Noble

Securing Operations and the Flow of Data Across Critical National Infrastructure

Critical National Infrastructure (CNI) Use Case

The Government's 2016 cyber security strategy states that the cyber security of the UK's critical national infrastructure (CNI)—from the physical infrastructure to the digital networks and data—is critical, because a successful attack "would have the severest impact on the country's national security". Yet the strategy also acknowledges that across many priority sectors "cyber risk is still not properly understood or managed, even as the threat continues to diversify and increase".

Challenges for Critical National Infrastructure Providers

Most of the UK's CNI is owned and operated by the private sector. In December 2017, the Joint Committee on the National Security Strategy, re-established the inquiry, into the Government's approach to ensuring the cyber security of UK's CNI, exploring how it works together with private-sector operators and industry regulators in doing so. Two of the nine topics within the inquiries terms of reference, call out key challenges that need to be addressed between the public and private sector:

- The effectiveness of the Government's relationships with, respectively, private-sector operators and regulators in protecting CNI from cyber attack
- The balance of responsibilities between the Government and private-sector operators in protecting CNI against cyber attack

According to a joint US Department of Homeland Security/FBI report, advanced persistent threats (APT) are targeting government entities and organisations in the energy, nuclear, water, aviation and critical manufacturing sectors. The APT activity appears to be a multi-stage intrusion campaign by threat actors targeting low security and small networks to gain access and move laterally to networks of major, high value asset owners within the energy sector.

Risks of Anomalies in the CNI Industry

As CNI providers move towards increasingly connected large networks that allow for monitoring and remote automated control, the potential for cyber attacks rises.

According to a report released by the UK government, cyber attacks on CNIs can be motivated by financial gain (e.g. by ransom), to manipulate public opinion, demonstrate an attacker's prowess, conduct espionage or cause physical disruption. Potential attackers range from individuals and activists with limited capability to organised crime groups and nation-states with significant expertise and resources. The report also notes that foreign states or state-sponsored groups regularly attempt to penetrate UK networks, specifically targeting the defence, finance, energy, telecommunications and government sectors.

The UK is proposing a hefty fine for critical national infrastructure (CNI) companies that fail to protect against loss of service due to cyber attacks. For companies that do not comply with the new regulations, the fine could be as high as

£17 million, or up to four percent of annual turnover.

Among other criteria, the fine would be assessed against companies that fail to:

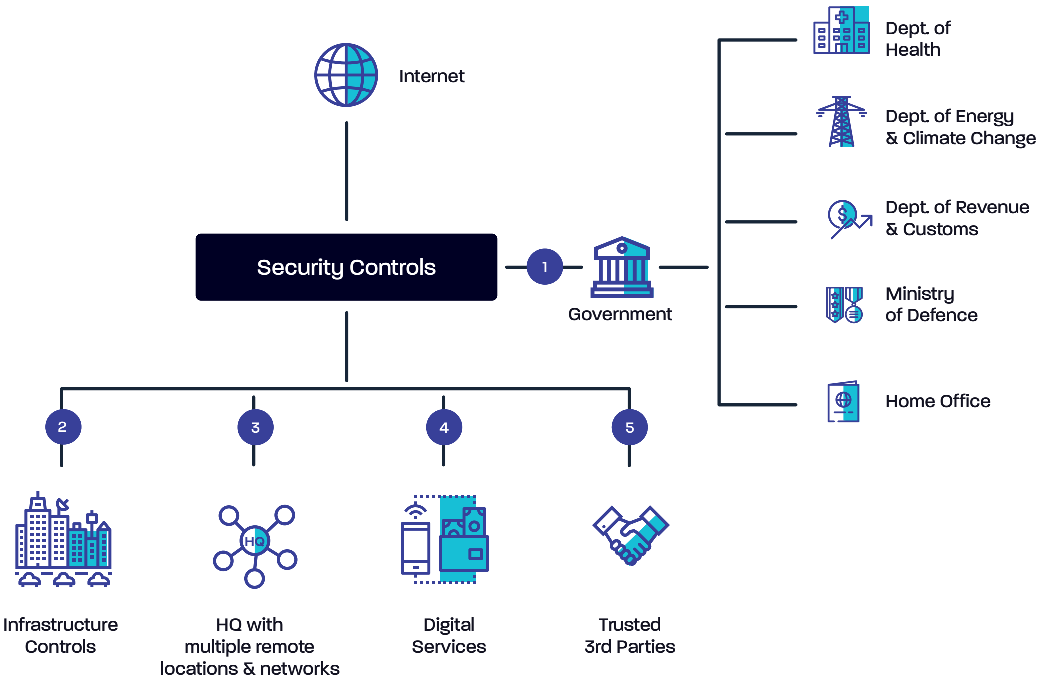
- Develop a strategy and policies to understand and manage their cyber security risks;
- Implement security measures to detect and prevent attacks or system failures;
- Deploy security monitoring;
- Take steps to raise staff awareness and require training;
- Assess their risks adequately or take appropriate security measures.

Noble Vision Addresses the Assessed Criteria to Mitigate Loss of CNI Service

The continuous operation of CNI services requires a wider appreciation of operational, targeted and compromised systems. The effect of cyber attacks are the cause of unsecure, reactive and ineffective processes and procedures, with operational and security technologies implemented with minimal integration capabilities. None of these "cause-effect" attributes are intentional, but a consequence of balancing budget, people and priorities.

Noble Vision continuously monitors and analyses CNIs activities in all their extents – from standard users to complex industrial control networks – to identify risks and take instant action to neutralise them.

Automation to drive operational excellence between departments is achieved through the flexible and powerful open integration offered by Noble Vision. Accurate detection of anomalies is attained through the use of expectations and our unique deep learning adaptable engine. Both provide actionable intelligence to manually or automatically take action, optimising the whole process. The diagram below outlines how Noble Vision implements and in many cases leads the strategy to reduce or neutralise the risks associated with CNIs.



1. Secure interactions with Government to coordinate with other CNIs

2. Secure safety critical systems and production systems

3. Secure operations and business as usual

4. Secure users' digital interactions and automated augmented services

5. Secure third parties' communications and enforce compliance