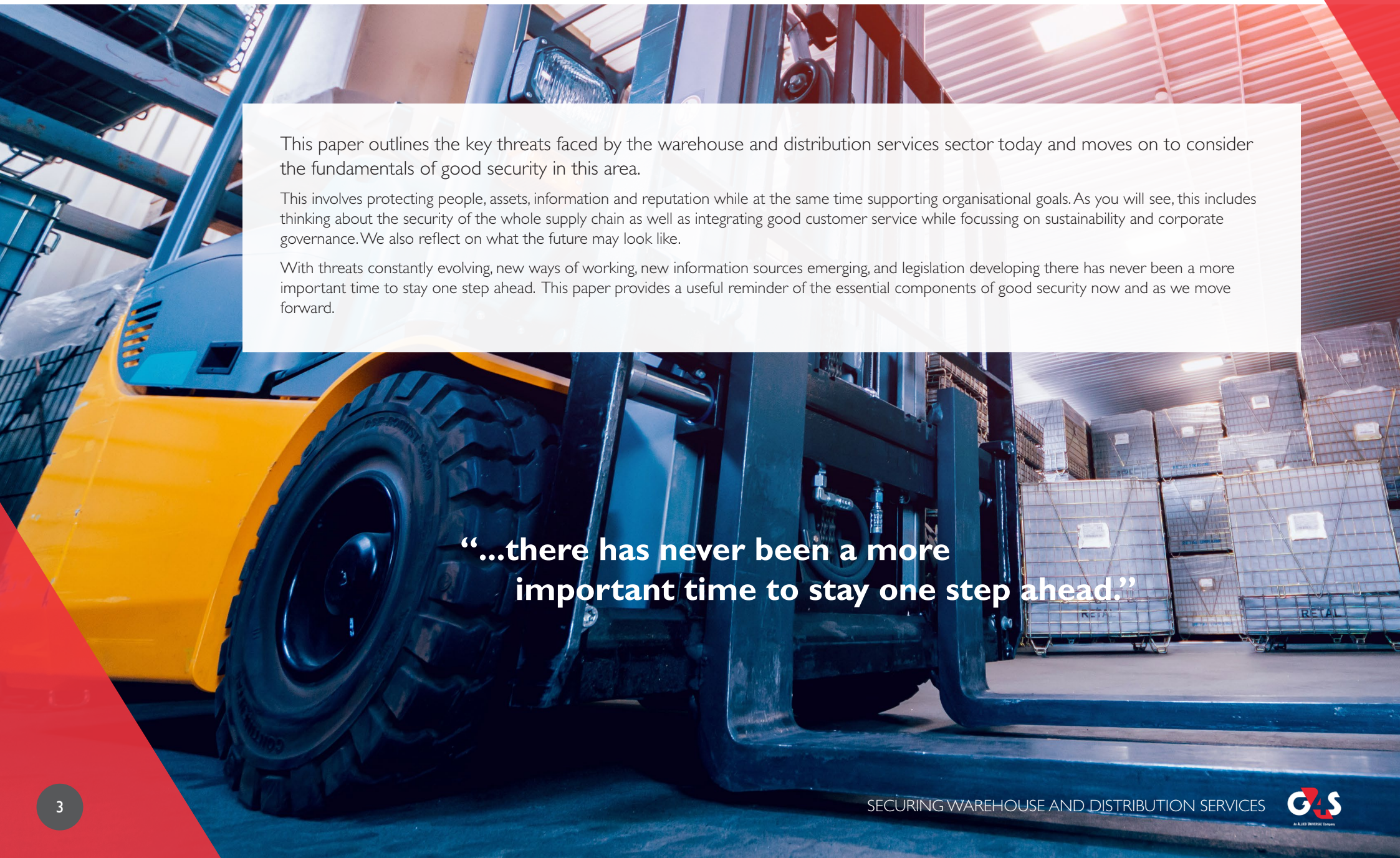
Securing Warehouse and Distribution Services

G4S

An Allied Universal Company

CONTENTS

I INTRODUCTION



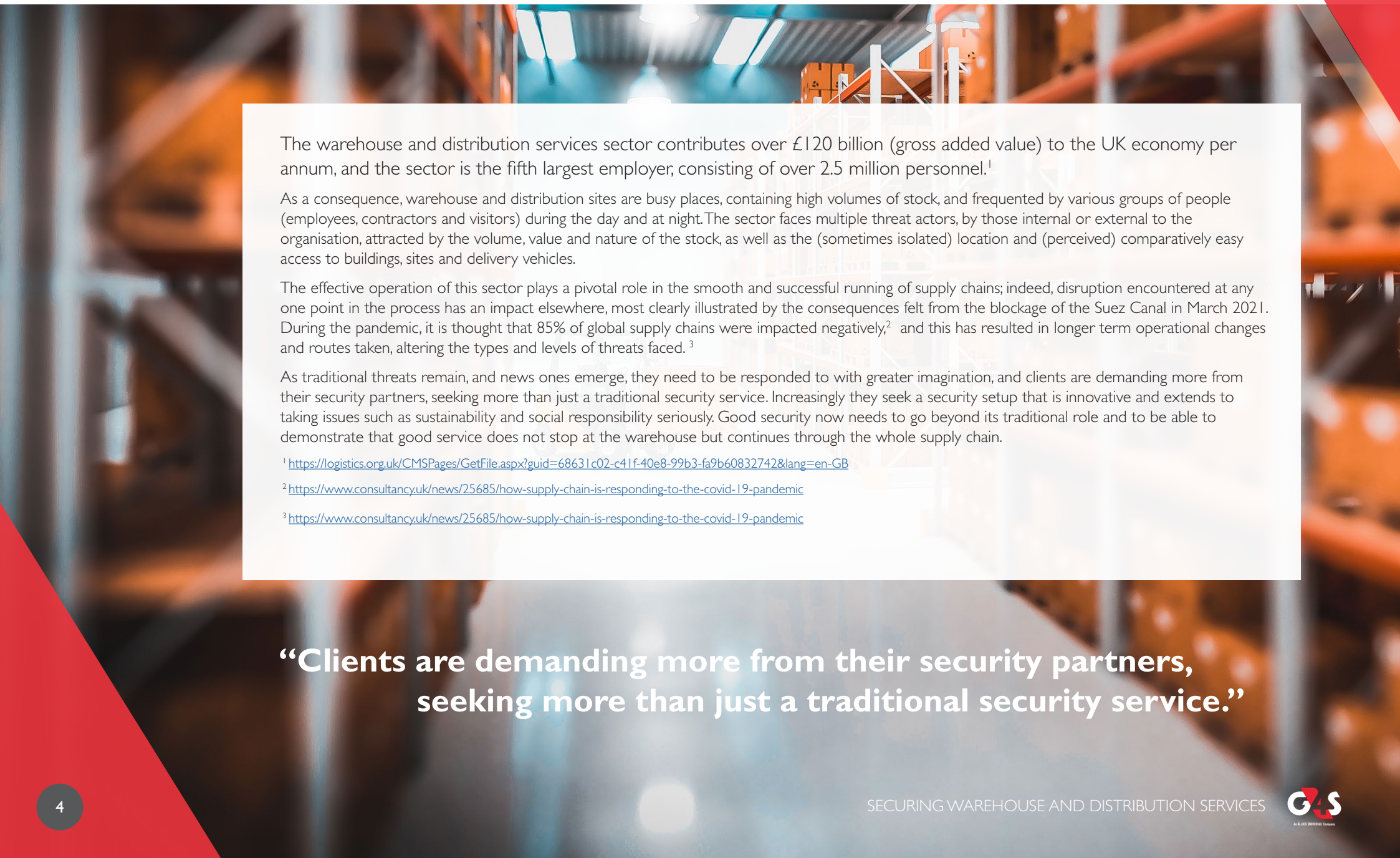
This paper outlines the key threats faced by the warehouse and distribution services sector today and moves on to consider the fundamentals of good security in this area.

This involves protecting people, assets, information and reputation while at the same time supporting organisational goals. As you will see, this includes thinking about the security of the whole supply chain as well as integrating good customer service while focussing on sustainability and corporate governance. We also reflect on what the future may look like.

With threats constantly evolving, new ways of working, new information sources emerging, and legislation developing there has never been a more important time to stay one step ahead. This paper provides a useful reminder of the essential components of good security now and as we move forward.

"...there has never been a more important time to stay one step ahead."

1 THE THREATS FACING THE SECTOR



The warehouse and distribution services sector contributes over £120 billion (gross added value) to the UK economy per annum, and the sector is the fifth largest employer, consisting of over 2.5 million personnel.[1]

As a consequence, warehouse and distribution sites are busy places, containing high volumes of stock, and frequented by various groups of people (employees, contractors and visitors) during the day and at night. The sector faces multiple threat actors, by those internal or external to the organisation, attracted by the volume, value and nature of the stock, as well as the (sometimes isolated) location and (perceived) comparatively easy access to buildings, sites and delivery vehicles.

The effective operation of this sector plays a pivotal role in the smooth and successful running of supply chains; indeed, disruption encountered at any one point in the process has an impact elsewhere, most clearly illustrated by the consequences felt from the blockage of the Suez Canal in March 2021. During the pandemic, it is thought that 85% of global supply chains were impacted negatively,[2] and this has resulted in longer term operational changes and routes taken, altering the types and levels of threats faced. [3]

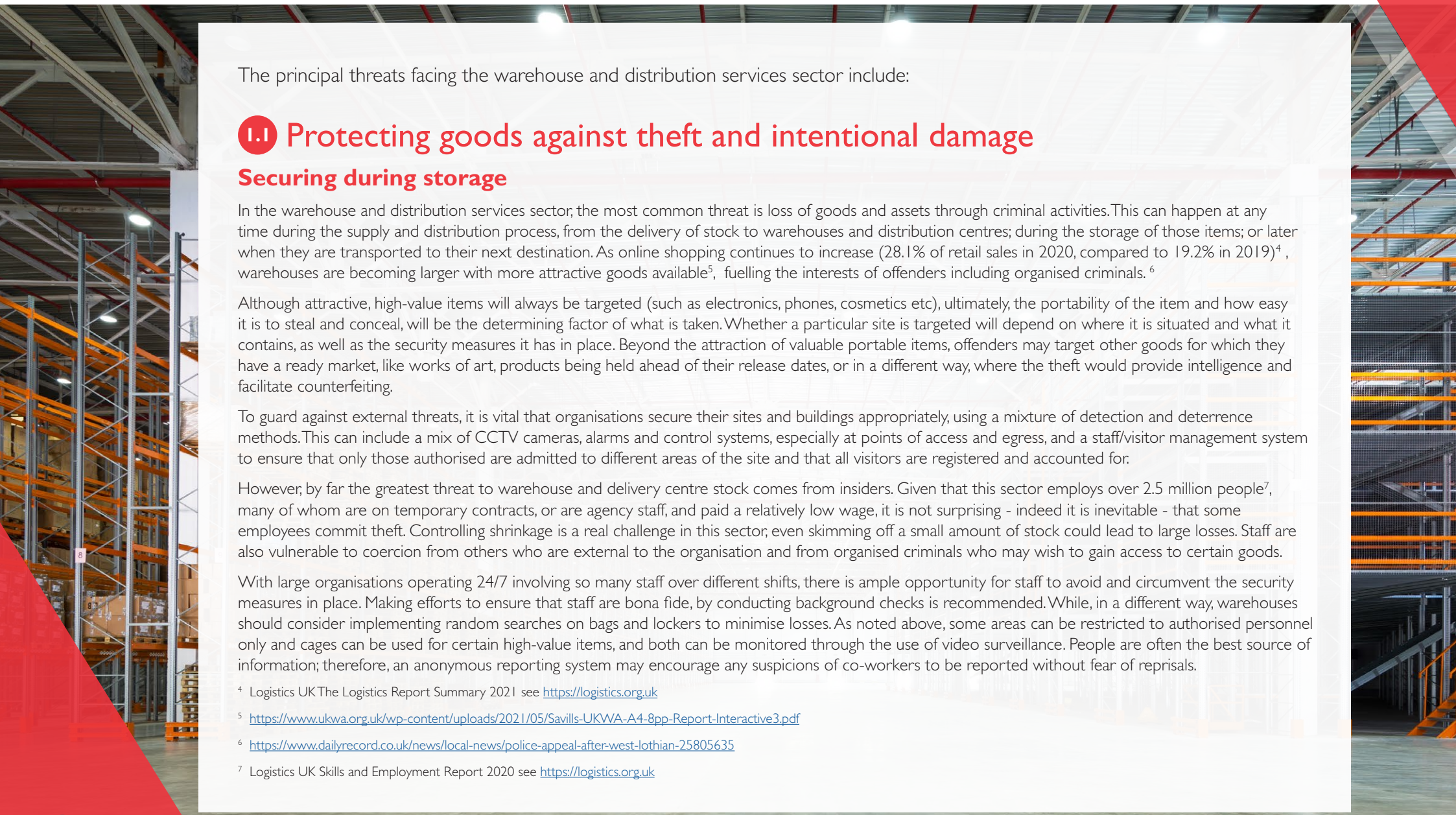
As traditional threats remain, and news ones emerge, they need to be responded to with greater imagination, and clients are demanding more from their security partners, seeking more than just a traditional security service. Increasingly they seek a security setup that is innovative and extends to taking issues such as sustainability and social responsibility seriously. Good security now needs to go beyond its traditional role and to be able to demonstrate that good service does not stop at the warehouse but continues through the whole supply chain.

[1] https://logistics.org.uk/CMSPages/GetFile.aspx?guid=68631c02-c41f-40e8-99b3-fa9b60832742&lang=en-GB

[2] https://www.consultancy.uk/news/25685/how-supply-chain-is-responding-to-the-covid-19-pandemic

[3] https://www.consultancy.uk/news/25685/how-supply-chain-is-responding-to-the-covid-19-pandemic

"Clients are demanding more from their security partners, seeking more than just a traditional security service."



The principal threats facing the warehouse and distribution services sector include:

1.1 Protecting goods against theft and intentional damage

Securing during storage

In the warehouse and distribution services sector, the most common threat is loss of goods and assets through criminal activities. This can happen at any time during the supply and distribution process, from the delivery of stock to warehouses and distribution centres; during the storage of those items; or later when they are transported to their next destination. As online shopping continues to increase (28.1% of retail sales in 2020, compared to 19.2% in 2019)[4] , warehouses are becoming larger with more attractive goods available[5], fuelling the interests of offenders including organised criminals. [6]

Although attractive, high-value items will always be targeted (such as electronics, phones, cosmetics etc), ultimately, the portability of the item and how easy it is to steal and conceal, will be the determining factor of what is taken. Whether a particular site is targeted will depend on where it is situated and what it contains, as well as the security measures it has in place. Beyond the attraction of valuable portable items, offenders may target other goods for which they have a ready market, like works of art, products being held ahead of their release dates, or in a different way, where the theft would provide intelligence and facilitate counterfeiting.

To guard against external threats, it is vital that organisations secure their sites and buildings appropriately, using a mixture of detection and deterrence methods. This can include a mix of CCTV cameras, alarms and control systems, especially at points of access and egress, and a staff/visitor management system to ensure that only those authorised are admitted to different areas of the site and that all visitors are registered and accounted for.

However, by far the greatest threat to warehouse and delivery centre stock comes from insiders. Given that this sector employs over 2.5 million people[7], many of whom are on temporary contracts, or are agency staff, and paid a relatively low wage, it is not surprising - indeed it is inevitable - that some employees commit theft. Controlling shrinkage is a real challenge in this sector, even skimming off a small amount of stock could lead to large losses. Staff are also vulnerable to coercion from others who are external to the organisation and from organised criminals who may wish to gain access to certain goods.

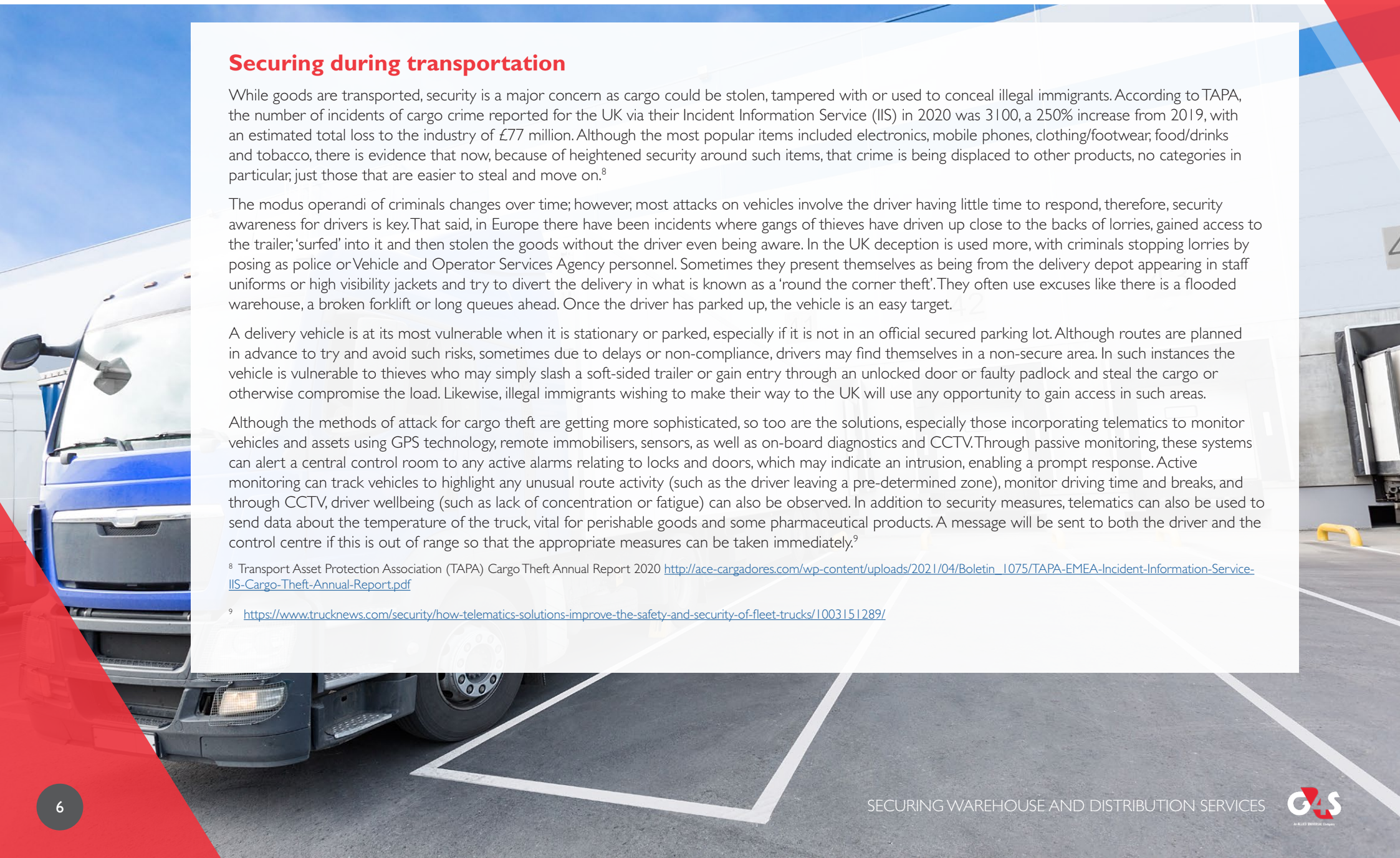
With large organisations operating 24/7 involving so many staff over different shifts, there is ample opportunity for staff to avoid and circumvent the security measures in place. Making efforts to ensure that staff are bona fide, by conducting background checks is recommended. While, in a different way, warehouses should consider implementing random searches on bags and lockers to minimise losses. As noted above, some areas can be restricted to authorised personnel only and cages can be used for certain high-value items, and both can be monitored through the use of video surveillance. People are often the best source of information; therefore, an anonymous reporting system may encourage any suspicions of co-workers to be reported without fear of reprisals.

[4] Logistics UK The Logistics Report Summary 2021 see https://logistics.org.uk

[5] https://www.ukwa.org.uk/wp-content/uploads/2021/05/Savills-UKWA-A4-8pp-Report-Interactive3.pdf

[6] https://www.dailyrecord.co.uk/news/local-news/police-appeal-after-west-lothian-25805635

[7] Logistics UK Skills and Employment Report 2020 see https://logistics.org.uk



Securing during transportation

While goods are transported, security is a major concern as cargo could be stolen, tampered with or used to conceal illegal immigrants. According to TAPA, the number of incidents of cargo crime reported for the UK via their Incident Information Service (IIS) in 2020 was 3100, a 250% increase from 2019, with an estimated total loss to the industry of £77 million. Although the most popular items included electronics, mobile phones, clothing/footwear, food/drinks and tobacco, there is evidence that now, because of heightened security around such items, that crime is being displaced to other products, no categories in particular, just those that are easier to steal and move on.[8]

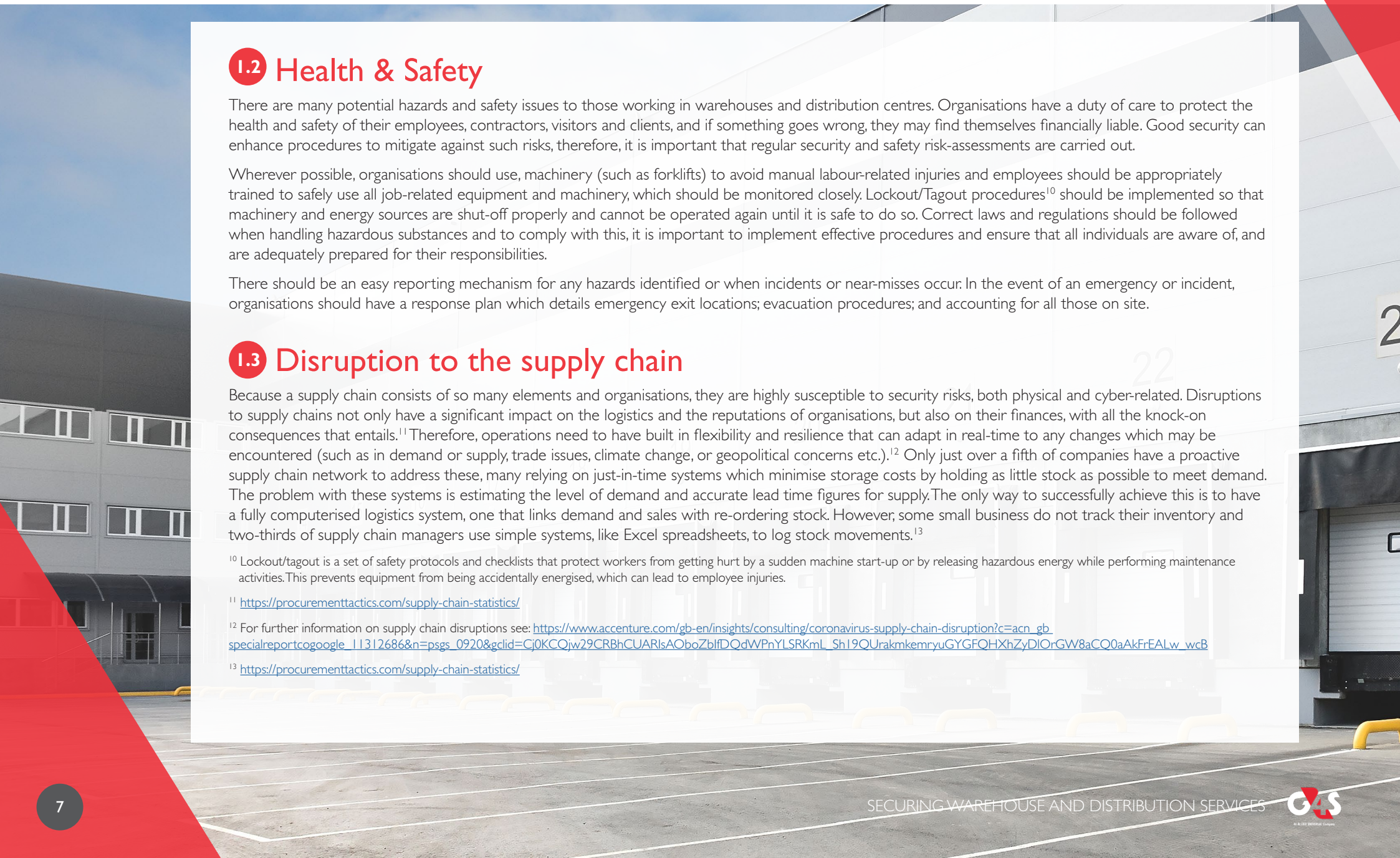
The modus operandi of criminals changes over time; however, most attacks on vehicles involve the driver having little time to respond, therefore, security awareness for drivers is key. That said, in Europe there have been incidents where gangs of thieves have driven up close to the backs of lorries, gained access to the trailer, 'surfed' into it and then stolen the goods without the driver even being aware. In the UK deception is used more, with criminals stopping lorries by posing as police or Vehicle and Operator Services Agency personnel. Sometimes they present themselves as being from the delivery depot appearing in staff uniforms or high visibility jackets and try to divert the delivery in what is known as a 'round the corner theft'. They often use excuses like there is a flooded warehouse, a broken forklift or long queues ahead. Once the driver has parked up, the vehicle is an easy target.

A delivery vehicle is at its most vulnerable when it is stationary or parked, especially if it is not in an official secured parking lot. Although routes are planned in advance to try and avoid such risks, sometimes due to delays or non-compliance, drivers may find themselves in a non-secure area. In such instances the vehicle is vulnerable to thieves who may simply slash a soft-sided trailer or gain entry through an unlocked door or faulty padlock and steal the cargo or otherwise compromise the load. Likewise, illegal immigrants wishing to make their way to the UK will use any opportunity to gain access in such areas.

Although the methods of attack for cargo theft are getting more sophisticated, so too are the solutions, especially those incorporating telematics to monitor vehicles and assets using GPS technology, remote immobilisers, sensors, as well as on-board diagnostics and CCTV. Through passive monitoring, these systems can alert a central control room to any active alarms relating to locks and doors, which may indicate an intrusion, enabling a prompt response. Active monitoring can track vehicles to highlight any unusual route activity (such as the driver leaving a pre-determined zone), monitor driving time and breaks, and through CCTV, driver wellbeing (such as lack of concentration or fatigue) can also be observed. In addition to security measures, telematics can also be used to send data about the temperature of the truck, vital for perishable goods and some pharmaceutical products. A message will be sent to both the driver and the control centre if this is out of range so that the appropriate measures can be taken immediately.[9]

[8] Transport Asset Protection Association (TAPA) Cargo Theft Annual Report 2020 http://ace-cargadores.com/wp-content/uploads/2021/04/Boletin_1075/TAPA-EMEA-Incident-Information-Service-IIS-Cargo-Theft-Annual-Report.pdf

[9] https://www.trucknews.com/security/how-telematics-solutions-improve-the-safety-and-security-of-fleet-trucks/1003151289/



1.2 Health & Safety

There are many potential hazards and safety issues to those working in warehouses and distribution centres. Organisations have a duty of care to protect the health and safety of their employees, contractors, visitors and clients, and if something goes wrong, they may find themselves financially liable. Good security can enhance procedures to mitigate against such risks, therefore, it is important that regular security and safety risk-assessments are carried out.

Wherever possible, organisations should use, machinery (such as forklifts) to avoid manual labour-related injuries and employees should be appropriately trained to safely use all job-related equipment and machinery, which should be monitored closely. Lockout/Tagout procedures[10] should be implemented so that machinery and energy sources are shut-off properly and cannot be operated again until it is safe to do so. Correct laws and regulations should be followed when handling hazardous substances and to comply with this, it is important to implement effective procedures and ensure that all individuals are aware of, and are adequately prepared for their responsibilities.

There should be an easy reporting mechanism for any hazards identified or when incidents or near-misses occur. In the event of an emergency or incident, organisations should have a response plan which details emergency exit locations; evacuation procedures; and accounting for all those on site.

1.3 Disruption to the supply chain

Because a supply chain consists of so many elements and organisations, they are highly susceptible to security risks, both physical and cyber-related. Disruptions to supply chains not only have a significant impact on the logistics and the reputations of organisations, but also on their finances, with all the knock-on consequences that entails.[11] Therefore, operations need to have built in flexibility and resilience that can adapt in real-time to any changes which may be encountered (such as in demand or supply, trade issues, climate change, or geopolitical concerns etc.).[12] Only just over a fifth of companies have a proactive supply chain network to address these, many relying on just-in-time systems which minimise storage costs by holding as little stock as possible to meet demand. The problem with these systems is estimating the level of demand and accurate lead time figures for supply. The only way to successfully achieve this is to have a fully computerised logistics system, one that links demand and sales with re-ordering stock. However, some small business do not track their inventory and two-thirds of supply chain managers use simple systems, like Excel spreadsheets, to log stock movements.[13]

[10] Lockout/tagout is a set of safety protocols and checklists that protect workers from getting hurt by a sudden machine start-up or by releasing hazardous energy while performing maintenance activities. This prevents equipment from being accidentally energised, which can lead to employee injuries.

[11] https://procurementtactics.com/supply-chain-statistics/

[12] For further information on supply chain disruptions see: https://www.accenture.com/gb-en/insights/consulting/coronavirus-supply-chain-disruption?c=acn_gb_specialreportcogoogle_11312686&n=psgs_0920&gclid=Cj0KCQjw29CRBhCUARIsAOboZblfDQdWPnYLSRKmL_Sh19QUrakmkemryuGYGFQHXhZyDlOrGW8aCQ0aAkFrEALw_wcB

[13] https://procurementtactics.com/supply-chain-statistics/

1.4 Cyber Security

Cyber threats against warehouses and distribution centres are a significant risk and can take many forms, including hacking, data breaches, and ransomware attacks. With many buildings and sites in this sector now depending on digital operations and 'smart' technology, the effects of attacks against legacy systems could range from a mere inconvenience at say points of entry, to a full shutdown, as recently seen by KP Snacks.[14]

Within the warehouse and distribution sector, the risks of cyber-attacks on a supply chain have never been higher, with many organisations relying heavily on automated processes and large amounts of data being exchanged between those within chain. Often hackers will find an entry point into the chain by attacking the less secure elements, enabling them to gain access to the systems and data of other third-party organisations within the chain. The 2020 Solar Winds supply chain attack[15], which affected businesses and customers globally, is a recent example of the damage such attacks can inflict.

However, not all businesses appear to be addressing these risks. Although the Cyber Resilience Captains of Industry Survey 2021 identified that the majority of the UKs business bosses regarded cyber threats as high risk to their organisations, only just over two-thirds said that their organisation actively manages cyber-related supply chain risks.[16] Meanwhile attackers have more tools and resources at their disposal than ever before, and there are predictions that there could be up to four times as many cyber-attacks on supply chains in 2022 than there were in 2021.[17] It is therefore important that as levels of interconnectivity and technological changes increase, organisations work together to build effective resilience in their chains.

[14] https://www.infosecurity-magazine.com/news/kp-snacks-under-cyberattack

[15] For more information, see https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[16] https://www.gov.uk/government/publications/captains-of-industry-cyber-resilience-research-2021/cyber-resilience-captains-of-industry-survey-2021

[17] https://procurementtactics.com/supply-chain-statistics/

Intelligence is key - sign up for regular G4S threat bulletins

The G4S Academy provides regular, free security bulletins on potential threats.

(https://www.g4s.com/en-gb/what-we-do/academy/repository/activist-bulletin-archive)

They can be a useful part of your security planning.

CLICK TO SUBSCRIBE FOR FREE

1.5 Damage due to fire, flood, and adverse weather conditions

Fires in warehouses and distribution centres are not uncommon, especially as they are usually full of tightly packed goods, some of which may be combustible, meaning that the smallest of fires can spread quickly and have devastating effects. The risk is not just about product loss either, but also smoke or water damage, as well as employee injury, or even loss of life, and of course, the resultant disruption to normal business activities. This was seen in August 2020 when a night-time fire ripped through Kent Foods in Basildon destroying their warehouse.[18] One of the reasons for the extensive damage was thought to be the lack of a sprinkler system, which unlike European organisations is only required for warehouses that are over 20,000m².[19]

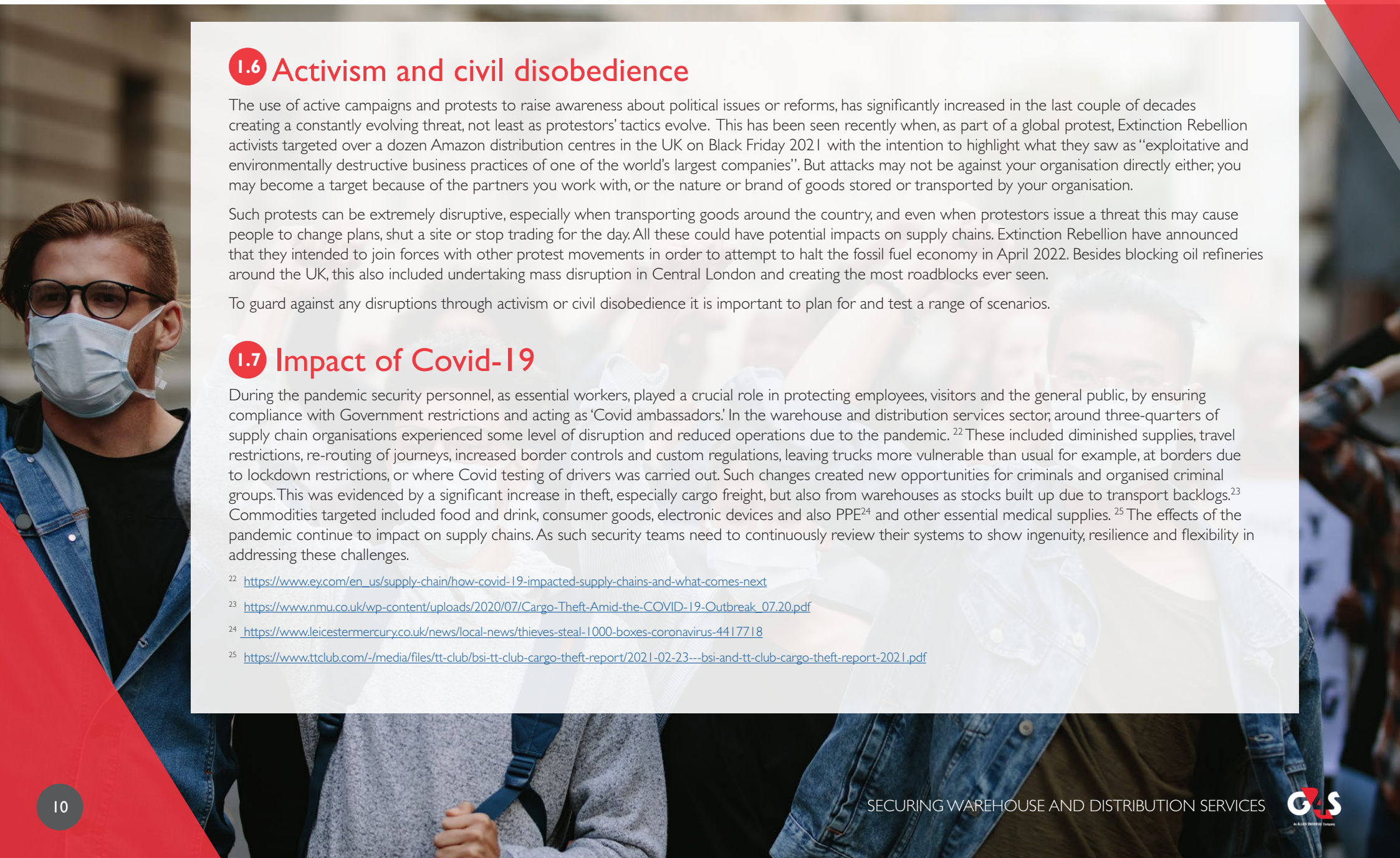
Due to the structural design of many warehouses and distribution centres (usually high walls, flat roofs and large windows), they are susceptible to damage especially with changing global weather conditions. The risk of flooding is increasing, in such cases the risk of damaging both stock and buildings are real, and at the same time disrupting daily operations.[20] Likewise, damage from high winds can be impactful, as recently seen in the UK with storms Eunice and Franklin.[21] As well as taking the appropriate traditional steps to minimise damage should such events occur, organisations should document procedures, ensure that staff are security aware and clear what to do in the case of an emergency including an evacuation.

[18] https://bakeryinfo.co.uk/manufacture/kent-foods-warehouse-destroyed-by-major-fire/647925.article

[19] https://ukfiremag.mdmpublishing.com/the-rise-of-the-warehouse-and-the-issue-of-fire-safety and https://www.zurich.co.uk/news-and-insight/fears-pandemic-led-e-commerce-boom-could-spark-rise-in-warehouse-blazes

[20] For example, see https://www.examinerlive.co.uk/news/west-yorkshire-news/couple-trapped-car-submerged-flood-23164455

[21] https://www.mylondon.news/weather/london-weather-250-people-evacuated-23144670



1.6 Activism and civil disobedience

The use of active campaigns and protests to raise awareness about political issues or reforms, has significantly increased in the last couple of decades creating a constantly evolving threat, not least as protestors' tactics evolve. This has been seen recently when, as part of a global protest, Extinction Rebellion activists targeted over a dozen Amazon distribution centres in the UK on Black Friday 2021 with the intention to highlight what they saw as "exploitative and environmentally destructive business practices of one of the world's largest companies". But attacks may not be against your organisation directly either, you may become a target because of the partners you work with, or the nature or brand of goods stored or transported by your organisation.

Such protests can be extremely disruptive, especially when transporting goods around the country, and even when protestors issue a threat this may cause people to change plans, shut a site or stop trading for the day. All these could have potential impacts on supply chains. Extinction Rebellion have announced that they intended to join forces with other protest movements in order to attempt to halt the fossil fuel economy in April 2022. Besides blocking oil refineries around the UK, this also included undertaking mass disruption in Central London and creating the most roadblocks ever seen.

To guard against any disruptions through activism or civil disobedience it is important to plan for and test a range of scenarios.

1.7 Impact of Covid-19

During the pandemic security personnel, as essential workers, played a crucial role in protecting employees, visitors and the general public, by ensuring compliance with Government restrictions and acting as 'Covid ambassadors.' In the warehouse and distribution services sector, around three-quarters of supply chain organisations experienced some level of disruption and reduced operations due to the pandemic. [22] These included diminished supplies, travel restrictions, re-routing of journeys, increased border controls and custom regulations, leaving trucks more vulnerable than usual for example, at borders due to lockdown restrictions, or where Covid testing of drivers was carried out. Such changes created new opportunities for criminals and organised criminal groups. This was evidenced by a significant increase in theft, especially cargo freight, but also from warehouses as stocks built up due to transport backlogs.[23] Commodities targeted included food and drink, consumer goods, electronic devices and also PPE[24] and other essential medical supplies. [25] The effects of the pandemic continue to impact on supply chains. As such security teams need to continuously review their systems to show ingenuity, resilience and flexibility in addressing these challenges.

[22] https://www.ey.com/en_us/supply-chain/how-covid-19-impacted-supply-chains-and-what-comes-next

[23] https://www.nmu.co.uk/wp-content/uploads/2020/07/Cargo-Theft-Amid-the-COVID-19-Outbreak_07.20.pdf

[24] https://www.leicestermercury.co.uk/news/local-news/thieves-steal-1000-boxes-coronavirus-4417718

[25] https://www.ttclub.com/-/media/files/tt-club/bsi-tt-club-cargo-theft-report/2021-02-23---bsi-and-tt-club-cargo-theft-report-2021.pdf

2 THE FUNDAMENTALS OF GOOD SECURITY

In this section we look at the key elements that need to be in place, in order to achieve good security.

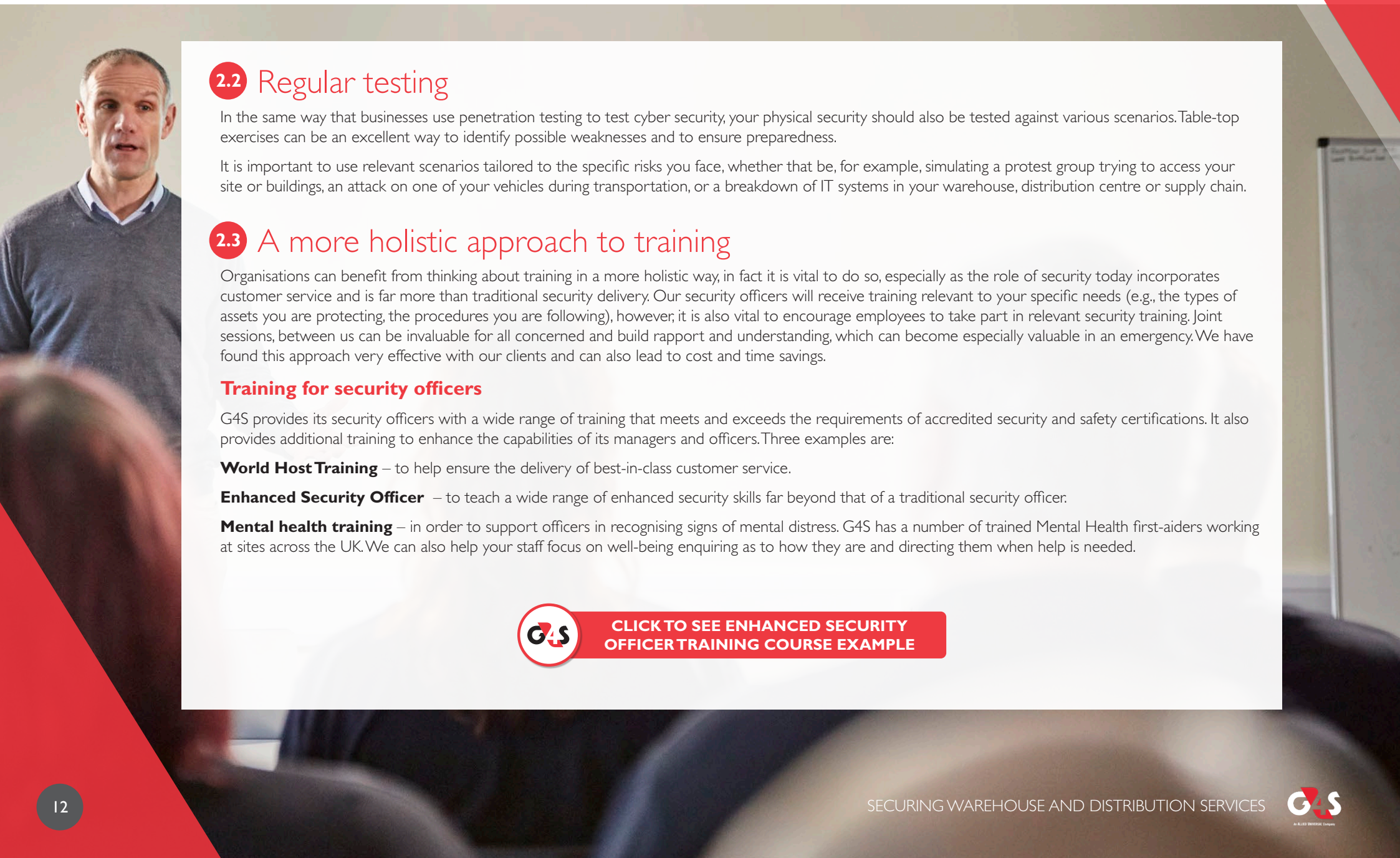
2.1 Regular risk assessment and planning

With regular risk assessment and planning being the foundation of good security, it's worth taking time to consider whether your organisational and supply chain risk assessments and plans are up to date, and whether you have a regular documented refresh plan. Have there been any changes in the assets you need to protect, be that people, property, information, or reputation? Are there any new vulnerabilities? Are your assessments incorporating the latest good intelligence – in real time - and if so, are you building these into your plan and the way you respond?

Free Risk Assessment Tool

G4S offers an online risk assessment tool, which asks a series of questions and creates a downloadable risk report, to help shape your security planning. It is ideal for those with very basic risk assessment requirements. It should take no more than five minutes to complete. G4S also offers consultative risk assessments with a G4S expert.

CLICK TO ACCESS YOUR FREE REPORT



2.2 Regular testing

In the same way that businesses use penetration testing to test cyber security, your physical security should also be tested against various scenarios. Table-top exercises can be an excellent way to identify possible weaknesses and to ensure preparedness.

It is important to use relevant scenarios tailored to the specific risks you face, whether that be, for example, simulating a protest group trying to access your site or buildings, an attack on one of your vehicles during transportation, or a breakdown of IT systems in your warehouse, distribution centre or supply chain.

2.3 A more holistic approach to training

Organisations can benefit from thinking about training in a more holistic way, in fact it is vital to do so, especially as the role of security today incorporates customer service and is far more than traditional security delivery. Our security officers will receive training relevant to your specific needs (e.g., the types of assets you are protecting, the procedures you are following), however, it is also vital to encourage employees to take part in relevant security training. Joint sessions, between us can be invaluable for all concerned and build rapport and understanding, which can become especially valuable in an emergency. We have found this approach very effective with our clients and can also lead to cost and time savings.

Training for security officers

G4S provides its security officers with a wide range of training that meets and exceeds the requirements of accredited security and safety certifications. It also provides additional training to enhance the capabilities of its managers and officers. Three examples are:

World Host Training – to help ensure the delivery of best-in-class customer service.

Enhanced Security Officer – to teach a wide range of enhanced security skills far beyond that of a traditional security officer.

Mental health training – in order to support officers in recognising signs of mental distress. G4S has a number of trained Mental Health first-aiders working at sites across the UK. We can also help your staff focus on well-being enquiring as to how they are and directing them when help is needed.

CLICK TO SEE ENHANCED SECURITY OFFICER TRAINING COURSE EXAMPLE

Training for your employees

We offer many training courses that can benefit you and your employees both for their security at work but also in their personal life. One example is our ACT online counter terrorism training for all staff working in crowded places, not just those who have a security role. It takes on average only 45 minutes to complete.

For further information (https://www.specialisttraining.g4s.com) or speak to your security provider about tailored training.

How the G4S Academy Helps

The G4S Academy helps to ensure that you receive the most up to date information and most important recommendations. Sharing specialist knowledge while supporting continuous professional development are key benefits, and registration is free.

2.4 Working in partnership

The best security solutions will be achieved where security providers and clients work closely together, whether it's the planning of an integrated security solution, or a small change in an existing plan, collaboration can help to reach the best solutions, more quickly.

As an example, working in partnership to extend the role of security from just the protection of the warehouse into supply chain transportation. This is something that G4S are actively pursuing with Yusen Logistics.

2.5 Developing a strong security culture

How would you rate your security culture? Getting this right will ensure that your employees are security-conscious and continually aware about the most effective ways of protecting your assets, including themselves. It is important to review the security culture on a regular basis, in line with changes to the threat landscape, your working practices and the technology you are deploying. Any change may have important implications for your security response.

There is guidance, useful tools and draft communications on the CPNI website here https://www.cpni.gov.uk/security-culture

In addition, we can assist you with specialist advice. We should never underestimate the power of 'hello'.

2.6 Insights, shared information and best practice

Good security utilises insights and shared information, while also using best practice from first responders.

2.7 Balancing security and customer service

In addition to providing an excellent security service, security officers working in the warehouse and distribution services sector must be proficient in customer service as often they are the first point of contact in the organisation.

G4S ensures security officers are friendly, reassuring and well-trained in communication skills with specialist courses and can be supplemented by.

2.8 Embracing new ideas and new technologies

Threats Threats on the one hand, and responses including technologies on the other are constantly evolving, and we will help you remain relevant. For example, we can supply security solutions for your delivery fleet either by providing escort services, or through the use of telematics. Our telematics employ the latest technology to ensure a continuous data flow through cameras, sensors, satellite tracking and CANBus data to our 24/7 secure operations centre. We can also provide remote monitoring of sensor measurements, such as temperature and humidity, to prevent unnecessary loss of food stuffs and other environmentally sensitive goods, enabling you to maintain the highest quality of service to your customers.

CLICK TO FIND OUT MORE ABOUT G4S TELEMATICS

2.9 Building integration in security

Security that is integrated and planned holistically, is likely to work better, precisely because it has been designed to ensure that there are no gaps to be exploited. Physical security for example is best when security professionals work in harmony with good technology, and when integrated with personnel security (protecting from the insider threat) and cyber security (protecting digital data and systems). All security needs to be integrated to maximise the opportunity to reduce risks.

CLICK TO SEE MORE ABOUT INTEGRATION SECURITY SOLUTIONS OFFERED BY G4S

3 THE FUTURE

The security world is changing in response to ever evolving threats. Those intending harm, by whatever means, are adjusting too learning to circumvent measures as soon as they are introduced, so building good intelligence and evolving practices, and integrating technologies are key. There are changes in legislation on the horizon too (see below). All this though provides opportunities not just to improve security but at the same time help evolve business goals, including those relating to sustainability.

3.1 The Impact of Covid

Above we have outlined some impacts of Covid and with it an acceleration of changes in supply chain operations, work patterns and locations that continue to evolve. Fewer workers, maybe more lone workers on warehouse and distribution sites can increase risks and require new methods of security support, meanwhile. What's more security is now asked to enforce COVID policies and protocols.

These new ways of working will require security provision to be flexible and better enabled with technology if threat actors are to be stopped from exploiting these changes. Covid is quickening the move to more sophisticated technology and systems, and we can help:

DOWNLOAD OUR COVID-19 WORK SAFELY PROGRAMME HERE

For a safe return to work - Our COVID-19 Work Safely Programme shares a set of practical guidelines and the lessons we have learned from keeping businesses running through the pandemic.

DOWNLOAD OUR G4S COVID-19 CHAMPION PROGRAMME HERE

3.2 Protect Duty

The government has published the findings of its consultation on the Protect Duty. This follows the devastating bombing at the Manchester Arena which killed 22 attendees at a concert. The plan is to introduce a legal duty on those responsible for some public places to be properly prepared for and provide protection from the danger of a terrorist attack. It is likely that the requirements will provide a basis for a more defined contribution from the private sector and a more effective partnership approach to combat terrorism. The raising of standards may have other benefits in attracting more and better recruits to a career in security.

The government has said that it is committed to bringing forward legislation this year.

You can read the full consultation findings here

G4S has already put in place many training initiatives to help ensure that its customers will meet the requirements of the proposed Protect Duty legislation, including running refresher counter-terrorism training, and providing further guidance on Public Places of Interest and hostile reconnaissance training.

Are you ready for Protect Duty?

To help ensure that you are ready for a Protect Duty, The G4S Academy have delivered an online briefing which provides an overview of what to expect from the new legislation.

DOWNLOAD OUR PROTECT DUTY ONLINE BRIEFING HERE

3.3 Social Responsibility

Corporate social responsibility (CSR) - sometimes referred to by other names such as environmental and social governance - is playing an increasingly important part in shaping how organisations deliver their services, ensuring a positive (and avoiding a negative) impact on society and taking account of environmental issues as well as economic and social ones.

This is not just about ticking boxes, but really embedding good practices in all business processes from employee recruitment to contract delivery, to support sustainability and add social value. Indeed, we have appointed a 'Head of Sustainability and Social Value' and identified four sustainability pillars: people, communities, planet and partnership which guide both our own work and that of our clients.

The focus on people includes a focus on health and well-being of staff which includes initiatives, indeed incentives, to maintain fitness (such as counting steps on patrols and providing Fitbits), providing helplines, and be engaged on mental health issues. Our pillar on communities includes, for example, encouraging and supporting volunteering such as offering local community groups security advice, or letting local businesses know about an impending event such as a protest and helping them to prepare.

The planet is increasingly important, and we can track our own carbon emissions, incentivise reduction of them by promoting and incentivising taking bikes or walking to work. We can source sustainable uniforms, use electric vehicles, and encourage our suppliers to do the same. In a different way there are a wide variety of possibilities to reduce the number of people on site like: using remote workers supported by technology, multi-skilling our frontline security staff, using dogs – which save on cost and at the same time generate environmental benefits.

Being a trusted partner is about demonstrating our commitment in not just what we do but how we interact with others and encouraging our partners, other service providers and our suppliers included, to do the same.

G4S has a board-level CSR committee that oversees these areas and has already begun supporting its clients' CSR objectives. It values diversity and proactively supports the wellbeing of its employees with various initiatives for example creating and supporting mental health ambassadors. Some other broader examples of the contributions G4S makes to this area include:

- Helping to achieve the U.N. Sustainable Development Goals through different projects worldwide
- Supporting and respecting human rights issues
- Committing to reducing the carbon footprint of buildings and vehicles
- Supporting police and crime prevention groups
- Giving paid leave for employees to participate in community projects
- Ethically sourcing uniforms and footwear
- Running a Match-it scheme that can helps employees to double the money employees raise for charity

FOR MORE DETAILS ABOUT OUR SOCIAL RESPONSIBILITY STRATEGY CLICK HERE

DOWNLOAD OUR SUSTAINABILITY REPORT 2020 HERE

3.4 Technology Led Transformation

G4S is at the forefront of the latest technology developments embracing, for example, SAAS, AI, Cloud, intelligent CCTV applications, the use of drones and robots and real time risk and threat analysis tools. Technology is powering a shift to a more proactive security model delivered at lower cost in a more environmentally friendly manner. Consumers of security expect forward thinking, innovative ways of tackling their issues.

As an example, in contrast to security teams watching hours of video from multiple camera feeds, AI now brings opportunities for the identification of unusual activity, motion detection and the automatic identification and classification of objects and individuals. It can support security personnel to identify threats and respond more quickly.

From a customer relationship perspective, it is no longer considered acceptable to leave the makeup of the security provision untouched without challenge. With large parts of warehousing and logistics fulfilling e-commerce there is a willingness to adopt technology and apply an innovative approach to security.

Therefore, a simple expectation exists that the security provider will regularly review risks and make recommendations on changes to the security design – using technology to underpin the delivery.

Often this will involve recommending technology to drive operational savings by reducing physical resources or to underpin sustainability goals by reducing energy consumption and emissions.

In some instances this may mean;

- Using increases in bandwidth to remotely control security equipment or fully monitor locations outside working hours;
- Using video analytics and contact-free access control to enable easier tenant movements
- Investing in operational technology (SMART devices) to provide a multi-tasked security officer.

The process should start by performing a detailed threat evaluation and risk assessment; we use our G4S Risk Assessment tool.

We then look at how security is currently delivered, and what the expectations are of the building occupants. A holistic solution design specialist, who has no product bias towards technology or personnel based services, should then challenge this; "Is there a better way?"

This should complete a report which illustrates a revised design, any cost-savings and associated benefits, including an illustration of the positive social value impact. This often includes a projection on the resulting carbon footprint improvement.

Staff use an approved calculator to monitor the impact of reduced travel and electricity usage on site over the course of a year. This is offset against any increased consumption to show a net saving, which is displayed for the client in a simple and easy to consume report.

READ THE ARTICLE 'HOW CAN SECURITY TRANSFORMATION IMPROVE YOUR CARBON FOOTPRINT?' HERE

READ CURTIS MCCLEMENTS ARTICLE AN EVER EVOLVING MONITORING LANDSCAPE HERE

3.5 The Connected Officer

In addition to infrastructure, technology is transforming the role of the security officer. Wearable technologies are increasingly common and the next generation of connected security officers will wear body accessories that are powered by sensors that gather information from their immediate surroundings and then relay that information for storage and analysis at the edge or in the cloud.

A simple example is a heads up display like augmented reality glasses that enable the officer to access critical data without requiring them to look away from their post. Other examples include smart clothing that can provide protection from hazards such as viruses and chemical weaponry and body-worn cameras that can continually record interactions with the public and therefore gather video evidence should the need arise.

However, despite these emerging technologies, the inter personal skills of the officer will remain critical.

READ JOE YOUNG'S ARTICLE 'CONNECTED OFFICERS TRANSFORM THE FUTURE OF SECURITY' HERE

3.6 Intelligence Underpins Delivery

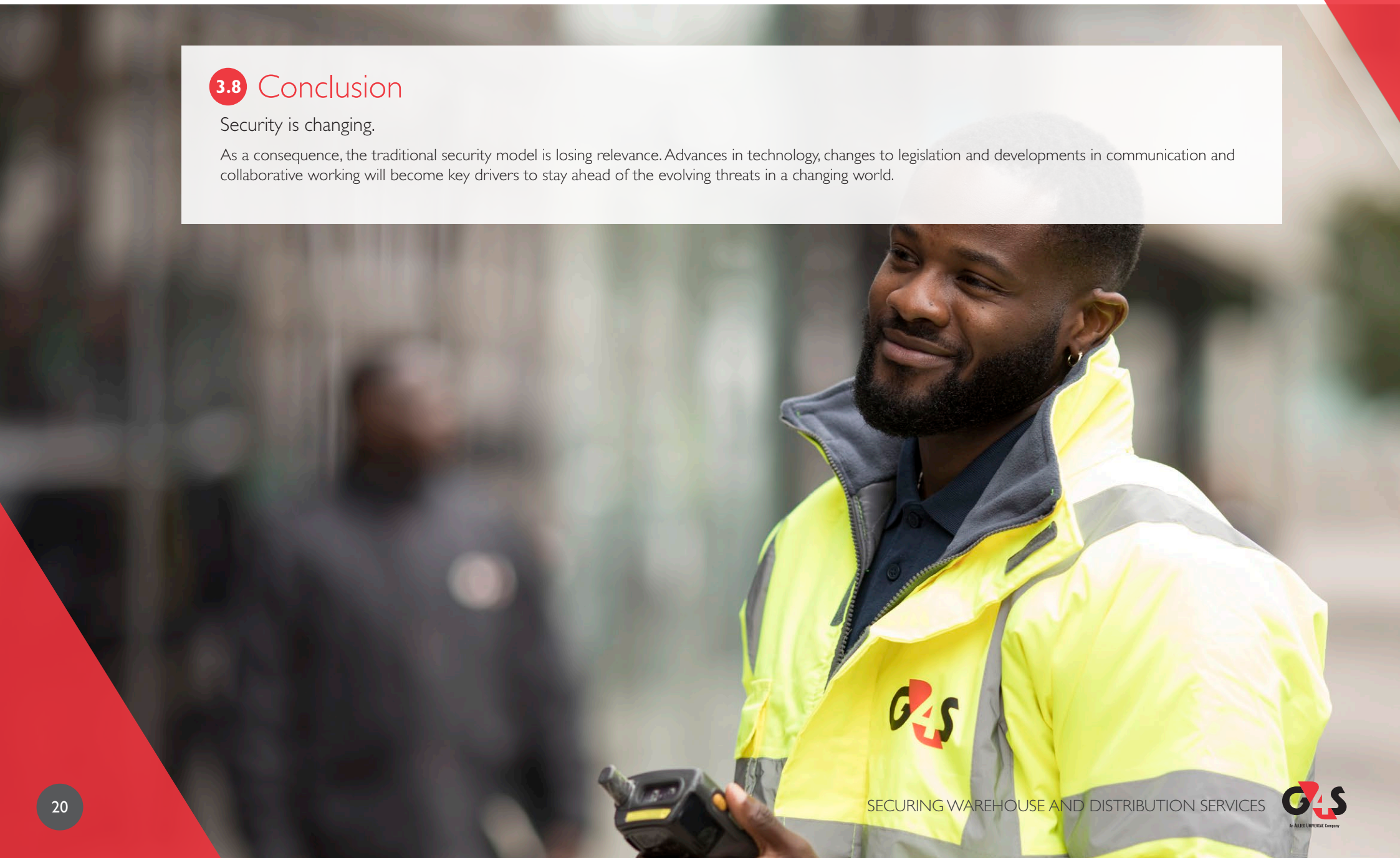
For too long security has been a reactive function. Intelligence – underpinned by technology will drive a shift to a more proactive model. Modern intelligence platforms map an organisation's assets alongside real-time risk feeds and visualise the data, giving a single view of risk.

The gathering of high-quality data and the ability to share intelligence in real-time is critical to provide meaningful metrics on specific assets, employees or business functions that may be at risk and to turn security from a reactive to a proactive service.

3.7 Real Time Performance Data

As security officers become more connected, advancements in cloud technology are allowing organisations to consolidate data in real time from various sources and make it available in simple easy to consume dashboards.

This makes the real time monitoring of contract key performance indicators a realistic proposition and will continue to provide a level of visibility that has historically been difficult to achieve.



3.8 Conclusion

Security is changing.

As a consequence, the traditional security model is losing relevance. Advances in technology, changes to legislation and developments in communication and collaborative working will become key drivers to stay ahead of the evolving threats in a changing world.

Introducing the G4S Academy

We go far beyond delivering security.

Joining the G4S Academy provides access to exclusive threat reports, thought leadership content as well as an opportunity to network with other security experts.

You will have access to:

- Regular risk bulletins, threat reports and white papers
- Event and seminar invites to hear the latest market evolution and trends
- An innovation forum which addresses emerging trends and technologies
- Podcast and webinars discussing security hot topics with leading experts

G4S Academy

CLICK TO SUBSCRIBE FOR FREE

Contact Us

UK: 08459 000 447
enquiries@uk.g4s.com

2nd Floor, Chancery House,
St. Nicholas Way,
Sutton,
Surrey,
England, SM1 1JB

Ireland: 1890 447 447
g4ssales@ie.g4s.com

G4S
An Allied Universal Company