Risk Control

Public Sector

State of the Nation Report 2023

In partnership with

GALLAGHER BASSETT

GUIDE. GUARD. GO BEYOND.

Contents

1 The State of the Nation Report 2023

Welcome to the State of the Nation Report 2023 produced by RMP Risk Control for the Public Sector. This document forms the basis of the first iteration of the report. It is anticipated that this report will be updated and republished on an annual basis.

It is hard to argue against the prevailing sentiment that the first few years of this decade have borne witness to a significantly disruptive period in modern human history. Seeking to return to a relative normality after the challenges faced by the COVID-19 pandemic, the world was quickly shocked by the outbreak of war in Ukraine. As well as the appalling loss of human life, this event acted as a catalyst for the creation of new global challenges, particularly within food and energy supply. The net result of these challenges was the creation of inflationary pressures leading directly to a cost of living crisis that hadn't been seen within the United Kingdom for over a decade.

Of course, the Public Sector does not operate within a vacuum and so has experienced the effects of this turbulent decade first-hand.

Throughout 2023 the Public Sector within the UK has faced a number of major challenges. Some of these challenges include:

- **Budget constraints**: The Public Sector has been operating within very tight budgets, with a constant pressure to balance limited resources with increasing demands for services
- **Increasing demand for services**: The Public Sector has been under constant pressure to meet the growing demands for services such as healthcare, education, and social care. This has been created by factors such as population growth, demographic changes, and evolving societal needs
- **Aging infrastructure**: Many Public Sector organisations, including transportation, housing, and utilities, are struggling with aging infrastructure that requires significant investment for maintenance and upgrades
- **Technological advancements**: The rapid pace of technological change presents challenges in terms of keeping up with digital transformation, cybersecurity, and ensuring that public services are readily accessible and efficient
- **Workforce challenges**: The Public Sector faces issues related to attracting and retaining skilled and diverse talent, succession planning, and adapting to changing workforce expectations and needs
- **Political and policy changes**: Changes in government priorities, policies, and regulations can impact the Public Sector and require organisations to adapt and respond effectively
- **Public trust and accountability**: Maintaining public trust and confidence in the Public Sector is crucial. Challenges related to transparency, accountability, and ethical conduct can arise and need to be addressed efficiently.

It is important to recognise that these challenges, and many others not considered above, can vary across different elements of the Public Sector and may evolve over time.

This report will seek to explore some of the most significant challenges that the Public Sector has faced in 2023 and should expect to face again in 2024.

2 Cyber Threat

Cyber threat is an on-going global concern.

The increasing integration of technologies within the critical functioning of societies is exposing nations of people to the direct threat posed by those who are motivated to disrupt the normal functioning of societies through attempts to disrupt critical technology-enabled resources and services.

At the organisational level, cyber incidents, such as IT outages, ransomware attacks or data breaches, was ranked by the Allianz Risk Barometer 2023[1] as the most significant risk both globally and nationally for the second year in succession.

The cyber threat in the Public Sector is significant. Government agencies and Public Sector organisations are prime targets for cyber-criminals due to the sensitive information that is held and the potential disruption that can be caused.

Some key cyber threats in the Public Sector include:

- **Phishing Attacks**: Cyber-criminals often use phishing emails to trick employees into revealing sensitive information or downloading malware. These attacks can lead to data breaches or unauthorised access to systems.
- **Ransomware Attacks**: Ransomware is a type of malware that encrypts data and demands a ransom for its release. Public Sector organisations have been targeted by ransomware attacks in the recent past, leading to data loss and significant financial costs.
- **Advanced Persistent Threats (APTs)**: APTs are sophisticated cyber-attacks that are typically carried out by nation-state actors or highly skilled hackers. These attacks can go undetected for long periods, allowing attackers to gain access to sensitive information or disrupt critical infrastructure.
- **Insider Threats**: Insider threats refer to the risk posed by employees or contractors who misuse their access privileges to steal or leak sensitive information. Public Sector organisations need to implement robust security measures to mitigate this risk.
- **Supply Chain Attacks**: Public Sector organisations often rely on third-party vendors and suppliers for various services. Cyber-criminals may target these suppliers to gain unauthorised access to the organisation's systems or data.

To address these threats, the UK Government has implemented various cybersecurity initiatives, such as the creation of the National Cyber Security Centre (NCSC)[2] and the Cyber Essentials Certification Scheme[3] which is an industry-supported scheme to help organisations protect themselves against common online threats.

Public sector organisations are positively encouraged to follow best practices, including regular cyber security assessments, employee training, and the implementation of strong cyber security controls, to protect themselves against the sustained threat.

3 Budget Constraints

According to the Office for National Statistics[4], as of October 2023, the Public Sector Net Debt (PSND ex) in the United Kingdom stood at a quite staggering £2,643.7 billion. This amount was provisionally estimated to be around 97.8% of the UK's annual Gross Domestic Product (GDP). Excluding the Bank of England, the Public Sector net debt was £2,394.8 billion, which was approximately 88.6% of GDP.

These eye-watering levels of Public Sector debt have not been seen in the UK since the early 1960s.

The almost inevitable consequence of the current state of the Public Sector economy is budget constraints caused by reductions in funding. In the worst case scenarios, Public Sector organisations are forced to issue a Section 114 Notice, effectively declaring that the organisation is about to incur expenditure that is unlawful according to the Local Government Finance Act 1988[5].

Budget constraints can have a significant impact on Public Sector organisations. Some effects may include:

- **Limited resources**: Budget constraints mean that Public Sector organisations have limited financial resources to allocate towards their various programs and initiatives. This can result in a lack of funding for important projects or services, leading to delays or even cancellations.
- **Prioritisation of spending**: Budget constraints force Public Sector organisations to prioritise their spending. They must carefully consider which programs or services are most essential and allocate funds accordingly. This can result in some programs being given higher priority while others may receive reduced funding or be eliminated altogether.
- **Efficiency and cost-cutting measures**: Budget constraints often lead to a focus on efficiency and cost-cutting measures within Public Sector organisations. They may need to find ways to streamline operations, reduce overhead costs, or find alternative sources of funding, such as through income generating projects, to make the most of their limited resources.
- **Impact on staffing and workforce**: Budget constraints can also affect the size and composition of the workforce within Public Sector organisations. Hiring freezes, layoffs, or reduced hours may be implemented to control staffing costs. This can lead to a strain on existing staff, increased workloads, and potential impacts on service delivery. Increased workloads can have a detrimental effect on productivity as well as the wellbeing of staff.
- **Innovation and creativity**: Budget constraints can drive innovation and creativity within the Public Sector. They may be forced to find new and innovative ways to deliver services or achieve their goals with limited resources. This can lead to the adoption of new technologies, partnerships with other organisations, or the development of alternative service delivery models such as outsourcing.
- **Public perception and trust**: Budget constraints can impact public perception and trust in Public Sector organisations. If services are reduced or eliminated due to budget constraints, it can lead to dissatisfaction among the public and a perception that the organisation is not effectively meeting their needs. This can erode trust and support for the organisation and ultimately harm its reputation.

Overall, budget constraints have a significant impact on the Public Sector, requiring them to carefully manage their resources, prioritise spending, and find innovative ways to deliver services with limited funding.

In such circumstances it is essential that Public Sector organisations utilise a risk-based approach within its considerations to ensure that it makes the most informed decisions possible, reducing the impact on the organisation itself and its service users.

4 Martyn’s Law

Martyn's Law refers to a proposed legislation within the UK which is aimed at improving public safety and security at public venues and events. It is named after Martyn Hett, one of the victims of the Manchester Arena bombing in 2017. The law seeks to make it mandatory for public venues to have effective security measures in place, including the development of comprehensive security plans, regular risk assessments, and staff training. The goal is to enhance the protection of the public and reduce the risk of terrorist attacks or other incidents at crowded places.

Martyn's Law has not yet passed as legislation, however, it will apply across the UK and will be implemented using a tiered model that considers the activities and capacity of each location.

Standard tier: For locations with a capacity of over 100 people, a standard tier will be applied. These locations can undertake low-cost yet effective activities to enhance preparedness. This may include training, sharing information, and creating a preparedness plan that incorporates practices like locking doors to delay attackers or knowledge of life-saving treatments that staff can administer while waiting for emergency services.

Advanced tier: An enhanced tier will focus on high-capacity locations, recognising the potential consequences of a successful attack. Locations with a capacity of over 800 people will be required to conduct a risk assessment to develop and implement a comprehensive security plan. Additional measures may include fostering a culture of vigilance and security, implementing physical measures like CCTV, or adopting new systems and processes to improve security considerations.

To ensure compliance and encourage positive cultural change, the government will establish an inspection and enforcement regime, issuing fair and credible sanctions for serious breaches.

The government will also provide dedicated statutory guidance and tailored support to help those affected by Martyn's Law fulfil their responsibilities. Even small venues will have the opportunity to benefit from this support and take voluntary action. Additionally, the online protective security hub, ProtectUK[6], already offers expert advice, training, and guidance.

To comply with Martyn's Law, Public Sector organisations should take the following steps:

- **Risk assessment**: Organisations should conduct risk assessments to identify potential risks and vulnerabilities at their publicly accessible locations. Factors to consider include venue capacity, the activities taking place, and the potential consequences of a terrorist attack.
- **Security plan**: Based on the risk assessment, organisations should develop and implement a detailed and comprehensive security plan that outlines the measures and procedures to be implemented to enhance public safety. This should include staff training, information sharing, physical security measures, emergency response protocols, and communication strategies.
- **Security culture**: Organisations should promote a culture of vigilance among staff and visitors, encouraging them to report any suspicious activities or concerns. This can be achieved through awareness campaigns, training programs, and regular communications.
- **Review and update**: Public Sector organisations should continuously review and update their security measures to adapt to changing threats and circumstances. This may involve conducting regular risk assessments, seeking expert advice, and staying informed about best practices.
- **Inspections and enforcement**: Organisations should cooperate with any inspection and enforcement regime established by the government to ensure compliance with Martyn's Law. This includes addressing any identified deficiencies or breaches promptly.
- **Guidance and support**: Public Sector organisations can benefit from the dedicated statutory guidance and bespoke support provided by the government to effectively discharge their responsibilities under Martyn's Law.

At the time of the production of this report, the UK National Threat Level was set by the Joint Terrorism Analysis Centre[7] as ‘**Substantial’** meaning an attack is likely.

5 Lithium-ion Batteries

Lithium-ion batteries, sometimes referred to as Li-ion cells, are widely used and can be found powering anything from disposable vapes, mobile phones, laptops, E-Bikes, E-Scooters, electric vehicles and aircraft. Lithium-ion cells are also being used to provide backup power to data centres, hospitals and any other facilities that may need a reliable back-up power source.

The popularity in the use of Lithium-ion batteries in an increasing array of equipment and applications is associated with multiple benefits which they offer over more long-standing battery technologies. They last longer, recharge faster, are more efficient, and maintain a longer lifespan.

However, as the use of Lithium-ion batteries has rapidly increased, so has the number of fires associated with their usage[8].

The reason for the increase in associated fires is that Lithium-ion batteries can be very volatile due to their high energy density and many combustible components utilised in their construction. If they are overcharged, damaged or treated incorrectly they can explode and / or cause serious fires.

Some common causes of Lithium-ion battery failures include manufacturing defects, mechanical damage, poor storage, overcharging and over-discharging, the use of incompatible chargers, unauthorised electrical modifications, and the use of DIY conversion kits (on bicycles and E-bikes etc.).

There is an abundance of advice available from authoritative sources to reduce the risks to members of the public and employees.[9] [10] [11] As we might expect, there is consistency in the advice provided, including:

- Always use the charger that was provided with the electronic device, or a replacement from a reliable brand and source. Be careful of fake or poor quality replacement chargers or cables.
- Avoid storing, using or charging batteries at very high or very low temperatures.
- Don’t leave electrical items continuously on charge after the charge cycle is complete.
- Never cover chargers or charging devices.
- Protect batteries against being damaged – whether crushed, punctured or immersed in water.
- Take any damaged batteries or chargers out of use immediately, even on suspicion alone.

Due to the risk of explosion and fire associated with Lithium-ion batteries, it is important that their use within the workplace is assessed for risk, and the appropriate controls identified and implemented. The specific duties in respect of fire safety in the workplace are contained within the Regulatory Reform (Fire Safety) Order 2005.[12]

The publication of the UK Government’s ‘Net Zero: Build Back Greener Strategy’[13] in October 2021 signalled a national shift from the use of fossil fuels to greener energy technologies across industry. As a part of this strategy a path to zero emission vehicles by 2035 has been defined, with 80% of new cars and 70% of new vans sold in Great Britain set to be zero emission by 2030, increasing to 100% by 2035.[14]

For many Public Sector organisations who operate large fleets of vehicles, the transition to zero emission vehicles to reduce their carbon footprint has already begun. In order to operate a fleet of zero emission vehicles, the organisation has to have access to the right infrastructure, including vehicle maintenance and charging equipment.

It is important that the risks associated with the introduction of these technologies into the workplace is managed effectively. This can be achieved through a suitable and sufficient risk assessment.

Organisations should ensure that they comply with all associated regulations and best practice guidance, and consult with their insurer.

In respect of the installation of electric vehicle charging points, careful consideration must be given to their location as to not unnecessarily increase fire risk. The Fire Protection Authority have issued reliable guidance on the subject within their publication ‘RC59 Recommendations for fire safety when charging electric vehicles’.[15]

6 Artificial Intelligence

Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. It involves the development of computer systems capable of performing tasks that typically require human intelligence, such as speech recognition, decision-making, problem-solving, and language translation. AI can be categorised into two types: narrow AI, which is designed for specific tasks, and general AI, which has the ability to understand, learn, and apply knowledge across various domains. AI technologies include machine learning, natural language processing, computer vision, and robotics.

The UK Government has issued 'A guide to using artificial intelligence in the public sector'.[16] It recognises that AI has the potential to revolutionise the public sector by improving efficiency, decision-making, and service delivery. Here are some ways AI could be used within the Public Sector:

- **Data analysis and insights**: AI can analyse large volumes of data to identify patterns, trends, and insights. This can help government agencies make data-driven decisions, detect fraud, predict outcomes, and optimise resource allocation.
- **Chatbots and virtual assistants**: AI-powered chatbots and virtual assistants can handle routine inquiries, provide information, and assist with transactions.
- **Predictive analytics for public safety**: AI can analyse historical crime data, social media feeds, and other relevant information to predict crime hotspots, identify potential threats, and allocate resources accordingly. This can enhance public safety and emergency response.
- **Personalised services**: AI can personalise services by analysing individual preferences, behaviour, and needs. This can enable tailored recommendations, targeted communication, and service delivery.
- **Automation of administrative tasks**: AI can automate repetitive administrative tasks, such as data entry, document processing, and record keeping. This can save time and resources.
- **Healthcare and public health**: AI can assist in diagnosing diseases, predicting outbreaks, and improving healthcare delivery. This can enhance patient care and improve public health outcomes.

While AI offers numerous benefits, caution should be exercised as there are also risks and challenges associated with its development and deployment. Forbes[17] have illustrated some of the key risks:

- **Job displacement**: AI has the potential to automate tasks currently performed by humans, leading to job losses and changes in the job market.
- **Bias and discrimination**: AI systems are trained on data, and if the training data is biased or reflects societal prejudices, the AI systems can perpetuate and amplify those biases.
- **Privacy and security concerns**: AI systems often require access to large amounts of personal data, raising concerns about privacy and data protection. If not properly secured, AI systems can be vulnerable to cyberattacks, leading to unauthorised access and misuse of sensitive information.
- **Lack of transparency and accountability**: Some AI algorithms, such as deep learning neural networks, can be complex and difficult to interpret.
- **Ethical considerations**: AI raises ethical dilemmas, such as the potential for autonomous weapons, invasion of privacy, and the impact on human autonomy and decision-making.
- **Dependence and overreliance**: Overreliance on AI systems without proper human oversight and intervention can lead to errors or failures. It is important to strike a balance between the capabilities of AI and human judgment.
- **Unemployment and socioeconomic inequality**: The widespread adoption of AI could lead to significant job displacement, potentially exacerbating socioeconomic inequalities. It is crucial to address these challenges through reskilling and upskilling programs and social safety nets.

It is important that in the fullness of time, any regulations, standards, and ethical guidelines which are developed to ensure the responsible and beneficial use of AI technology are fully adhered to.

7 Supply Chain

A supply chain refers to the network of organisations, individuals, activities, information, and resources involved in the production, distribution, and delivery of goods or services to the end consumer. It encompasses all the steps and processes required to transform raw materials into finished products and deliver them to customers.

A typical supply chain includes various entities such as suppliers, manufacturers, distributors, retailers, and customers. It involves the flow of materials, information, and finances from the initial sourcing of raw materials to the final delivery of the product to the consumer.

Public Sector organisations can maintain various positions within a supply chain, from supplier right though to consumer.

Supply chain management involves activities such as demand forecasting, procurement and sourcing, production planning, inventory management, transportation and logistics, and customer relationship management. It also involves the use of technologies and systems to track and manage the flow of goods, information, and finances throughout the supply chain.

Overall, a supply chain is a complex and interconnected system that plays a crucial role in the efficient and effective movement of goods and services from suppliers to customers.

Supply chains are vulnerable to various risks, including poor supplier performance, demand planning complexity, global labour shortage, rising inflation, volatile global economy, complex regulatory environments, geopolitical risk, reputational risk, natural disasters and climate risk, and cyber risk.[18]

Supply chain risk management aims to proactively identify and assess potential risks, develop strategies to mitigate them, and establish contingency plans to ensure business continuity. It involves the following key steps:

- **Risk identification**: Identifying and understanding potential risks that can impact the supply chain, including both internal and external factors.
- **Risk assessment**: Evaluating the likelihood and potential impact of identified risks on the supply chain. This involves analysing the probability of occurrence and the severity of consequences.
- **Risk mitigation**: Developing strategies and measures to reduce the likelihood and impact of risks. This may involve diversifying suppliers, implementing backup plans, improving communication and collaboration with suppliers, and investing in technology and systems to enhance visibility and traceability.
- **Risk monitoring**: Continuously monitoring and tracking potential risks to identify any changes or emerging risks. This allows for timely response and adaptation to mitigate the impact of risks.
- **Contingency planning**: Developing contingency plans and response strategies to effectively manage and recover from disruptions. This includes establishing alternative sourcing options, creating emergency response plans, and maintaining adequate inventory levels.

Identifying critical supplies is a crucial aspect of effective supply chain risk management. Critical supplies are those materials, components, or services that are essential for the production or operation of an organisation and whose disruption or unavailability can significantly impact its ability to meet customer demands or maintain business operations.

'ISO 28004-1:2007 Security management systems for the supply chain'[19] emphasises the importance of collaboration and cooperation among supply chain partners to ensure the effective implementation of security measures. It encourages organisations to establish communication channels and share relevant security information to mitigate risks and enhance the overall security of the supply chain.

By implementing ISO 28004-1:2007, organisations can enhance their security management systems, reduce vulnerabilities, and improve the resilience of their supply chains. It helps organisations to identify and address potential security threats, protect their assets, and maintain the integrity and reliability of their supply chain operations.

References

1. https://www.allianz.com/en/press/news/studies/230117_Allianz-Risk-Barometer-2023.html
2. https://www.ncsc.gov.uk/
3. https://www.ncsc.gov.uk/cyberessentials/overview
4. https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/publicsectorfinance/bulletins/publicsectorfinances/october2023
5. https://www.legislation.gov.uk/ukpga/1988/41/section/114
6. https://www.protectuk.police.uk/
7. https://www.mi5.gov.uk/threat-levels
8. https://www.fia.uk.com/news/safety-alert-overheating-lithium-batteries-may-cause-a-christmas-fire-hazard-for-e-bikes-and-e-scooters.html
9. https://www.london-fire.gov.uk/safety/the-home/electrical-items/batteries-and-chargers/
10. https://www.thefpa.co.uk/advice-and-guidance/free-documents?q=RE2:%20Lithium-ion%20Battery%20Use%20and%20Storage
11. https://www.osha.gov/sites/default/files/publications/shib011819.pdf
12. https://www.legislation.gov.uk/uksi/2005/1541/contents/made
13. https://assets.publishing.service.gov.uk/media/6194dfa4d3bf7f0555071b1b/net-zero-strategy-beis.pdf
14. https://www.gov.uk/government/news/government-sets-out-path-to-zero-emission-vehicles-by-2035
15. https://www.thefpa.co.uk/advice-and-guidance/firesafetywhenchargingelectricvehicles
16. https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector
17. https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/
18. https://www.moodysanalytics.com/articles/2022/the-top-10-supply-chain-risks-that-companies-face
19. https://www.iso.org/standard/44962.html

Further Support

RMP Risk Control has a proven track record in strengthening organisational risk and safety culture and lowering claims numbers and costs. By working in close partnership with our clients we raise and augment the profile of enterprise risk management across organisations. Our team of qualified and experienced consultants based throughout the country have extensive experience of working closely with organisations, within the realms of health and safety, enterprise risk management, and fleet risk management to develop and deliver bespoke risk control programmes which are tailored to our clients' needs.

If you would like further information on any of our risk control services or to discuss your risk and safety needs, please contact your appointed RMP Risk Consultant, Ashley Easen - Director of Risk Consulting and ESG, or your appointed RMP Account Director.

Ashley Easen
Director – Risk Consulting and ESG

Tel: (+44) 07825 365090

ashley_easen@gbtpa.com

www.gallagherbassett.co.uk

On occasion, RMP Risk Control will deliver services via our extended network of approved Associate Consultants. These consultants have successfully passed our stringent vetting processes and their use will be agreed with our clients prior to project initiation.

Risk Management Partners

67 Lombard Street
London EC3V 9LJ
020 7204 1800
contact@rmpartners.co.uk

rmpartners.co.uk

Visit our website and find out more facts about the public sector:
rmpartners.co.uk

Dedication in action

FP162-2024