SECURING CRITICAL NATIONAL INFRASTRUCTURE

G4S
An Allied Universal Company

CONTENTS

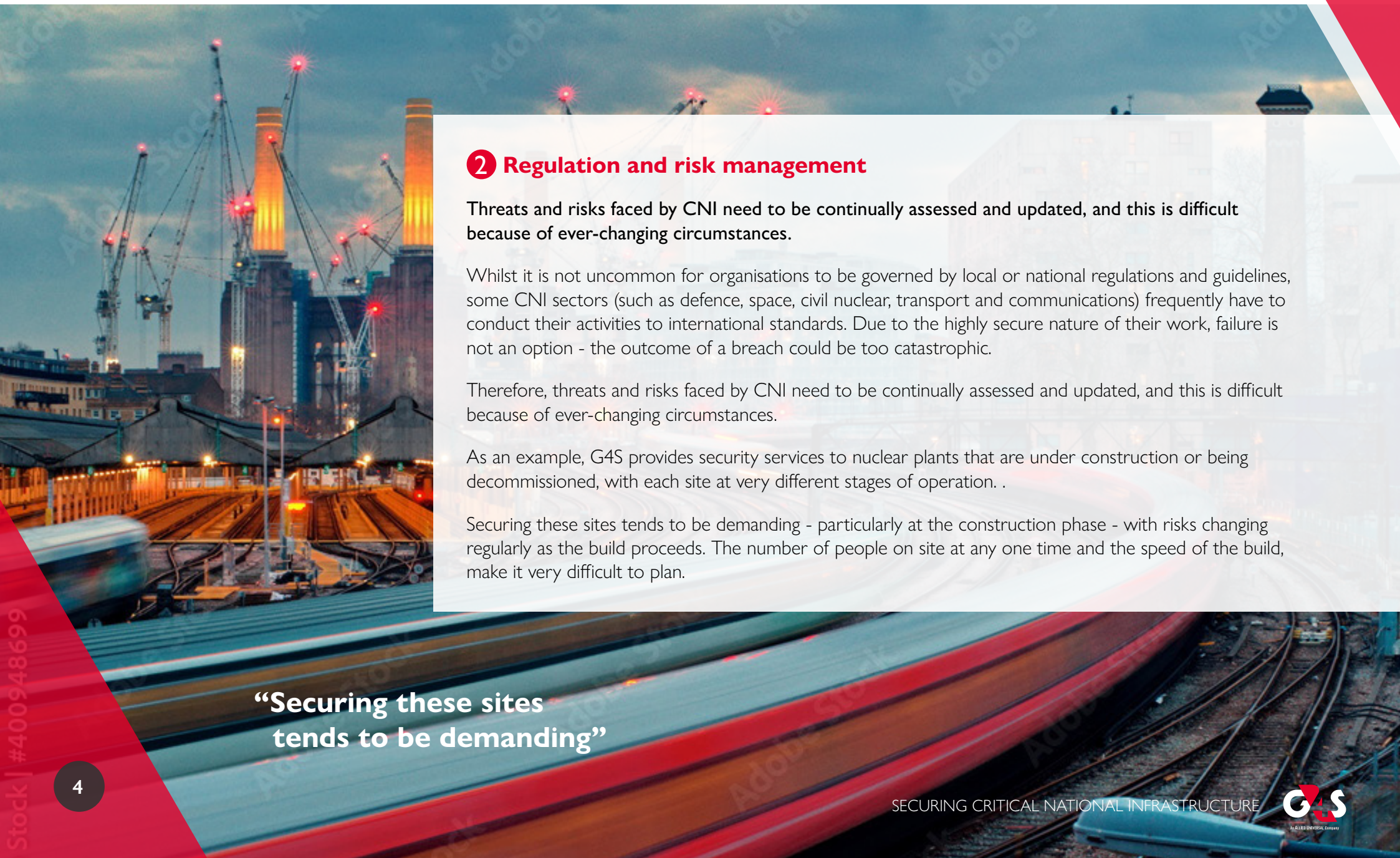
1 Introduction

Critical national infrastructure (CNI) is, by its very nature, fundamental to the running of any country. Without the contribution from sectors such as energy, water, finance, communications, transport and health etc, society would be severely impacted. It should therefore be no surprise that CNI is a perfect target for those who may wish to cause major disruption or harm.

Threats against CNI may be external or come from the inside and are constantly evolving. The principal threats against CNI include theft or damage to property, assets and materials, unauthorised entry (including terrorist, activist and urban exploration) and cyber attacks.

The infrastructure which supports and underpins these sectors therefore needs to be protected against threat and harm, using modern methods and the latest technology, to ensure that critical operations are not disrupted should an attack occur. Such arrangements need a holistic approach to protect the entire infrastructure, including both physical and cyber security, and ensuring that culture, awareness and behaviour among staff, contractors and others, is ultimately driven from the top.

"(CNI) is fundamental to the running of any country"



2 Regulation and risk management

Threats and risks faced by CNI need to be continually assessed and updated, and this is difficult because of ever-changing circumstances.

Whilst it is not uncommon for organisations to be governed by local or national regulations and guidelines, some CNI sectors (such as defence, space, civil nuclear, transport and communications) frequently have to conduct their activities to international standards. Due to the highly secure nature of their work, failure is not an option - the outcome of a breach could be too catastrophic.

Therefore, threats and risks faced by CNI need to be continually assessed and updated, and this is difficult because of ever-changing circumstances.

As an example, G4S provides security services to nuclear plants that are under construction or being decommissioned, with each site at very different stages of operation. .

Securing these sites tends to be demanding - particularly at the construction phase - with risks changing regularly as the build proceeds. The number of people on site at any one time and the speed of the build, make it very difficult to plan.

“Securing these sites tends to be demanding”

2 Regulation and risk management

Revisions of the UK threat levels relating to potential terrorist attacks also have an impact, with an expectation that security services have the ability to react to these changes instantly. This means having the resources to upscale security to the appropriate level at short notice with suitably qualified personnel for the individual CNI environment.

Having access to a pool of Suitably Qualified and Experienced Personnel (SQEP), plus a broad range of supporting services (such as canine, which can screen for explosives and firearms etc.), as well as being able to rapidly deploy surveillance technology (such as CCTV Towers), allows organisations such as G4S to effectively react to such demands and build an integrated security solution suitable to mitigate the threat.

"... having the resources to upscale security to the appropriate level at short notice."

“All CNI sites take a layered protection approach to security”

3 Managing ingress and egress

All CNI sites take a layered protection approach to security, with security checks kicking in before the perimeter for people, equipment and goods.

However, this is frequently not as simple as securing one area, because many sites have multiple entry points, especially larger plants that may have connections via road, rail and ports. It is important that only authorised personnel are admitted to site and that they are adequately screened, without causing any unnecessary delays. This can be a real challenge when high volumes of people enter the site at short notice.

4 Achieving the standards

To achieve the required standards in CNI environments it is important to adopt intelligent security, using a risk-based approach, backed by specialist people and approved products. Personnel in design, installation and operations need to be suitably and highly qualified to carry out their roles. Many of these sites are visited by high-profile individuals, making them a target for terrorist activity and regularly selected by protesters. They are also a popular choice for urban exploration. For these reasons G4S uses enhanced security officers (ESOs) on its high-risk sites, who can undertake a skilled and informed approach to appease any hostile situations. ESOs are highly experienced (often with ex-military backgrounds) in the de-escalation of hostile situations such as protests.

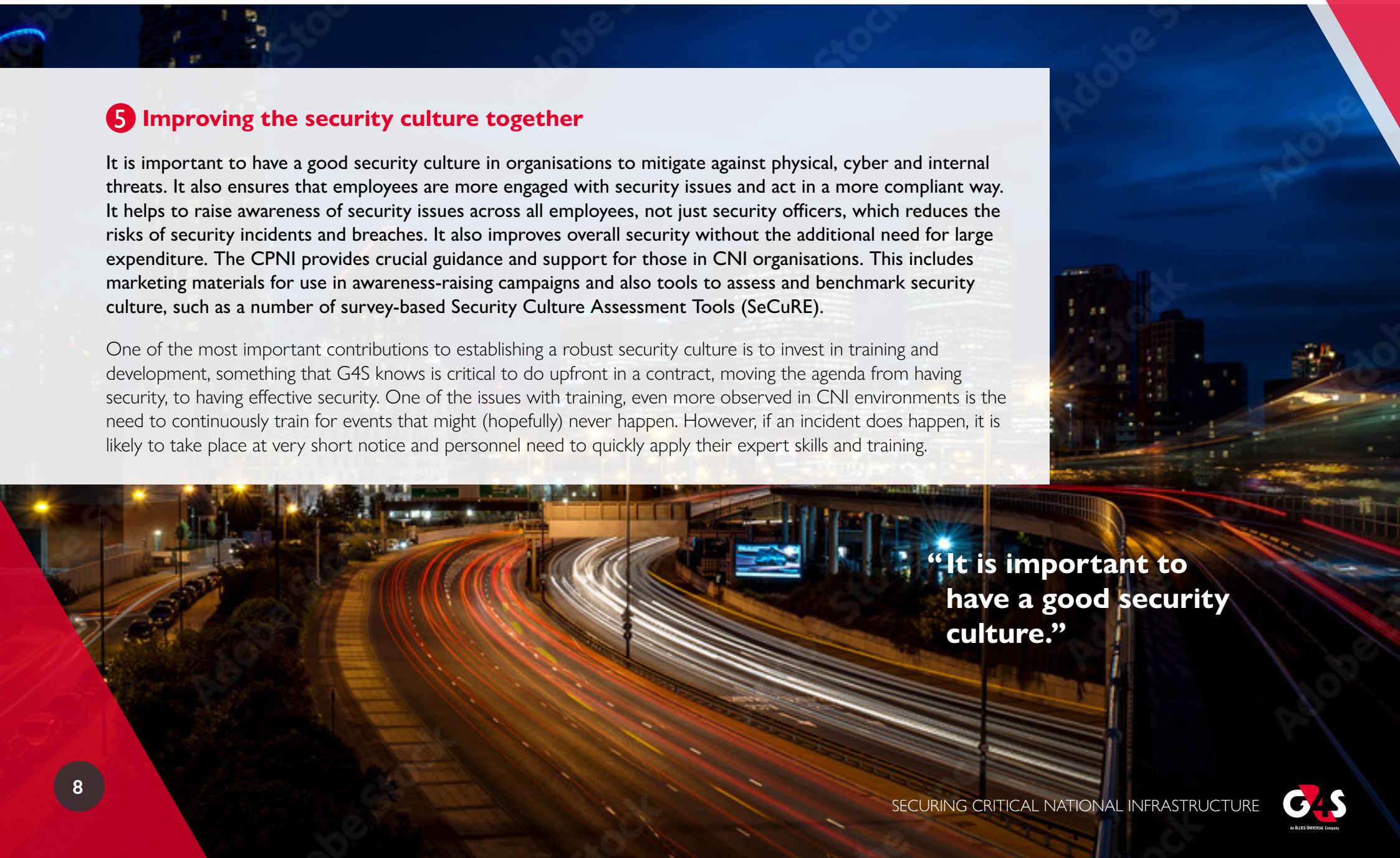
Likewise, only the highest standard of equipment and technology can be employed because external and insider threats are a real risk given the sensitive nature of the work undertaken at some locations. The Centre for the Protection of National Infrastructure (CPNI) is the government authority focussed on providing advice and assistance to those who have responsibility for protecting these most crucial elements of the UK's national infrastructure, and to reduce their vulnerability to terrorism and other security threats.

CPNI evaluates security products for use in CNI and Government, against specific CPNI security standards to assist organisations to identify the most appropriate physical security equipment. A product may be given a 'Class' level grading, meaning it has characteristics that will defend against surreptitious attacks, or a 'Protection' level, meaning it shows resistance to forced attacks. Occasionally, a product will be awarded both grades. The CPNI evaluations are set well above the standard expected of a 'normal' security product, even the 'lowest' grading is an indication of a very capable product.

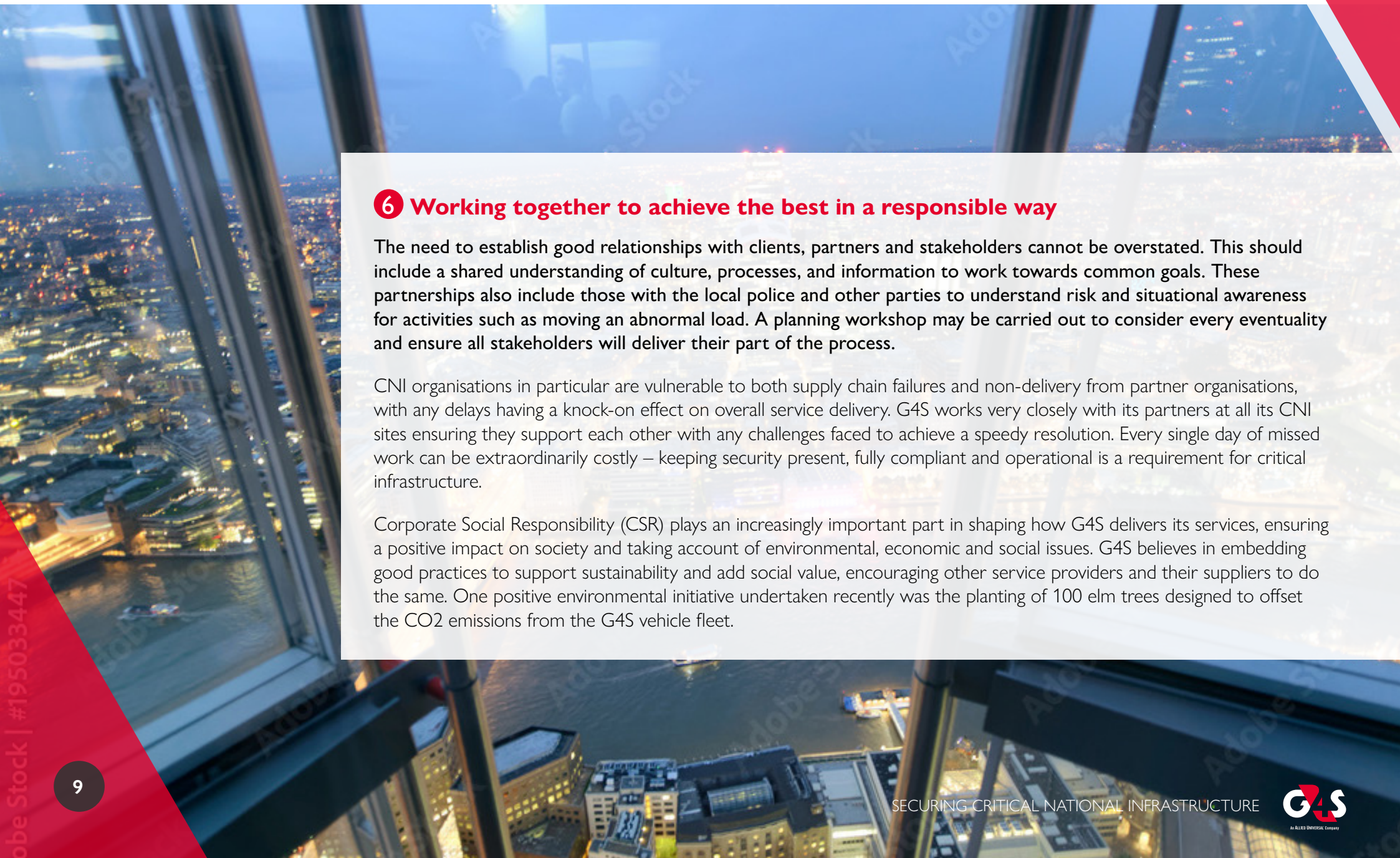
5 Improving the security culture together

It is important to have a good security culture in organisations to mitigate against physical, cyber and internal threats. It also ensures that employees are more engaged with security issues and act in a more compliant way. It helps to raise awareness of security issues across all employees, not just security officers, which reduces the risks of security incidents and breaches. It also improves overall security without the additional need for large expenditure. The CPNI provides crucial guidance and support for those in CNI organisations. This includes marketing materials for use in awareness-raising campaigns and also tools to assess and benchmark security culture, such as a number of survey-based Security Culture Assessment Tools (SeCuRE).

One of the most important contributions to establishing a robust security culture is to invest in training and development, something that G4S knows is critical to do upfront in a contract, moving the agenda from having security, to having effective security. One of the issues with training, even more observed in CNI environments is the need to continuously train for events that might (hopefully) never happen. However, if an incident does happen, it is likely to take place at very short notice and personnel need to quickly apply their expert skills and training.



"It is important to have a good security culture."



6 Working together to achieve the best in a responsible way

The need to establish good relationships with clients, partners and stakeholders cannot be overstated. This should include a shared understanding of culture, processes, and information to work towards common goals. These partnerships also include those with the local police and other parties to understand risk and situational awareness for activities such as moving an abnormal load. A planning workshop may be carried out to consider every eventuality and ensure all stakeholders will deliver their part of the process.

CNI organisations in particular are vulnerable to both supply chain failures and non-delivery from partner organisations, with any delays having a knock-on effect on overall service delivery. G4S works very closely with its partners at all its CNI sites ensuring they support each other with any challenges faced to achieve a speedy resolution. Every single day of missed work can be extraordinarily costly – keeping security present, fully compliant and operational is a requirement for critical infrastructure.

Corporate Social Responsibility (CSR) plays an increasingly important part in shaping how G4S delivers its services, ensuring a positive impact on society and taking account of environmental, economic and social issues. G4S believes in embedding good practices to support sustainability and add social value, encouraging other service providers and their suppliers to do the same. One positive environmental initiative undertaken recently was the planting of 100 elm trees designed to offset the CO2 emissions from the G4S vehicle fleet.

We'll go far beyond simple security delivery.

Our G4S Academy is open to all those that operate in the security industry and provides a unique opportunity for networking, CPD and a constant stream of intelligence - such as our weekly threat intelligence report.

Our G4S Academy providing a monthly security bulletin on potential as well as a repository of white papers, webinars and other continuous professional development material

Our Events and Seminars where guest speakers debate the latest market evolution and trends

Our Innovation Forum where we work closely with our customers to discus new security issues and how best to address emerging trends and technologies

Our Podcasts where we support continuous professional development through engaging debate - available at your leisure

G4S Academy

Listen to Noah's introduction and subscribe with our G4S Academy at https://www.g4s.com/en-gb/what-we-do/academy

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

An Allied Universal Company