countering Threats – this pillar identifies that deterrents, detection and proactive steps should be explored in addition to robust defences.

Whilst this strategy is in its early stages, it gives a strong indication of the Government's future aims and objectives and appears to hit on the key themes we would expect. Additionally, the UK has already taken steps to encourage public bodies and businesses to have a commercial interest in bolstering their defences, which appears an obvious hurdle, through the implementation of the Cyber Essentials certification.

Cyber Essentials is a Government backed certification scheme that helps organisations, regardless of size, improve their cyber resilience through the implementation of five key technical controls. It helps them better understand and proactively manage the increased risks attached to digital growth and protects them against the vast majority of common, internet-based cyber attacks.

There are two levels of certification under the scheme, both of which implement the same technical standards, with different degrees of assurance – Cyber Essentials and Cyber Essentials Plus. Cyber Essentials is completed through a verified self-assessment that is certified by an approved certification body. Cyber Essentials Plus includes a technical audit of the controls by a licensed assessor.

From a more regulatory standpoint, the UK's regulator for information rights (the Information Commissioner's Office (ICO)) has wide ranging powers to deter non-compliance with the UK General Data Protection Regulation (UK GDPR) and/or the Data Protection Act 2018 (DPA). That said, it takes a measured view when breaches are reported to it, acknowledging the fact that complete compliance is difficult, and vulnerabilities cannot always be helped. This provides a balanced environment for smaller public institutions to proportionally assess their position, whilst larger organisations may not have such flexibility.

As the National Cyber Strategy 2022 indicates, there is considerable amount of work being done to grow the cyber sector and address its risks but there is always more that can be done.

Is the UK's current cybersecurity strategy working?

Whilst the Government has put cybersecurity firmly on its agenda, the reality is that the message is not filtering down to all tiers of the public sector and furthermore their supply chains.

Historically, there has been a stigma associated with cybersecurity, and in particular compliance with data protection legislation. It is seen as high cost and low reward given the consequences are hypothetical until they are not.

Despite good progress made since 2016, there is still more that the Government and other public bodies can do to encourage good cybersecurity practices and improve cyber resilience in organisations of all sizes.

> *"Effective management of supply chain cybersecurity is key to a resilient UK economy (...) As supply chains become interconnected, vulnerabilities in suppliers' products and services correspondingly become more attractive targets for attackers who want to gain access to the organisations (...) Recent high-profile cyber incidents where attackers have used Managed Service Providers as a means to attack companies are a stark reminder that cyber threat actors are more than capable of exploiting vulnerabilities in supply chain security, and seemingly small players in an organisation's supply chain can introduce disproportionately high levels of cyber risk."*

Call for views on Cybersecurity in supply chains and managed service providers, 15 November 2021, DCMS Policy Paper

Case study one: Redcar & Cleveland Borough Council

In February 2020 a cyber-attack occurred causing disruption to almost all Council functions. The cyber-attack left the Council's computer systems crippled and unusable for almost two weeks with appointment bookings, planning documents, social care advice and council housing complaints systems offline. It took the Council around eight weeks to restore most services, and a further five weeks to restore the "low-priority" data that it held.

A single email with an attachment was the source of the attack. Council IT staff recognised what was going on, powered down the servers and called in the National Cyber Security Centre (NCSC). A subsequent external investigation by the council's auditor concluded that the Council had "proper arrangements and controls in place to reduce the likelihood of a cyber security breach" given the resources available.

Ransomware is a specific type of malware that encrypts computer files, essentially locking the owner out of their systems. Once this has happened, the ransomware will display a message demanding that the victim make a payment to regain access to their files.

The cybercriminals said they would keep the data encrypted until the Council paid them £1m. The Council refused given that there was no guarantee that the data would be released and due to requests from central government that it refuse to pay.

The Council costed the damage caused by the cybercriminals at £8.7m following a financial impact assessment completed in June 2021. Redcar and Cleveland is, as far as we are aware, the only local authority to have received any money from central government (that was not a loan) to deal with the aftermath of a cyber attack. The sum of £3.68m offered by central government to compensate for the cyber attack still left the Council at a significant loss.

More than 135,000 residents have been affected by the incident, which is believed to have been caused by ransomware.

This attack highlights the financial and functional implications of a cyber attack. Financial support offered from central government does not cover the losses of local authorities incurred as result of cyber attacks irrespective of whether a ransom requested by cybercriminals is paid by a local authority or not.

“Recent successful cyber-attacks have shone a brighter light on organisations understanding their supply chain risk. It underscores the importance of organisations understanding their network, data flows and extent of shadow IT. It’s vital that organisations understand the ‘extended enterprise’ and perform risk assessments as far as is possible through their supply chains.

Only when an organisation fully understands its supply chain and where protections are required can it assess if those protections are adequate.

The risk has been increased over the past two years. The response to Covid-19 increased adoption of software-as-a-service solutions, often launched at a pace and without the same level of rigour from information governance teams. It is important that organisations have due diligence processes at procurement stage and on an ongoing basis to help minimise supply chain risk.”

Praveen Gupta, National Head of Tax/ Tax Partner, Azets

Legislative position

Criminal

Whatever form they may take, cyber-attacks are examples of cybercrime: a term used to describe crimes, commonly frauds, attempted or committed using a computer network and the internet.

The key legislation that governs cybercrime is the Computer Misuse Act 1990 (as substantially amended by the Police and Justice Act 2006 and the Serious Crime Act 2015) (CMA 1990).

There are three specific offences created by the CMA 1990:

- Causing a computer to perform any function with intent to secure access to any program or data held in any computer the person is not authorised to access (section 1);
- Committing a section 1 offence with the intention of committing further offences (section 2); and
- Doing any unauthorised act in relation to a computer that a person knows to be unauthorised with intent or being reckless as to whether his act will:
    - Impair the operation of any computer;
    - Prevent or hinder access to any program or data held in any computer;
    - Impair the operation of any program or the reliability of any data; or
    - Enable any of the things above to be done.

Collectively referred to as the **CMA Offences**.

The unfortunate purpose of some cyber-attacks is to permanently deprive the victim, whether an organisation or individual, of data, for example, and to do so by dishonest means. In light of this, given the nature of the CMA Offences, it is also very common for offences under the Fraud Act 2006 or Theft Act 1968 to be committed.

> *“New legislation has been proposed in both criminal and civil cases which means the regulatory landscape is likely to change in the near future so now is the point of intervention. It is the responsibility of all businesses with know-how to let their views and issues be known to ensure that these new regimes factor in supply chain and any other ubiquitous issues.*
>
> *There is a real opportunity to make waves in how the UK approaches its cybersecurity defences but unfortunately only time will tell as to whether any new policy is successful.”*
>
> Amardeep Gill, Partner, Towers & Hamlins

Civil

In addition to criminal consequences, the UK GDPR and DPA also seek to encourage strong data protection practices, with the ICO providing a wealth of guidance for such compliance.

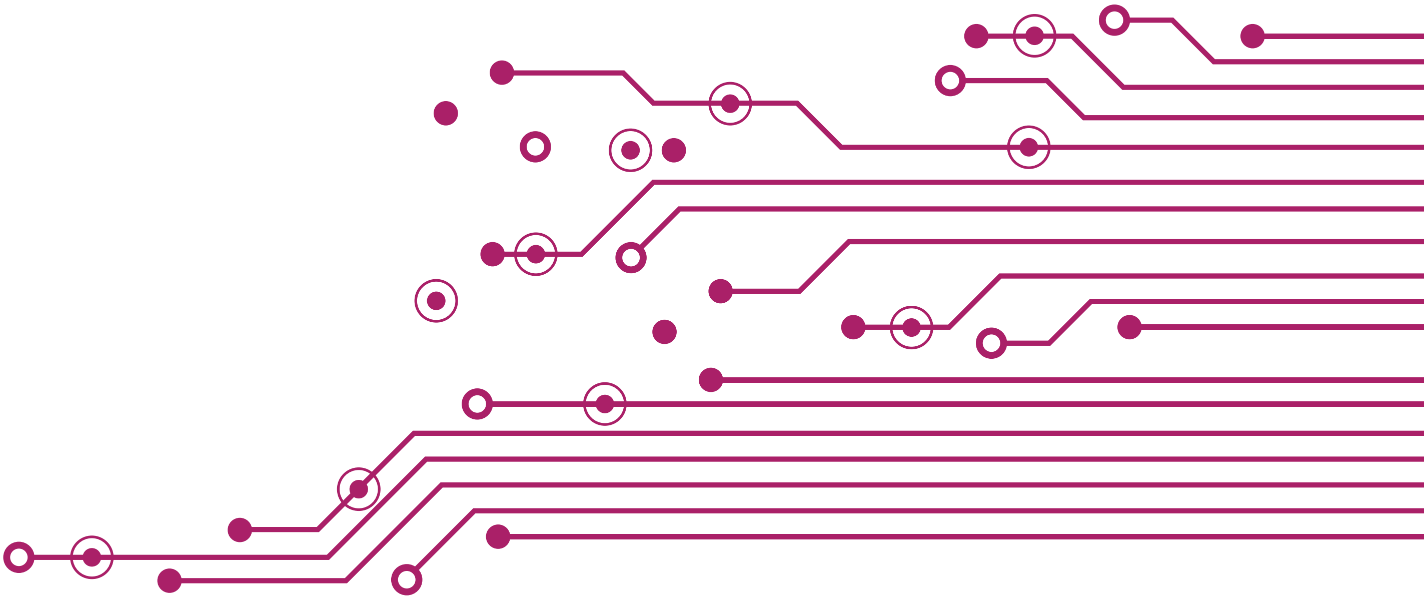
The ICO has wide ranging powers under UK GDPR to fine UK businesses and public bodies (up to £8,700,000 or 2% of the undertaking's total annual worldwide turnover in the proceeding financial year, or up to £17,500,000 or 4% of the Target's total annual turnover, whichever is higher depending on which Data Protection Law is breached). These significant penalties are intended to encourage a compliance culture, as well as setting an international preferred standard.

UK GDPR and the European Union (EU) counterpart (whilst they are currently aligned) are seen as the 'gold standard' of data protection legislation. However, there are many that consider their scope to be too broad, and as a consequence, their inflexibility prohibitive to national and international trade.

Additionally, the wide-ranging rights granted to data subjects, whilst protecting their privacy, may be considered to put public institutions on the back foot, with fruitless and vexatious claims often being cheaper to pay-off rather than defend.

Following Brexit, the UK has indicated that it wishes to address these concerns, and during the Queen's Speech earlier this year, a data reform bill was published. This document currently lacks substance, and many commentators suggest that material deviation from the EU regime is unlikely, as the consequences to industry and the economy are not worth the benefits achieved from deregulation. The overarching intention of the Bill is to simplify data protection legislation, reducing the burden on businesses by creating a more flexible, outcomes-focused approach rather than "box-ticking exercises".

It is unclear how this will affect the public sector and its suppliers. The big question is whether these institutions and the smaller businesses that form a key part of public sector supply chains will be able to cope with having to undertake an outcomes based approach rather than being able to put in place or sign up to standard processing terms. Any change to policy will require an investment by all organisations to review their existing practices and educate themselves and their supply chains on any new requirements.



Case study two: Newham Council

In January 2017, a sensitive police database detailing 203 alleged gang members and the weapons they are believed to carry was leaked by the Council and subsequently fell into gang hands.

An employee of the Council sent an email to 44 people that contained both redacted and unredacted versions of the gangs' matrix - a police intelligence database. The recipients included members of the Council's youth offending team and external organisations.

The unredacted database had included alleged gang affiliation, dates of birth, home addresses, and information on whether they were a prolific firearms offender or knife carrier.

The Information Commissioner's Office (ICO) found that between May and September 2017, rival gang members had obtained photographs of this information from the unredacted version of the gangs matrix via social media app Snapchat. Some victims of serious gang violence that year were people who featured on the matrix.

These included a 14-year-old who was shot dead in September 2017. News of the leak emerged as part of a serious case review into his death. The ICO said that it was not possible to say whether there was a causal connection between the violence and the data breach. The ICO did criticise the Council's "unnecessary, unfair and excessive" decision to share an unredacted version of the data in an unsecure email to 44 recipients.

Newham Council has been fined £145,000 by the ICO in relation to the data breach.

It is clear from this case, as well as the Advanced case below (Case study four), that the consequences of cyber security breaches are not only inconvenience and financial loss. Data in the wrong hands, or kept out of the right hands (as the case may be), can cause a risk to the safety of the public.

Public sector organisations should invest time in the creation and upholding of policies and procedures to ensure the secure sharing of data. The implementation of such policies and procedures by staff and suppliers should be a priority of organisations. Training, restrictions on access and contractual obligations should be considered.

Direction of travel

This paper highlights that, whilst the Government has put cybersecurity firmly on its agenda, the reality is that the message is not filtering down to all tiers of the public sector and furthermore their supply chains.

Organisations need to be accountable for their own cybersecurity and the public sector has a particular role in educating SMEs in their supply chains. 60% of SMEs who were victims of cyber attacks did not recover and closed within 6 months (as warned by WMCA). One way in which they can be encouraged to improve is to factor cybersecurity into their environmental, social and corporate governance ("ESG") strategy. ESG is a particularly prevalent topic at the moment and a lot of organisations are making strides when it comes to ESG in general. Rather than relying on cyber insurance to manage their cybersecurity risks, organisations need to start managing their cybersecurity risks as part of their ESG strategy, particularly the "G". Cyber-attacks present a huge risk to the reputation of public bodies and the value of companies and, from a wider perspective, the fabric of society given the impact that a cyber-attack can have on an organisation's clients, partners and suppliers.

Institutions that fail to implement good governance on cybersecurity, using appropriate tools and metrics for their organisation, will be less resilient and less able to deliver the essential services they provide. This failure, in turn, will have an impact on the individuals they serve, and ultimately, on the stability of industries, communities and governments.

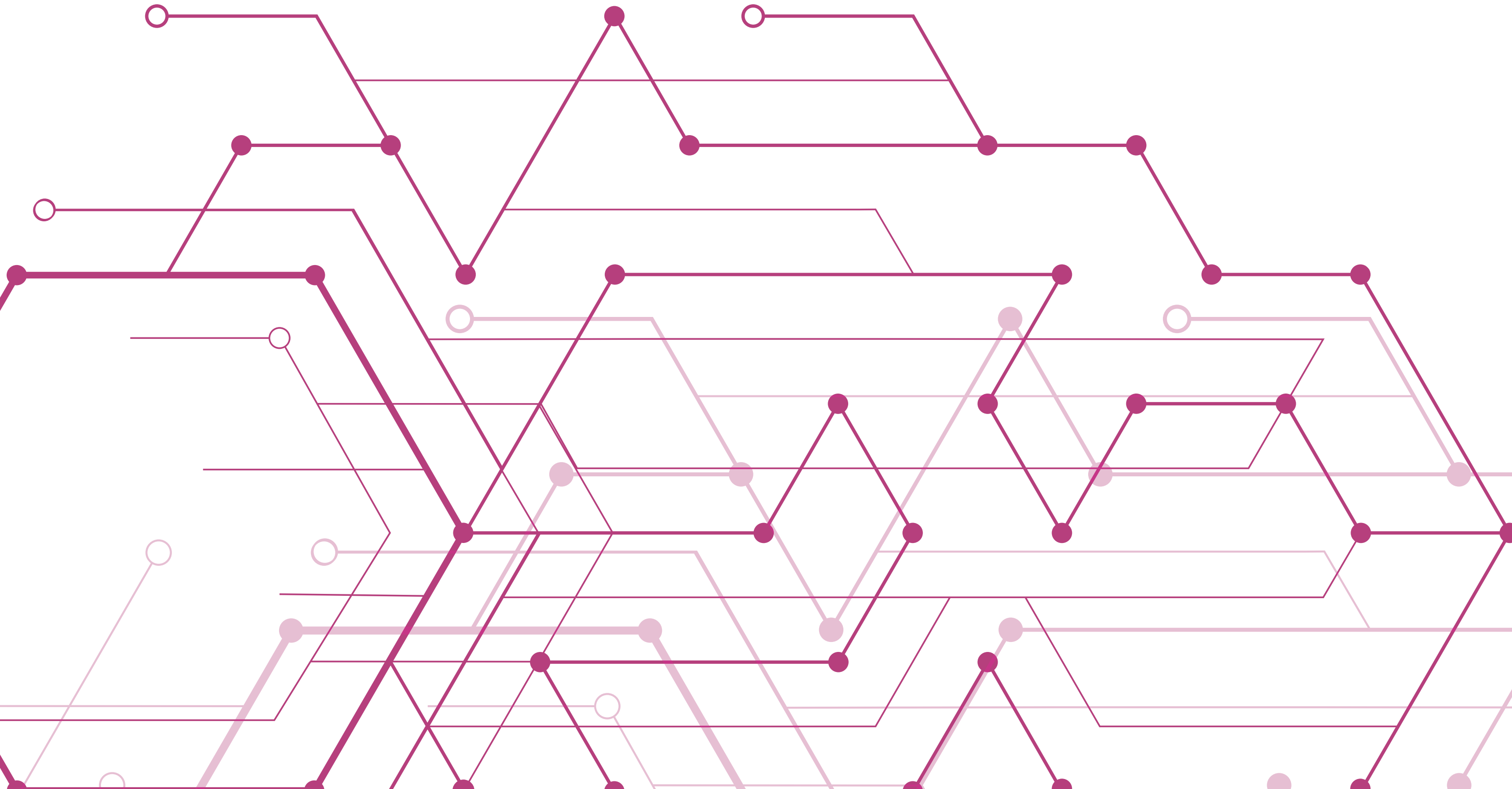
Cybersecurity is not just an issue for IT departments. Public bodies and their elected representatives need to identify their organisation's key assets (the ones that they cannot operate without) and how to protect them so that, in the event of a breach, operational efficacy is not lost (or the loss is, at least, kept to a minimum). Whilst not expected to be cyber experts, equipping themselves with a panel of third party cyber experts will allow public bodies to better assess their organisation's cyber risk.

We encourage all public bodies, therefore, to "get on board" and actively engage in their organisation's cybersecurity risks, an to promote the same engagement throughout their supply chains.. This will become an increasingly important aspect of how citizens, stakeholders and customers see your operations.

Investigations into data breaches are being handled in a more sophisticated manner than they were, which organisations also need to bear in mind. The ICO have specialists on board that deal with the cyber investigation after an organisation has reported a data breach. If the ICO considers that the reporting organisation did not have sufficient measures in place to prevent a data breach, a hefty fine is likely to follow. British Airways, for example, was fined £20 million by the ICO for failing to protect the personal and financial details of more than 400,000 of its customers. BA's failure to have adequate security measures in place to protect customers' personal data led to BA being subject to a cyber-attack in 2018, which was not detected for over two months. BA faced civil claims after the cyber-attack. The claimants alleged that they suffered harm in the form of distress and/or pecuniary loss and/or loss of control of data. Despite the fine imposed on it by the ICO, BA denied the civil claims and claims were settled in July 2021.

“The research is stark and should serve as an immediate warning. Small and medium-sized enterprises are the new big target for cyber-attacks. Some 93% of organisations have suffered a direct breach due to weaknesses in their supply chains over the past year, with experts predicting an attack every 11 seconds. 60% of SMEs who were victims of cyber-attacks did not recover and closed within 6 months. It is absolutely imperative that businesses large and small, and public sector authorities, not only protect their own organisations from cyber-attacks, but that they take steps to ensure their supply chains are protected, too.”

Allan Andrews, Senior Policy Advisor, WMCA



A key risk that public sector organisations need to get a much better handle on is that posed by their supply chain. Suppliers have access to confidential and sensitive data held by supply chain owners in order to facilitate the performance of their contractual obligations. Unless monitored, an organisation's supply chain can act as an open door for hackers to infiltrate its systems.

What this paper has shown is how important it is for public bodies to improve their supply chain's cybersecurity compliance and keep this under regular review. With public bodies tying to bring ever more local SMEs into their supply chain, the risks will increase as discussed in this paper. Supply chain cyber management should be viewed as a shared responsibility between the organisation and their suppliers. Some ways in which organisations can do this include:

- Carry out risk assessments across your supply chain – how sensitive are your supply contracts? What value of information/assets do your suppliers hold or have access to? What are their current security arrangements?
- Set minimum security standards for suppliers depending on their risk profile and include this as pass/fail criteria in your procurement processes.
- Audit and monitor your suppliers – put in place checks and measures to stress test the cyber protection gained from your suppliers. For example, do you have a right to audit provision in your supplier contracts? Do your suppliers regularly run penetration tests and external audits? Have you communicated key performance indicators to your suppliers and are they compiling with these?

The above measures show that putting in place sufficient measures to protect your supply chain from a cyber-attack does not have to be costly, complex or confusing. It is a matter of taking the time to better understand the risks in your supply chain and taking appropriate steps to manage those risks.

“Many people often see private sector organisations discussing cyber security issues, but public sector organisations are arguably targeted institutions too as they hold a lot of critical data. As the number of cyber-attacks is on the increase, and the change to working habits over the last two years has amplified our reliance on technology, public sector leaders need to adapt their strategies to new risk challenges. Often seen as a discretionary cyber spend, especially in a difficult economic climate, with public sector spending restricted, the reality is that costs arising from any cybersecurity attack could greatly exceed any proactive cyber security investment. Society needs to keep pace with threat actor sophistication and criminal use of advanced technologies, to be able to enhance cyber defences appropriately in the fight against cybercrime – the cooperation between the public and private sectors is fundamental to any success. Local authorities, the NHS and other public organisations should reach out and seek more cyber expertise and cyber solutions to help defend themselves.”

Karen Morrall, CEO, Lockdown Cyber Security

Case study three: Multi-Authority shared services

In 2016, three Local Authorities, close in location, created a shared service (the Service) between them to provide a more efficient way of delivering services ranging from ICT to Legal and Building Controls. The Local Authorities were driven to create the Service by financial need but also by a strategic desire to deliver public services in a unified and consumer friendly manner to improve the community's relationship and engagement with Local Government.

The Local Authorities faced a number of obstacles to achieve the Service including the best way to connect three separate 'walled garden' ICT environments (each with their own policies, procedures and culture) in a manner that complied with the relevant IT Security and Governance requirements whilst achieving the ability to share data with a large network of external organisations not connected to the Service. The Service's supply chain also posed a significant risk under the Service's ESG strategy.

The Service appointed cybersecurity experts via the Government's Digital Marketplace to assist in developing the capability to share data with key individuals and organisations in a secure manner (therefore being aligned with the NCSC's Cloud Security Principles and GDPR). This capability also had to be consumer friendly to ensure security was not circumvented by consumers for the sake of convenience.

The appointed cybersecurity experts provided tailored support services to augment the Service's capabilities in business analysis, process mapping, best practice assessment, options appraisal and specification development. Such digital transformation is a complex process for any organisation but, in this case study, the continued focus on the community's requirements whilst balancing the need to share data with the Service's supply chain made this transition successful.

This case study illustrates the importance of having secure data sharing systems in place for your supply chain especially when you are partnering with other organisations to share data and need to take into account other stakeholders. You need to balance the requirement for easy access to data with the need for the data to be secure given the expected variance of your supply chain's cybersecurity compliance.

Case study provided by cybersecurity experts, Nine23 Ltd

Case study four: Advanced

Healthcare organisations across the world are facing increased pressure from cybercriminals. In August 2022, a ransomware attack against a software supplier had severe consequences for the NHS.

Criminal hackers took offline seven of Advanced's health systems, including software used for patient check-ins, the NHS 111 service, patient referrals, ambulance dispatch, out-of-hours appointment bookings, mental health services and emergency prescriptions. No group has been named by the attacker to our knowledge.

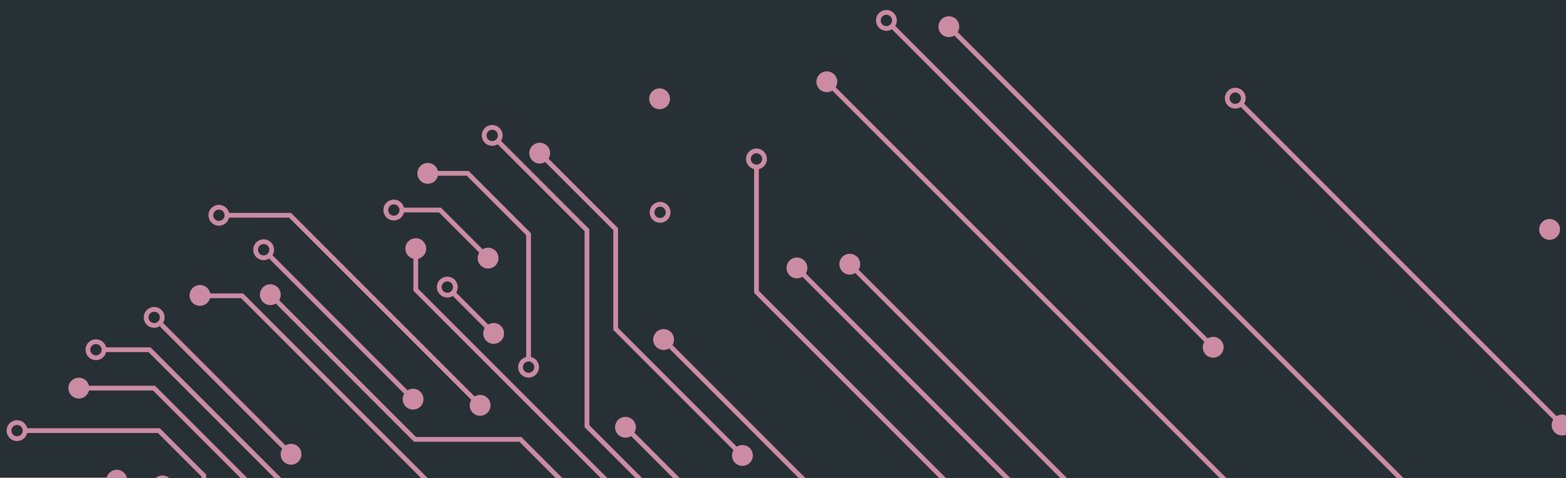
It is reported that Advanced software is used in 36 acute or mental health trusts in England and at least 9 of those trusts have been affected by the outage. We understand that it took the affected trusts weeks to recover from the incident.

This attack demonstrates the importance of understanding your third-party risk. Most public sector organisations now rely on digital integration and interoperability. Secure data sharing and access is therefore a necessity.

It is important that public bodies not only safeguard their own cyber security but also that of their supply chains. It is essential for public organisations to consider preventative measures and response procedures suppliers have in place.

With such severe implications of cyber-attacks, functionally and financially, it is also important that public organisations consider the recourse available against suppliers when negotiating contracts for the supply of digital services.

> *“Cyber insurers now closely examine an applicant’s cybersecurity posture and demand sensible levels of risk management before they grant coverage. A service which highlights critical vulnerabilities will help our clients manage risk and allows them to present as a truly cyber-resilient and insurable organisation.”*
>
> Matthew Clark, Cyber Director at Partners& Ltd



Conclusion

While cybersecurity remains complex and costly, parliament and the Government can make protection against cyber risks straightforward and affordable for the wider public sector. There is a need for a straightforward way to measure, monitor and manage cybersecurity within public institutions and across their supply chains. Organisations need to be driven by a strong commercial and reputational rationale for prioritising cybersecurity.

Further investment is needed in cybersecurity education at all levels, simplifying legislative compliance without detracting from the required protections it offers. This is not an easy ask with ever developing technology, but the reality is the UK holds a plethora of cyber expertise which needs to be unlocked and made available to all of those in need. Simplicity should be the aim to demystify defences but also to encourage collaboration, both internally and externally within organisations.

Supply chains are the backbone of the economy in the United Kingdom and provide a plethora of public services. Whilst cybersecurity threats in the supply chain have been somewhat thrust into the spotlight given the war in Ukraine, this issue needs constant monitoring. These issues will never be entirely solved by legislation and so public bodies are called to take necessary steps themselves and implement the solutions already in existence – mitigation is the key.

Contact us

Amardeep Gill
Partner

+44 (0)121 214 8838
agill@trowers.com

Louis Sebastian
Senior Associate

+44 (0)121 214 8836
lsebastian@trowers.com

Gemma Fairbrother
Associate

+44 (0)161 838 2095
gfairbrother@trowers.com

Scott Dorling
Partner

+44 (0)20 7423 8391
sdorling@trowers.com

Matt Whelan
Associate

+44 (0)121 203 5651
mwhelan@trowers.com

Bahez Talabani
Solicitor

+44 (0)121 203 5660
btalabani@trowers.com

trowers & hamlins

trowers.com

For further information, including about how we process your personal data, please consult our website https://www.trowers.com.

With contributions from…

AZETS

West Midlands Combined Authority

nine23

PARTNERS

Lockdown CYBER SECURITY