SECURING REAL ESTATE SERVICES

G4S
An Allied Universal Company

SECURING REAL ESTATE SERVICES

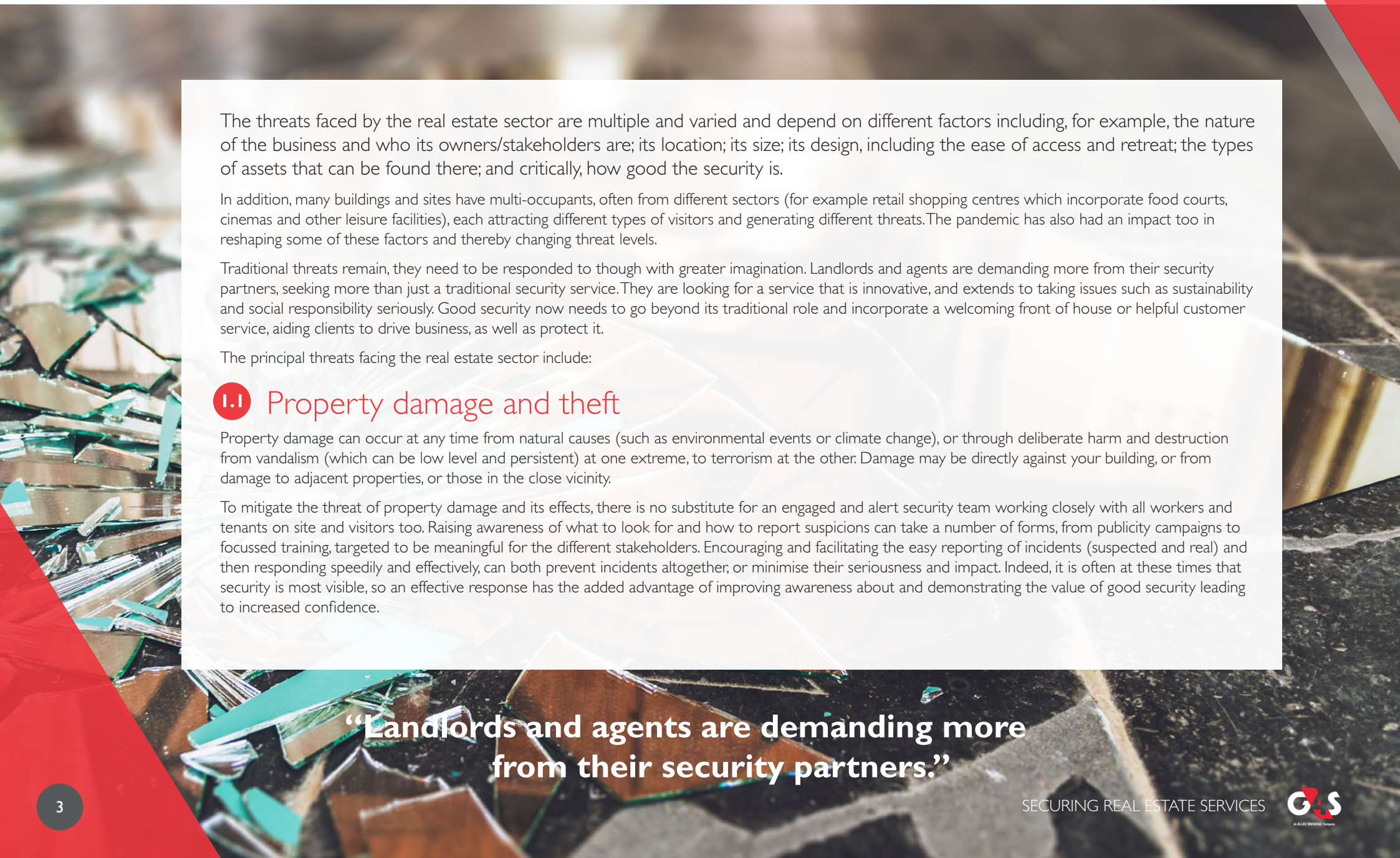
This paper outlines the key threats faced by the real estate sector (including retail, commercial, and residential buildings) today before moving on to consider the fundamentals of good security for real estate services.

This focuses protecting people, property, information and reputation, but it also involves supporting organisational goals. As you will see, this includes integrating good customer service into security; delivering technology led transformation programmes and 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, and legislation on the horizon, 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 and also takes a look at how security is evolving.

TABLE OF CONTENTS

1 THE THREATS FACING THE REAL ESTATE SECTOR



The threats faced by the real estate sector are multiple and varied and depend on different factors including, for example, the nature of the business and who its owners/stakeholders are; its location; its size; its design, including the ease of access and retreat; the types of assets that can be found there; and critically, how good the security is.

In addition, many buildings and sites have multi-occupants, often from different sectors (for example retail shopping centres which incorporate food courts, cinemas and other leisure facilities), each attracting different types of visitors and generating different threats. The pandemic has also had an impact too in reshaping some of these factors and thereby changing threat levels.

Traditional threats remain, they need to be responded to though with greater imagination. Landlords and agents are demanding more from their security partners, seeking more than just a traditional security service. They are looking for a service 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 incorporate a welcoming front of house or helpful customer service, aiding clients to drive business, as well as protect it.

The principal threats facing the real estate sector include:

1.1 Property damage and theft

Property damage can occur at any time from natural causes (such as environmental events or climate change), or through deliberate harm and destruction from vandalism (which can be low level and persistent) at one extreme, to terrorism at the other. Damage may be directly against your building, or from damage to adjacent properties, or those in the close vicinity.

To mitigate the threat of property damage and its effects, there is no substitute for an engaged and alert security team working closely with all workers and tenants on site and visitors too. Raising awareness of what to look for and how to report suspicions can take a number of forms, from publicity campaigns to focussed training, targeted to be meaningful for the different stakeholders. Encouraging and facilitating the easy reporting of incidents (suspected and real) and then responding speedily and effectively, can both prevent incidents altogether, or minimise their seriousness and impact. Indeed, it is often at these times that security is most visible, so an effective response has the added advantage of improving awareness about and demonstrating the value of good security leading to increased confidence.

“Landlords and agents are demanding more from their security partners.”

1 THE THREATS FACING THE REAL ESTATE SECTOR

Theft against real estate remains a real problem. This includes opportunist thieves exploiting security lapses, and professional thieves targeting premises known to hold valuable assets, such as computers, tablets, sound systems, and even microchips. Thieves also target employees and customers' own personal items such as bicycles, mobile phones, or staff passes. When such offences occur, they highlight weaknesses in security, for example, where individuals are able to enter and wander around buildings unchallenged. Such incidents can be embarrassing for organisations, sometimes adversely impacting on their reputation and this can be a greater loss than the theft itself.

However, not all business assets are physical, and increasingly threats against company data and intellectual property are emerging. This is not just an external threat, often it is people in buildings who commit thefts (and damage and harm). Insider threats can be particularly sinister. Experience suggests that workers with a grievance and/or who are not paid highly are often culprits. This highlights a key point, that good security is about good business practices too. Examples of insider threats include:

- **The deliberate insider –** someone who obtains employment with the intent of abusing their position and access rights
- **The self-initiated insider –** someone who joins the company without criminal intent but at some point, decides to do so
- **The exploited or recruited insider –** someone who is recruited by a third-party to obtain data or information, under situations of coercion or blackmail. They may already be in employment with the target organisation or be required to gain employment.
- **The accidental insider –** someone who might inadvertently leak information, or provide other types of access, either because they do not realise they should not do this or understand the implications of their actions. This may be due to insufficient training or a poorly defined role.

To ensure that real estate buildings are adequately protected against accidental and intentional damage, and different types of thefts, it is important to have a plan in place and adopt the appropriate security measures. This will include employing security personnel with the relevant training and experience, as well as the ability and skills to engage meaningfully with the business, to reduce risks and minimise the impact should such events occur.

An effective security presence can prevent unauthorised access to buildings and act as a visible deterrent against further crimes and other anti-social activities.

"An effective security presence can prevent unauthorised access to buildings."

1 THE THREATS FACING THE REAL ESTATE SECTOR

1.1 Vacant Premises

Vacant properties are exposed to a number of different threats and hazards that generate different risks from burst water pipes and flooding which may not be identified quickly and responded to effectively, to a range of different threat actors, all with different intentions. .To set a context, in September 2019 there were 617,527 empty buildings in the UK, of which over a quarter were commercial buildings.[1] At that time, the leading area for commercial sector vacancies was Birmingham, closely followed by Liverpool, Manchester, Leeds and Bradford.[2] The pandemic has exasperated this situation with increasing reliance on staff working from home leaving more offices unoccupied.[3] Securing vacant properties speedily and managing authorised access thereafter (for example contractors) is important. There are a number of risks.

Theft and vandalism can be commonplace in vacant properties, graffiti, broken windows, damage to furniture and fittings are amongst the most likely offences, while the theft of valuable items includes metal and cabling. Fly-tipping is also an increasing issue on vacant sites. In 2020/21 local authorities in England dealt with 1.13 million fly-tipping incidents, an increase of 16% on the previous year.[4] Not only is this illegal and a nuisance, but it can also cause a significant impact on the local environment. It can be a source of pollution which impacts on public health and wildlife not least since what is dumped can include, for example, clinical waste or asbestos. One final note of relevance here, the British Safety Council reports that up to 60 fires occur daily in or next to an empty property in the UK, and arson attacks are not uncommon.[5]

However, by far the greatest concern for real estate owners is illegal occupation of their sites, either from casual trespass; organised events (such as parties, raves, or car meets); urban explorers; to squatting or traveller settlement. Since residential squatting was made a criminal offence in 2012, this has resulted in non-residential properties being targeted more, because it is a civil offence only.[6] Owners of real estate have a legal duty of care to protect people on their sites from foreseeable harm, including those who trespass, further underlining the value of good security.

Clearly, different threats need to be responded to with appropriate security solutions, be that via the use of technology or appropriately trained and deployed security personnel. Having good reporting systems in place is a must while responses have to be effective.

[1] -https://www.todaysconveyancer.co.uk/main-news/empty-unused-buildings-increase-2019

[2] https://www.piuagency.co.uk/news-insights/the-rise-of-unoccupied-properties/#:~:text=As%20of%20September%202019%2C%20there,dwellings%20and%20172%2C217%20commercial%20buildings.&text=Closely%20followed%20by%20Birmingham%20with,)%20and%20Liverpool%20(4%2C266

[3] https://wiserd.ac.uk/sites/default/files/documents/Homeworking%20in%20the%20UK_Report_Final_3.pdf

[4] https://www.gov.uk/government/statistics/fly-tipping-in-england/fly-tipping-statistics-for-england-2020-to-2021

[5] https://www.britsafe.org/publications/safety-management-magazine/safety-management-magazine/2020/idle-and-at-risk/

[6] https://www.isurv.com/info/390/features/8454/squatting_residential_and_commercial_property

1.2 Conflict and abuse

Proactive employers will take their duty of care seriously and actively protect the health, safety and welfare of their employees, contractors, visitors and clients. This duty of care challenge can be successfully met by effective security, and undermined by bad security. Services need to be tailored. For example the guidance and support offered to those working alone, including at night, when travelling to and from the workplace, when at risk of abuse, harassment or voyeurism require a different focus. Security services are increasingly front facing with a strong focus on enhancing the customer experience. As a consequence frontline security personnel need more skills, training and support.

Engagement with people runs the risk of verbal and even physical abuse, which was especially evident during the pandemic when people were stressed and worried, and sometimes took out these feelings on security personnel. Research in 2021 found that 36% of security staff are physically attacked at least monthly and 51% are verbally abused every time they work. This has resulted in some personnel leaving the service and complicated the process of recruiting replacements. Conflict at work can have a destabilising effect on all those who are involved, including witnesses, and if handled badly can have a range of adverse (and sometimes serious) consequences. How security personnel approach and deal with potential conflict situations can greatly influence their outcome, underlining the importance of effective training and management.

1.3 Impact of Covid

During the pandemic security personnel were officially designated as essential workers highlighting the important role they played. Acting as 'Covid ambassadors', managing access and egress, enforcing social distancing requirements, ensuring the correct room and buildings capacities are understood and met, reminding employees and visitors about mask wearing, checking temperatures, managing queues and flows of (sometimes agitated) people, following PPE requirements, are all cases in point. This also took place alongside working in more sensitive areas such as test and vaccination centres, assisting at Nightingale Hospitals, or managing those quarantining in hotels, to name but a few.

In a different way, new ways of working meant cyber security, as well as physical security, was more difficult for many organisations. The Government's cyber security breaches survey of March 2021, found that, with the move to home working, employees and businesses became more vulnerable to cyber-attack (discussed further below). Working without colleagues to immediately and easy to call upon, with protection systems not originally designed for high levels of home working, and with not all working environments being conducive to secure working practices, the risks often increased considerably.

There were other challenges. The wearing of masks complicated the process of identifying individuals while making it easier for offenders to hide their identity in a legitimate way and to conduct hostile reconnaissance undetected. In these circumstances higher levels of training and vigilance are required.

Unfortunately, pandemics can reoccur, so learning and building resilience are key. Moreover, as employees return to work, following recommended Government guidelines, and fulfilling the duty of care and ensuring that staff, and visitors feel safe, welcomed and supported is key. Security is playing a vital role, adapting to change, and it is important it remains flexible and alert.

1.4 Terrorism

With the current threat to the UK from terrorism classified as 'substantial', meaning that an attack is likely, terrorism represents one of the biggest security concerns to properties in the real estate sector. Attacks may involve explosive devices being planted by unknown people, it could involve suicide bombers, or take a different form, for example and involve active shooters. Others fear that the use of more advanced technology or drones will happen at some point, and that the effects of this could be devastating.

Whatever the form, there are also concerns that the lockdowns, brought in to help control the pandemic, increased the number of radicalised, potential 'lone wolf' attackers, as people spent more time alone, online. Meanwhile, young people became more vulnerable to being groomed by extremists. Recent Home Office figures have shown an increase in the number of children being detained over terror crimes.[7] There is also evidence that far-right groups have been trying to recruit anti-vaxxers on messaging platform chat rooms.[8] Experts fear that the far right and anti-vaccine movements could result in individuals carrying out terror attacks after being radicalised by talk of martyrdom, taking up arms, and executions. For more on Covid related activists see page 8.

While attacks could occur at any location, the most vulnerable are those highly populated buildings/areas, while specific targets may include financial, social, political and religious institutions, as well as iconic landmarks. Prevention is key, and very possible. For example, since the start of the pandemic, seven late-stage terror attacks have been stopped in the UK by the Counter Terrorism Policing (CTP) and the UK Intelligence Services, bringing the total number of foiled terrorist plots in the last five years to 32[9]. These will often have been foiled by alert people noticing and then reporting something unusual or suspicious. It is vital that all staff, visitors too, and especially security personnel, are trained and can undertake this work effectively. Businesses need to be aware how terrorist attacks could be undertaken, including the danger of being supported by an insider, and need to keep abreast of the changing threat level and adjust their security approach accordingly. Therefore, they should have in place preparedness strategies, as well as evacuation procedures should an emergency occur.

[7] https://www.gov.uk/government/statistics/operation-of-police-powers-under-the-terrorism-act-2000-quarterly-update-to-june-2021

[8] https://www.thetimes.co.uk/article/covid-antivaxers-recruited-far-right-apps-euro-2020-racism-73b96j27b

[9] https://www.counterterrorism.police.uk/latest-home-office-statistics-reveal-7-late-stage-plots-foiled-since-march-2020/

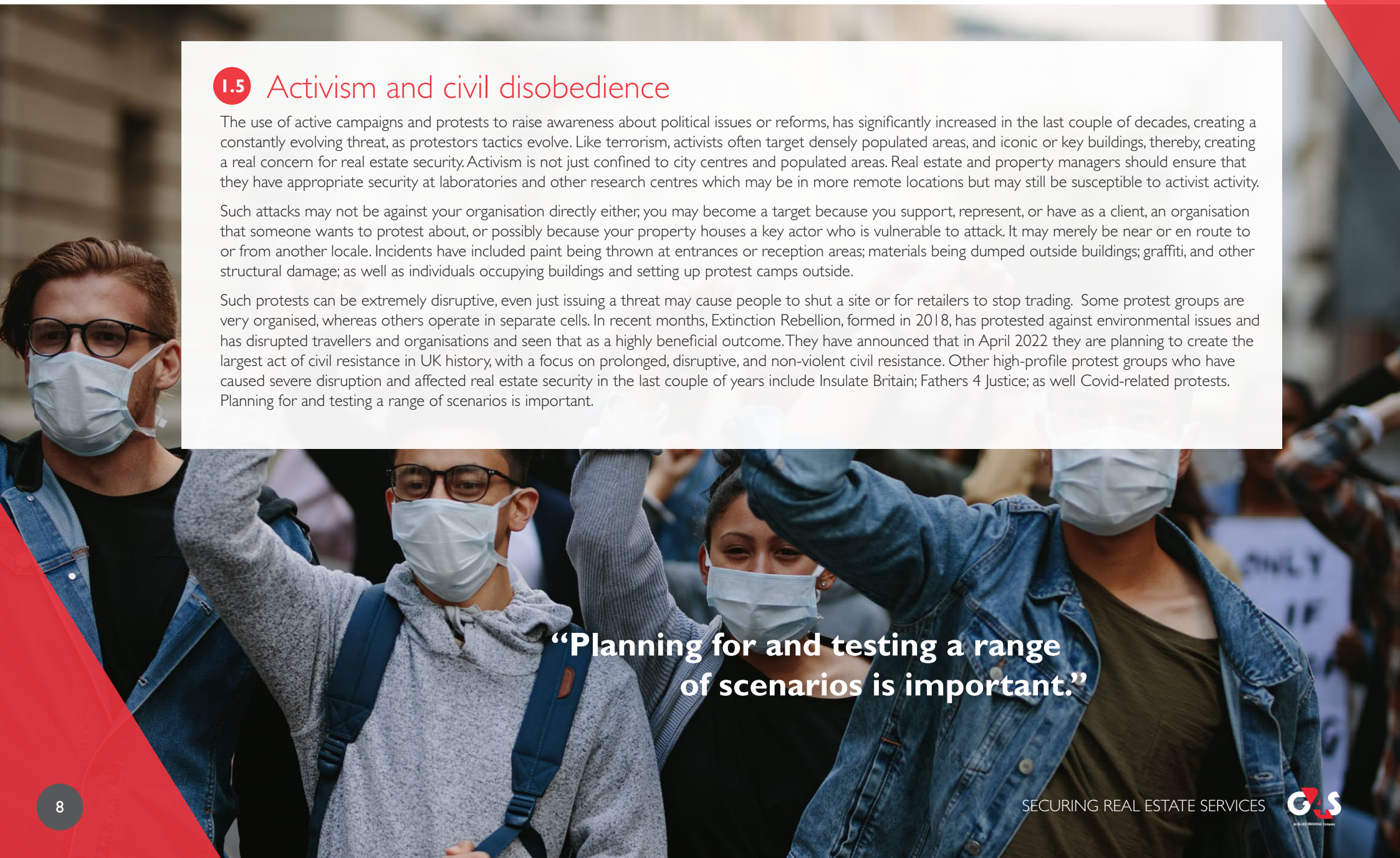
"terrorism represents one of the biggest security concerns to properties in the real estate sector."

1.5 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, as protestors tactics evolve. Like terrorism, activists often target densely populated areas, and iconic or key buildings, thereby, creating a real concern for real estate security. Activism is not just confined to city centres and populated areas. Real estate and property managers should ensure that they have appropriate security at laboratories and other research centres which may be in more remote locations but may still be susceptible to activist activity.

Such attacks may not be against your organisation directly either, you may become a target because you support, represent, or have as a client, an organisation that someone wants to protest about, or possibly because your property houses a key actor who is vulnerable to attack. It may merely be near or en route to or from another locale. Incidents have included paint being thrown at entrances or reception areas; materials being dumped outside buildings; graffiti, and other structural damage; as well as individuals occupying buildings and setting up protest camps outside.

Such protests can be extremely disruptive, even just issuing a threat may cause people to shut a site or for retailers to stop trading. Some protest groups are very organised, whereas others operate in separate cells. In recent months, Extinction Rebellion, formed in 2018, has protested against environmental issues and has disrupted travellers and organisations and seen that as a highly beneficial outcome. They have announced that in April 2022 they are planning to create the largest act of civil resistance in UK history, with a focus on prolonged, disruptive, and non-violent civil resistance. Other high-profile protest groups who have caused severe disruption and affected real estate security in the last couple of years include Insulate Britain; Fathers 4 Justice; as well Covid-related protests. Planning for and testing a range of scenarios is important.



“Planning for and testing a range of scenarios is important.”

1.6 Cyber security

As noted above, cyber threats are of particular concern in the real estate sector and these can take different forms including hacking, data breaches, and ransomware attacks. With many properties now relying 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.[10] Vulnerability is increased where commercial buildings have multiple occupancy, with interconnectivity and interdependent IT systems, that involve third parties.

Information on work systems that is illegally accessed and leaked can cause acute embarrassment and adversely impact on an organisation's reputation. The UK Government's Cyber Security Breaches Survey 2021 identified that 39% of businesses reported cyber security breaches or attacks in the previous 12 months, with 21% losing either money or data, with an average cost of £8,460.[11] But costs are not just direct, often loss of reputation can be far more damaging to a business, as seen in recent data breaches by Facebook, LinkedIn, Volkswagen and Audi, Amazon and British Airways, to name but a few. Organisations need to guard against staff behaving illegally or even with neglect; as noted, the insider threat is a very real one. That almost a quarter (24%) of employees in the UK say they plan to move jobs within the next three to six months, as part of the 'great resignation',[12] fuels the need for a focus on cyber security.

1.7 Responding to ad-hoc threats

Organisations cannot plan for everything, but when unforeseen events occur, security is typically a 'first responder' to a wide range of issues and incidents, such as a medical emergency, suicide threat, gas leak or active fire alarm. Because security plays such a key role in these unexpected situations, it is important for organisations to find a security partner who is observant, proactive and takes pride in supporting their clients.

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

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

[12] https://www.randstad.co.uk/about-us/industry-insight/great-resignation/

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

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 organisation's 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, information, reputation or changes to your real estate portfolio? 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 be tested against various scenarios. Table-top exercises can be an excellent way to identify possible weaknesses and to be prepared. It is important to use relevant scenarios tailored to the specific risks you face, whether that be, for example, simulating an urban explorer incident, a terrorist attack, or a protest group trying to access the building.

Regular testing and practising of scenarios builds up active resilience - at G4S we have even run bespoke "tabletop exercises" for our clients. These provide practical incident simulation and put skills to the test

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. This is especially important in the real estate sector, where the security force is often seen as an extension to the real estate provider. 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

A number of free courses are available that could benefit you and your employees both for their security at work but also in their personal life. One example is the 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.

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.

CLICK TO SUBSCRIBE FOR FREE

2.4 Working in partnerhip

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.

The partnership between G4S and JLL (one of the world's largest property management companies) has transformed the approach to security, through embedding technology and challenging existing personnel procedures. This has resulted in delivering security solutions in a more innovative, efficient, cost-effective, and sustainable way.

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.

Sharing information and resources

G4S is proud to be a member of The City Security Council, originally a collaborative partnership between City based security companies and the City of London Police, but now developing a broader remit. Its aim is to explore ways to improve collective responses to threats from terrorism, or another crisis or emergency. Plans by the Home Office, via the Joint Security and Resilience Centre, means we will likely see more of the public domain being 'policed' by private security companies. Moreover, 2022 will see the launch of a new communication and incident management platform that will facilitate real-time reporting into and out of the City of London Police via a new Joint Contact and Control Room. As well as real time reporting of incidents such as missing persons, suspicious vehicles and change of security alerts, it will provide the police with the ability to galvanise support from security companies to help quickly set up cordons or support mass evacuations.

In addition, the Home Office in collaboration with the National Counter Terrorism Security Office (NaCTSO) and Pool Reinsurance is planning to launch (in 2022) a new interactive online platform to provide a central digital location for advice, guidance, e-learning and other helpful content.

Best Practice

G4S incorporates practices developed as part of The Joint Emergency Services Interoperability Programme (JESIP) which was developed to improve and standardise the way the police, fire and rescue and ambulance services work together when responding to major incidents. Its principles include creating shared situational awareness using M/ETHANE[15], as the recognised common model for passing incident information between services and their control rooms.

[15] ETHANE stands for Exact location; Type; Hazard; Access; Numbers; Emergency Services. An 'M' is added for a major incident.

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

2.7 Balancing security and customer service

Above it was noted that in addition to providing an excellent security service, security officers working in the real estate sector must be proficient in customer service. G4S ensures security officers are friendly, reassuring and well-trained in communication skills with specialist courses. This can be supplemented by technology and not just for security. For example, we can also supply concierge staff with appropriate technology to optimise the check-in experience.

Taking customer service a stage further, as we have with other clients, G4S can provide staff in an award-winning hybrid receptionist and security role, which can not only save on costs and improve security, it results in an outstanding front of house experience for staff and visitors alike. These 'ambassadors' are mobile rather than static, use portable IT equipment, and better enable staff to both welcome visitors and assist them while fulfilling their security duties. In this way, security can become an integral part of the property management organisations' service proposition.

2.8 Embracing new ideas and new technologies

Threats on the one hand, and responses including technologies on the other, are constantly evolving and we will help you remain relevant. For example, lone worker devices enable your staff working remotely to be in permanent contact with our security centre. We can also provide hand held devices that perform tasks that previously required officers to be sitting in a control room - thus greatly enhancing the security service on the frontline.

Developments in access control, including biometrics and facial recognition can also deliver better and frictionless security which can be especially important in the post COVID environment.

For more on the future of technology in security see page 18.

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 to learning to circumvent measures as soon as they are introduced, so building good intelligence, 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 work patterns and locations that continue to evolve. Fewer workers, and maybe more lone workers on site, can increase risks and require new methods of security support. Meanwhile, the security requirements of employees working from home are evolving too. The future may see more blended arrangements, with employees in the office for fewer but longer days to maximise their time with colleagues. Buildings may accommodate a larger number of businesses. Sometimes the same office space will be used by different companies on different days.

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

With many real estate operators providing services in public spaces such as retail parks, they are likely to be heavily impacted by this legislaton. 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. At G4S, we've 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 the health and well-being of staff which includes initiatives, to maintain fitness (such as counting steps on patrols and providing Fitbits), providing helplines, and engagement 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.

Action to tackle climate change 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.

In addition, we deliver environmental performance improvements through our contracts by adopting technology where possible to reduce unnecessary travel and energy consumption, without increasing risk.

Finally, 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. For major managed service contracts - commonplace amongst providers of property management services - there is a simple expectation 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.

The G4S paper 'How can Security Transformation Improve Your Carbon Footprint?' provides more detailed information and demonstrates how improvements should be quantified.

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

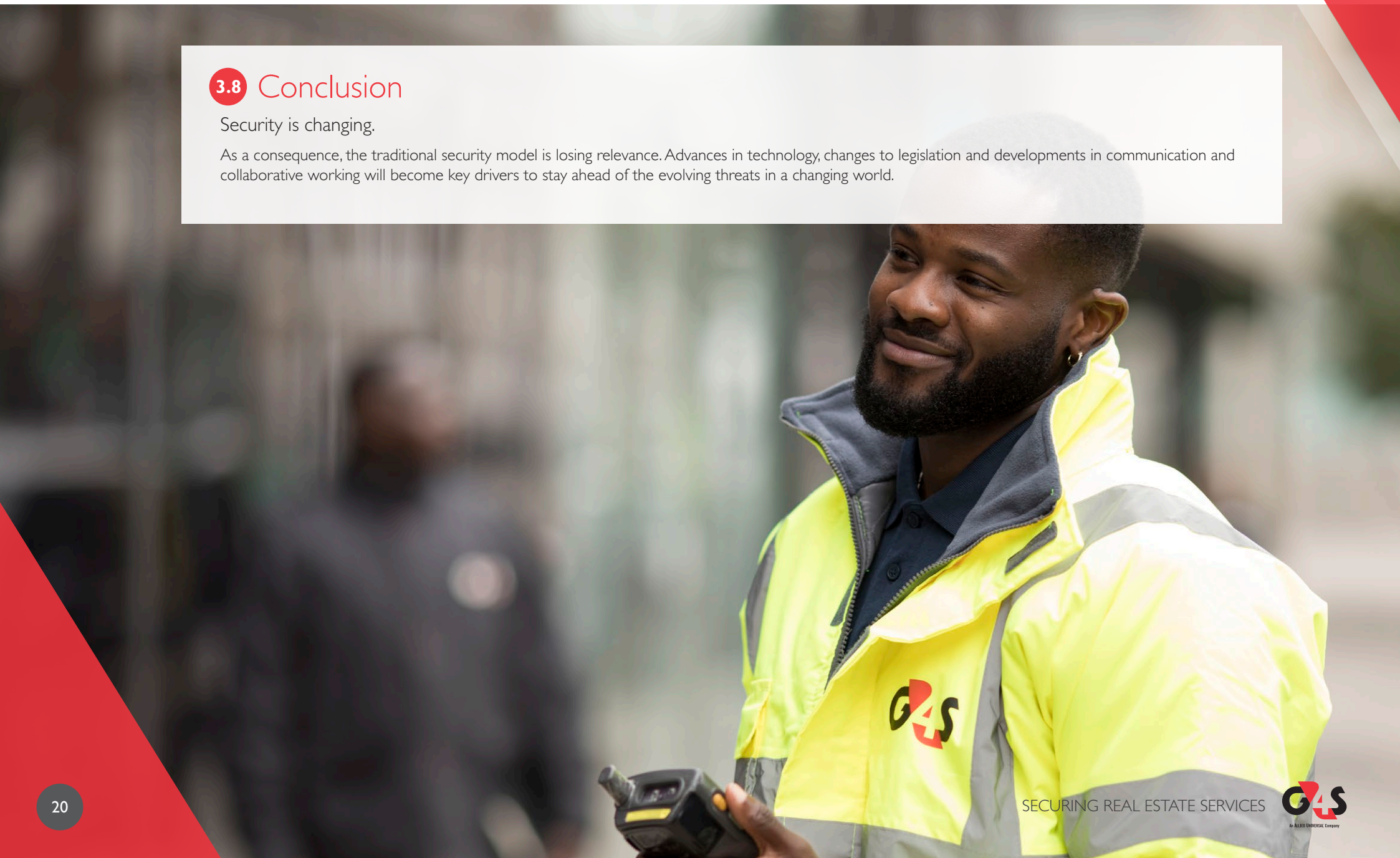
As security officers become more connected, advancements in cloud technology are allowing organisations to consolidate data in real time from various sources and make it available in simple easy to consume dashboards.

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