

Security solutions: insider threat mitigation

Frazer-Nash Consultancy delivers security services to public and private sector clients, including Critical National Infrastructure (CNI).

OUR APPROACH: BLENDED SOLUTIONS

We live in a world increasingly connected in cyberspace, and where the insider threat poses significant risk. The modern adversary will seek to exploit vulnerabilities across all domains - physical, cyber and social. So, at Frazer-Nash, we address the challenges posed by these multi-faceted threats, with cost-effective blended solutions.



WE UNDERSTAND YOUR CHALLENGES

The insider is regarded as the top enterprise security risk and is one of the most challenging to evaluate and mitigate, in a cost-effective way. It is estimated that only 26% of businesses have an insider threat mitigation programme (ITMP) and yet insiders have caused multi-million pound losses and untold damage to reputation and competitiveness.

We recognise that insider risk covers not only malicious intent but also unwitting employee harm. The former is a counter-intelligence challenge and the latter demands a training and education focused approach.

Your business may already have an ITMP in place and you want to validate its effectiveness and improve it; or you may wish to establish such a programme and would like well qualified independent advice to help design and implement it.

WHY FRAZER-NASH

At Frazer-Nash, we tailor all our blended security and resilience services to individual client needs. Whatever size of business you are, we have a solution for you.

Our consultants have decades of relevant multi-disciplinary experience, including:

- ▶ Physical, cyber, personnel and transport security
- ▶ Information assurance
- ▶ Human factors and psychology
- ▶ Training and education

- ▶ Programme management and
- ▶ Operational requirements

INSIDER THREAT MITIGATION PROGRAMME

Overview

The Frazer-Nash ITMP framework is effects based:

- ▶ **Identify** the risks
- ▶ **Protect** critical assets
- ▶ **Detect** potential insider events
- ▶ **Respond** to specific threats and
- ▶ **Recover** quickly

Each component of an ITMP has a distinctly human element. While external cybersecurity threats can usually only be prevented or detected through technical tools, insider threats commonly exhibit human behaviours that signal an attacker's intent. Best practices for insider threat mitigation, therefore, involve an integrated technical and a human focused approach.

Design

We can support the design of your enterprise level ITMP, founded on a bespoke insider risk assessment, following Government best practice methodology; to understand the nature of the risks being carried. A clear set of requirements sets the conditions to achieve the desired outcomes and realise the benefits.

Implementation

The programme is implemented through a clear plan, contingencies and procedures, supported by adequate governance, management, and assurance; together with broad stakeholder engagement, adequate recruitment, training, education and internal communication.

Continuous improvement

In line with security management system best practice, the ITMP should aspire to continuous improvement. We can help achieve this, founded on a performance measurement and review process; complemented by independent assurance, validation and a lessons learned capability.

BENEFITS

An effective ITMP can offer your business the following benefits:

- ▶ Reduced exposure to insider related risk
- ▶ Increased resilience to an insider event
- ▶ Improved client confidence and competitiveness
- ▶ Compliance with regulatory expectations
- ▶ Reduce risk of hefty fines for data loss
- ▶ Safeguards enterprise reputation and
- ▶ Employee confidence

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

Copyright© Frazer-Nash Consultancy Ltd 2017

