# Physical security: protecting your business

Frazer-Nash Consultancy delivers security services to public and private sector clients, including critical national infrastructure (CNI).

OUR APPROACH: DELIVERING VALUE

In a world increasingly connected in cyberspace, and where the insider threat poses significant risk, we don't believe that physical security should be considered in isolation of cyber and human factors.
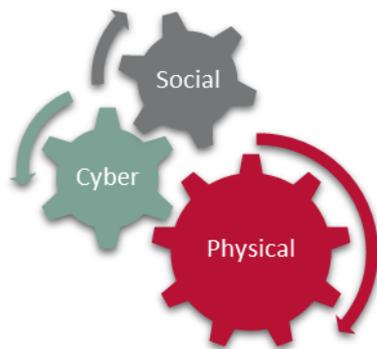
Blended solutions

The modern adversary does not distinguish between the physical, cyber and social domains – where perpetrators are increasingly using a range of tactics to achieve their aims.

At Frazer-Nash, we address the challenges posed by the 'blended threat' by adopting an approach that delivers bespoke, effective, and comprehensive protective security solutions. Our services help to:

- align security to business objectives
- define and effectively manage risk
- facilitate regulatory compliance
- measure performance and achieve continuous improvement
- build an effective security culture
- realise operational and capital expenditure efficiencies
- safeguard reputation
- protect business growth

WE UNDERSTAND YOUR CHALLENGES

The range and severity of today's security risks to business are unprecedented. Terrorism grabs the headlines, and security staff also have to manage threats from cybercrime, industrial espionage, fraud, organised crime, extremism and the insider.

Our clients face significant internal challenges too. These include understanding the risks they face; defining the enterprise risk appetite; developing a healthy and effective security culture; and meeting their regulatory obligations –

whilst gaining Board level support, and implementing an effective Security Management System (SeMS).

OUR SERVICES

At Frazer-Nash, we tailor our Blended Security Services, to provide cost effective solutions.

Security risk management

We help our clients to better understand their security risks, through comprehensive analysis of a broad range of threats; enterprise and asset characterisation; identification of vulnerabilities; and an estimation of the impact of malicious events. We use qualitative and quantitative techniques, where risks are prioritised and cost effective controls recommended.

Design basis threat (DBT)

We have extensive experience of working with DBT, to inform a broad range of risk analysis work. DBT is a proscriptive approach to the threat, where adversary capabilities are characterised in some detail and inform subsequent risk estimation and treatment.

DBT ensures all users are applying a similar standard of threat to different assets and locations, as appropriate. It can also help clients better define their risk appetite and provides a single standard which can be measured against, during drills, exercises and audits.

We help clients interpret DBT imposed in their sector or to formulate their own bespoke DBT, to support their security risk management process.

Blended security penetration testing

Your business is vulnerable to credible physical, cyber and social domain threats. A traditional 'silo' approach to counter these threats will not provide adequate protection. Threats should not be considered individually or in isolation but rather as a whole.

Working with our sister company Context Information Security, we provide a bespoke test exercise regime that blends the physical, social and technical penetration testing aspects, to provide a comprehensive stress test of your security arrangements.

Typical tasks include:

- open source internet profiling and hostile reconnaissance
- development of realistic threat scenarios
- identifying asset vulnerability and critical activities
- a study of staff vigilance and 'challenge culture'

A comprehensive debrief and after action report will include evidence, in multi-media form, to support both decisions around security improvements and the development of powerful messaging for staff internal security awareness training.

Insider Threat Management Programme

A malicious employee or contractor, with privileged access, could cause your business considerable harm; it is not surprising that this is a priority concern for security

---

FRAZER-NASH
CONSULTANCY

professionals. Drawing on our security and human factors expertise, we can work with you to develop a comprehensive Insider Threat Management Programme – to reduce the risk of a deliberate or unintentional malign insider.

Our behavioural analysis approach complements established risk management tools, including screening, vetting, aftercare, training, network and end point monitoring.

Security strategy policy, plans and procedures

Every security business unit needs direction, goals and a framework within which to operate; our consultants can help you produce, and implement your security strategy, policy, plans and procedures to achieve this.

Recent work has included developing site security plans, counter terrorism emergency response, and enhancing crisis management arrangements.

Secure by design

Designing in security retrospectively can be expensive and inefficient. Our consultants can help you design novel and holistic protective security solutions; from early stage concepts, level 1 and 2 operational requirements, through to security design engineering solutions.

Early involvement of security engineering specialists in any design project ensures security aspects are fully integrated, sympathetic, commensurate with the threat and cost effective.

We also offer blast, ballistic impact and hostile vehicle mitigation design, with structural response analysis, to inform the design stage or analyse an existing structure's resilience to attack.

Security management systems (SeMS)

Many organisations enjoy the benefits of efficient safety, environment and quality management systems. We can help you realise similar added value through implementation and refinement of a SeMS; including application of performance metrics to support continuous improvement.

We have contributed at a national level to the development of the SeMS concept and are leaders in this field.

Assurance and compliance

Many of our clients face significant security compliance challenges, in heavily regulated industries. These challenges include a move towards 'outcomes-based' regulation and an increasing emphasis on entities developing their own internal assurance capability.

We understand this environment; our consultants include former CNI regulators, who can help you meet your regulatory requirements and to evolve your own internal assurance process. We also offer second and third party security assurance inspections and audits, where recent demand has been focused on our clients' supply chain.

Training design, exercises and drills

Are you struggling to identify what constitutes suitably qualified and experienced for your security staff? Employees need to be kept up to date with organisational and operational changes, malicious attacks, security audits, legislative change, and ongoing training obligations. We offer a systematic approach to training needs analysis, leading to effective and efficient training design and pragmatic delivery solutions. Our consultants will pass on their experience in delivering and assessing niche security, emergency response and crisis management exercises and drills, in highly regulated and safety conscious environments.

3D security design and simulation software modelling

In partnership with the UK's National Nuclear Laboratory, we offer a software modelling and simulation capability – to evaluate the adversary threat against a defined physical protection system, and measure the effectiveness of the response force.

It also provides an overall graphical and statistical assessment of security system effectiveness and visualisation of tactics, variants, and outcomes, with supporting analysis information for oversight, assurance, audit, and comparison.

CASE STUDY

Our consultants provided security specialist support to one of the largest CNI security and resilience improvement programmes in Europe.

This work, over a number of years, included vulnerability assessment, site security plans, emergency response plans (including counter-terrorism), crisis management advice, developing operational requirements for the physical protection solutions, senior level stakeholder engagement (including regulators), improving the security management system, security training, and acting in an intelligent customer role to ensure quality.

The benefits we delivered included: clarity on risks and tolerance; cost effective and performance tested mitigation strategies; integrated plans, procedures and response arrangements; and regulatory compliance.

FRAZER-NASH CONSULTANCY

Frazer-Nash is a leading systems and engineering Technology Company. We're renowned for our work in the aerospace, transport, nuclear, marine, defence, power and energy sectors and our security, resilience, cyber and information technology expertise.

For more information about Frazer-Nash please visit our website.
www.fnc.co.uk/security

www.fncaustralia.com.au

Offices throughout the UK and Australia

FRAZER-NASH
CONSULTANCY