trowers & hamlins

CYBERSECURITY

Whitepaper on enhancing cyber resilience

Contents

3 Introduction

4 Background

6 Case study one: Redcar & Cleveland Borough Council

8 Legislative position

10 Case study two: Newham Council

12 Direction of travel

16 Case study three: Multi-Authority shared services

17 Case study four: Advanced

18 Conclusion

19 Contact us

> *"Over the past two years, every business has had to adapt to disruption in one form or another. Within timeframes that would have been thought impossible just a short time ago, progressive organisations rolled out new customer-facing technology and cloud-based tools that supported remote working and kept the channel to market open. But the speed of change came with a heavy price. Many businesses did not involve cybersecurity in the decision-making process, whether through oversight or an urgency to move as quickly as possible. As a result, new vulnerabilities entered an already fast-moving environment and continue to threaten many businesses today."*

Paul Brown, Director, Government & Public Sector, EY.

Introduction

Globalisation and digitisation over recent decades have moved at such a pace that cybersecurity has failed to maintain the same momentum.

Such juxtaposition has resulted in ill-prepared and misinformed businesses of all sizes being unable to, or mistakenly deciding not to, maintain the necessary protections to operate a cyber-secure business. Furthermore, it is clear that this issue is prevalent in supply chains, and no matter how much companies 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 businesses, their supply chains, and acknowledge the quantity of education which is required to reduce cybercrime. At present, the message is not getting across.

The Government 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 Government'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 businesses 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 32 per cent of UK businesses had experienced a cyber-attack in the previous 12 months. This is a decrease from 39 per cent in 2022, however, the drop is driven by smaller organisations. The results for medium business (59 per cent) and large businesses (69 per cent) remain at similar levels to last year. Of those reporting incidents, 40 per cent said they were being attacked at least once a week. According to this year's Survey, the proportion of micro businesses saying cyber security is a high priority has decreased from 80 per cent in 2022 to 68 per cent this year. Businesses, especially smaller organisations, are juggling a lot particularly given wider economic concerns like inflation and uncertainty. Cybersecurity is, however, still an issue which is clearly prevalent and needs to be a priority for all businesses.

What is currently being done to combat these worrying statistics?

The Government is actually doing a great deal to address cybersecurity concerns in line with 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.

Additionally, the UK has already taken steps to encourage 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**) but also takes a measured view when breaches are reported to them (the ICO appears to acknowledge the fact that complete compliance is difficult, and vulnerabilities cannot always be helped). This provides a balanced environment for small businesses to proportionally assess their position, whilst larger organisations may not have such flexibility.

The National Cyber Strategy 2022 – Annual Progress Report (the Report) indicates promising movement in the 18 months since publication of the Strategy. For example, over 27,000 organisations have certified to either Cyber Essentials or Cyber Essentials Plus, 12,000 small businesses are using the UK National Cybersecurity Centre's (NCSC) Cyber Action Plan, and over 15,000 are using the new 'check your cyber security' tool. The Report, however, acknowledges that interventions that are self-sustaining must be developed by working together with academia, business, the Government and the Devolved Administrations.

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 businesses (in particular SMEs) 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 therefore still more that the Government and other organisations can do to encourage good cybersecurity practices and improve cyber resilience in businesses 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: SolarWinds

In early 2020, the United States had its largest cyber-attack in recent memory, ultimately affecting Microsoft, Cisco, the Pentagon and the National Nuclear Security Administration amongst others; all of whom supposedly had strong cybersecurity practices. The significance of these entities being compromised culminated in a credible national security threat and could be sourced back to a Texas based information technology firm called SolarWinds.

The perpetrators were able to create a code which when added to SolarWinds routine system update, was installed by more than 18,000 of SolarWinds' customers, ultimately allowing access to spy on companies and government entities. This cyber-attack went undetected for 9 months, leaving SolarWinds' supply chain severely vulnerable during this time; some of whom will never know they were affected.

This attack makes it very clear that the cost of lax cybersecurity, at any point in the supply chain, can be significant, beyond simply losing data. Furthermore, it is not necessarily rogue hacking factions that businesses should be solely concerned with, but rather international governments and agencies who are often the instigators.

Following the SolarWinds hack, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency highlighted that the attack could have been prevented, or at the very least mitigated, by a decade long security recommendation to ensure all firewalls are configured to block outbound connections to the internet.

This case study illustrates the importance of being conscious of your supply chain's cybersecurity compliance, as well as your own. The question is, how many organisations changed their cybersecurity strategies as a result, including evaluating their supply chain's cybersecurity credentials, and are they still keeping on top their practices, two years down the line.

“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); and
- Committing a section 1 offence with the intention of committing further offences (section 2).

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 additional 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.

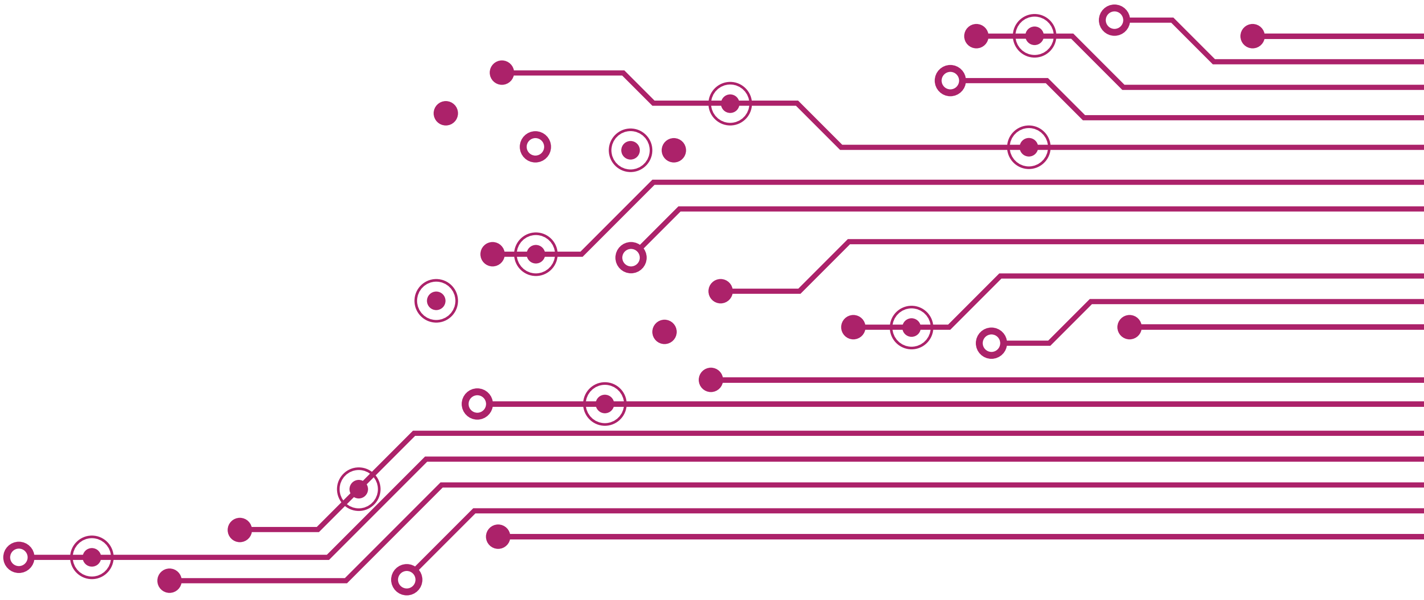
The ICO has powers under UK GDPR to fine UK businesses which are intended to encourage a compliance culture, as well as an international preferred standard. Fines of up to £8,700,000 or 2% of the undertaking's total annual worldwide turnover in the proceeding financial year, or up to £17,500,000 or 4% of the Target's total annual turnover, whichever is higher depending on which Data Protection Law is breached can be imposed..

UK GDPR and the European Union (EU) counterpart (whilst they are currently aligned) are seen as the 'gold standard' of data protection legislation. There are, however 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 businesses on the back foot, with fruitless and vexatious claims often being cheaper to pay-off rather than defend.

Following Brexit, the UK indicated that it wished to address these concerns. The Data Protection and Digital Information Bill was introduced in the House of Commons on 18 July 2022 but was subsequently withdrawn on 8 March 2023. At the same time, the Data Protection and Digital Information Bill (No. 2) Bill was introduced (the Bill). The intention is to simplify data protection legislation, reducing the burden on businesses by creating a more flexible, outcomes-focused approach rather than "box-ticking exercises". The Bill takes into account the need for a most common-sense led version of the EU GDPR to reduce cost and burden for businesses and charities.

It is unclear how the Bill will affect supply chains and whether smaller businesses 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: KP Snacks

In February 2022, KP Snacks fell victim to a Conti ransomware attack causing it to inform retailers that it could not safely process orders or dispatch goods. Conti is a highly damaging ransomware in light of the speed at which it encrypts data and spreads to other IT systems.

The cyber criminals responsible for the attack published on the darknet personal documents from employees of KP Snacks with its letterhead. The page also had a countdown timer displayed to a deadline when more documents would be published until a ransom was paid.

The disruption to KP Snack's IT systems by the ransomware attack caused supply chain issues for the large company by compromising its ordering processes. No orders could be placed or delivered by the company's supply chain until at least a month later and during that time KP Snacks had to cap orders to reflect the remaining stock.

KP Snacks initiated their cybersecurity response plan as soon as they became aware of the incident, which included engaging forensic accountants and legal counsel to assist in their investigation into the ransomware attack. Despite acting with such efficiency, the incident caused extensive supply chain upheaval for KP Snacks.

Data security is fundamental for all organisations, which this case study demonstrates. Organisations need to understand the types of data that their suppliers need to access to fulfil their contractual obligations and the risks associated with such third party relationships. How sensitive are your contracts with your suppliers? What value of information and/or assets do your suppliers hold or have access to? What are your suppliers' own security arrangements? Understanding your supply chain better and monitoring their cybersecurity measures will allow you to establish better control over access to your valuable data and reduce the risk of cyber criminals gaining access to such data.

Whilst KP Snacks did not pay the ransom demanded, there are many organisations who do contrary to the Police and NCSC's advice not to do so. Given the effect that a cyber-attack can have on stakeholders, suppliers and staff of an organisation, we understand why organisations that fall victim might feel that they have no choice but to pay the ransom. Due to a recent rise in payments to ransomware criminals, however, the NCSC and ICO emphasised in July 2022 that paying a ransom will not keep data safe or be viewed by the ICO as a mitigation in regulatory action[1]. Paying ransomware attackers also doesn't guarantee recovery of data and often takes days or weeks. In addition, whilst it is currently not illegal to pay a ransom demand in the UK there may be other criminal implications under the UK anti-money laundering and terrorist financing regime. Ransoms should not, therefore, be paid.

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 businesses and furthermore their supply chains.

Organisations need to be accountable for their cybersecurity, in particular SMEs, given 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 do this 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 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.

Boards that fail to implement good governance on cybersecurity, using appropriate tools and metrics for their organisation, will be less resilient and less sustainable. This failure, in turn, will have an impact on the other organisations they rely on to operate effectively, and ultimately, on the stability of industries, communities and governments.

Cybersecurity is not just an issue for IT departments. Boards need to be thinking about what are their organisation's key assets that it cannot operate without and how do you protect these so that, in the event of a breach, value 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 boards to better assess their organisation's cyber risk.

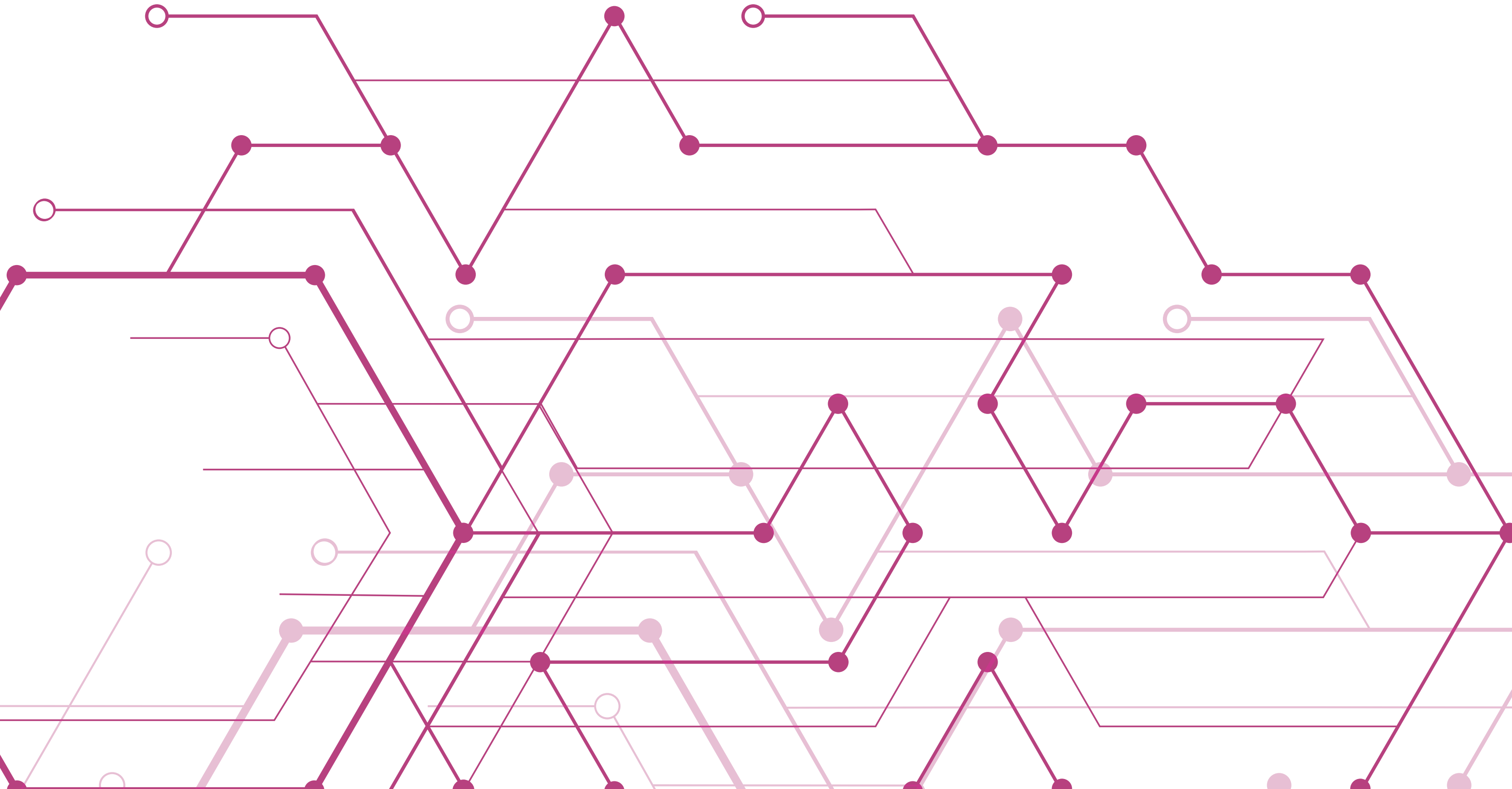
Boards, therefore, need to "get on board" and actively engage in their organisation's cybersecurity risks as part of their ESG strategy. This will become an increasingly important aspect of how investors, stakeholders and customers see your business.

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.

Given what we are starting to see across the pond, directors and officers should be mindful that they could start being held personally liable for loss suffered by the business from a data breach. Lawsuits in the USA have started to be filed against individual directors and officers for the costs of a data breach adopting the reasoning applied in the Caremark case in 1996 that directors and officers must not demonstrate a "conscious disregard" for their duties or ignore "red flags". Whilst no individual directors and officers have been held liable yet for the costs of a data breach in the USA, it feels like it is only a matter of time until this happens.

> *"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



As they say, when America sneezes, the world catches a cold. It, therefore, can only be a short while until we start seeing directors and officers in England and Wales being held personally liable for losses suffered as a result of a data breach. This possibility further highlights the importance of boards getting their ducks in a row when it comes to their cybersecurity strategy.

A key risk that organisations need to get a much better handle of 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.

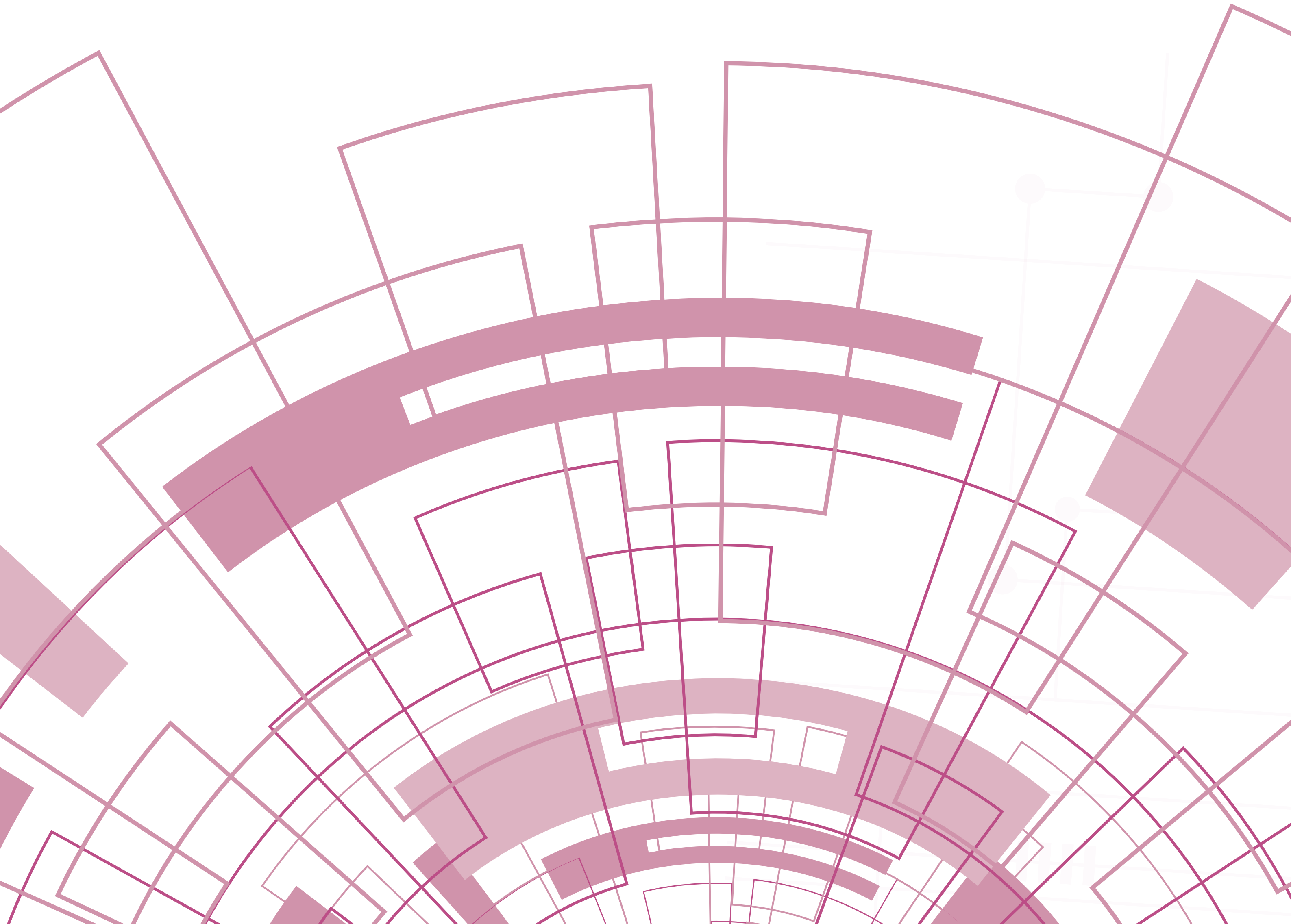
What this paper has shown is how important it is for organisations to improve their supply chain's cybersecurity compliance and keep this under regular review. Supply chain cyber management should be viewed as a shared responsibility between the organisation and their suppliers. Some ways in which organisations 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.
- 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 you 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.

> *“SMEs all too often believe they are too small to be of interest to the cybercrime groups; however, these criminal groups do not have a scope which excluded anyone. An SME with a low security budget and lack of cyber resources can offer a major vulnerability in the wider supply chain of a large organisation. It is therefore vital that every organisation firstly understands the cyber risk each supplier could bring to the business and secondly works to build cyber-resilient supplier relationships.”*

Arunava Banerjee, Senior Cyber Risk Consultant, Zurich Resilience Solutions



Case study three: Multi-Authority shared services

IIn 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.

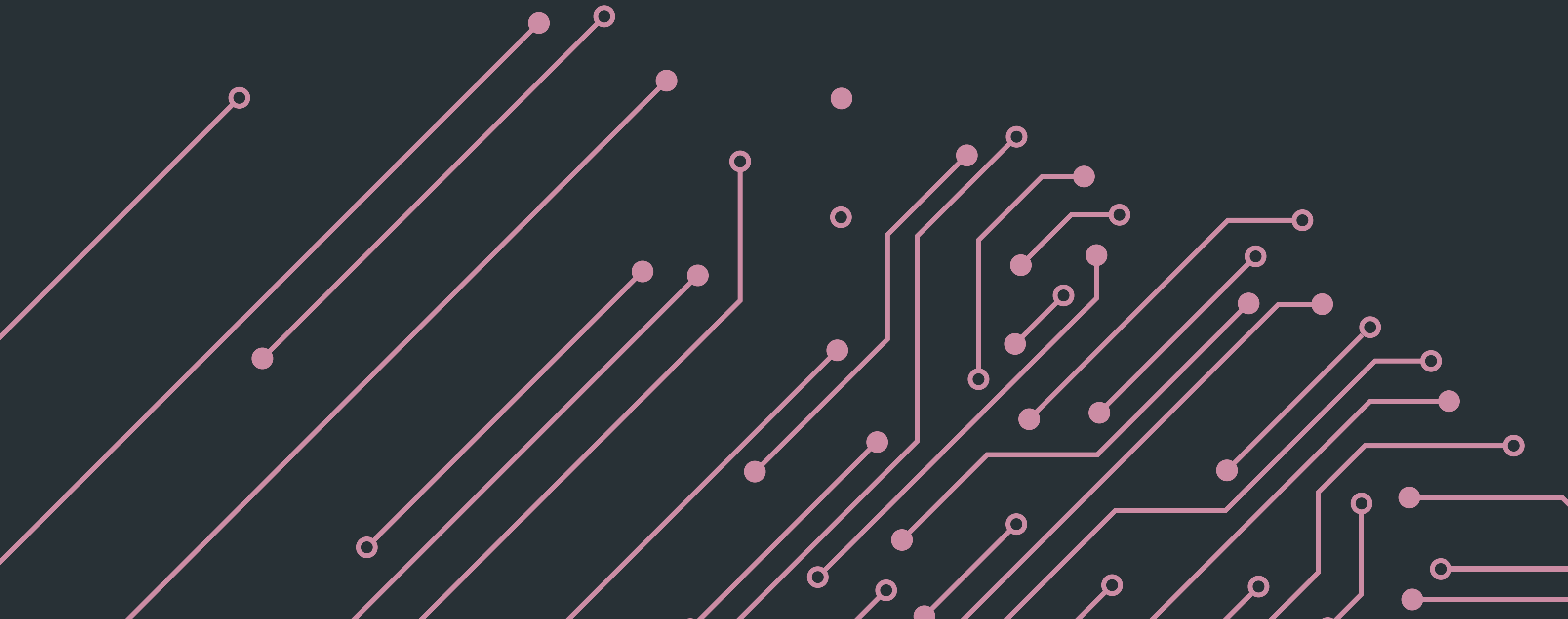
The Local Authorities faced a number of obstacles to achieve the Service including the best way to connect three separate 'walled garden' ICT environments (each with their own policies, procedures and culture) in a manner that complied with the relevant IT Security and Governance requirements whilst 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 cases 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.

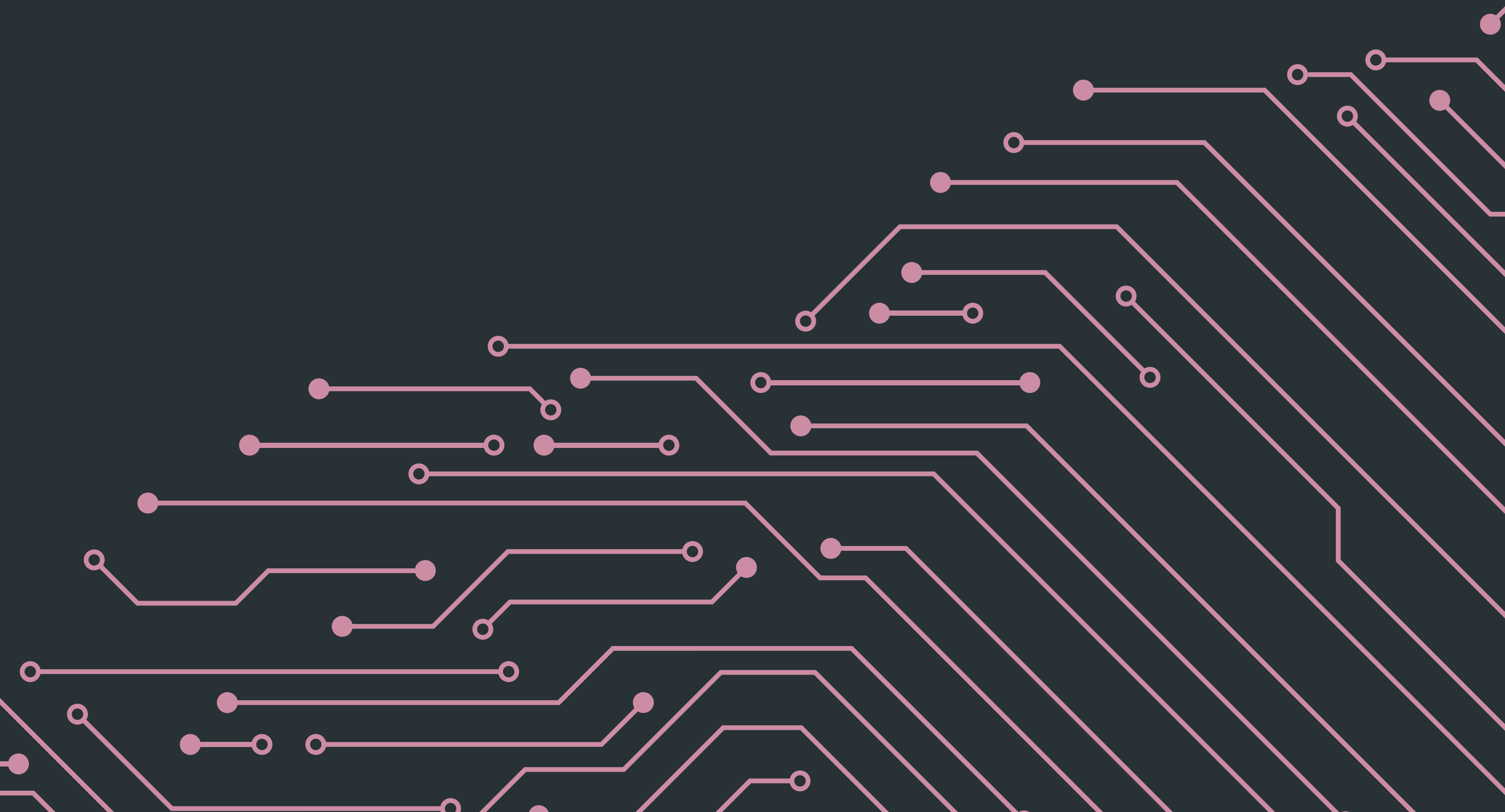
This case study illustrates the importance of having secure data sharing systems in place for your supply chain especially when you are partnering with other organisations to share data and need to take into account other stakeholders. You need to balance the requirement for easy access to data with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



“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 may be misconstrued as being complex and costly, parliament and the Government can make protection against cyber risks straightforward and affordable. There is a need for a straightforward way to measure, monitor and manage cybersecurity in a business and across supply chains. Organisations need to be driven by a strong commercial 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 in many senses and whilst cybersecurity threats in the supply chain have been somewhat thrust into the spotlight given the war in Ukraine, this issue needs constant monitoring. Sadly some problems are not entirely solvable but through the taking of small steps and utilising solutions already in existence, mitigation is the key.

> *“While large companies and organisations have invested heavily in cybersecurity, they remain vulnerable to supply chain hacking. They can protect themselves by measuring, monitoring and managing the cybersecurity across their supply chain. Cyber Risk Score was developed to allow supply chain owners to do this at no cost to them while increasing cyber awareness and resilience with their suppliers. We believe the best way forward is to protect all businesses and organisations by working together to make cybersecurity simple, straightforward and affordable.”*

Dr. Richard Fallon, Director, Cyber Risk Score, www.cr-score.com

Contact us

Amardeep Gill
Partner

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

Helen Briant
Partner

+44 (0)121 214 8867
hbriant@trowers.com

Charlotte Clayson
Partner

+44 (0)20 7423 8087
cclayson@trowers.com

Liz Mulley
Managing Associate

+44 (0)121 214 8864
emulley@trowers.com

Matt Whelan
Associate

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

Richard Fallon
Co-Founder of Cyber Risk Score

+44 (0)7789 952 251, www.cr-score.com
richard@cr-score.com

JJ Burke
Co-Founder of Cyber Risk Score

+44 (0)121 232 4699, www.cr-score.com
jj@cr-score.com

Paul Cadman
Co-Founder of Cyber Risk Score

+44 (0)121 232 8666, www.cr-score.com
pmcadman@outlook.com

trowers & hamlins

trowers.com

With contributions from…

AZETS

West Midlands Combined Authority

nine23

PARTNERS &

Lockdown CYBER SECURITY