Meta
MISSION DATA

Case Study: Cyber Vulnerability Investigations

Cyber Vulnerability Investigations (CVIs) are socio-technical assessments used to identify cyber risks. Uniquely, CVIs take an 'aggressor' view, applying adversary techniques to locate vulnerabilities, exercise viable attacks paths and develop mitigations. CVI output benefits a wide audience and a programme of CVIs can support enterprise-level risk management.

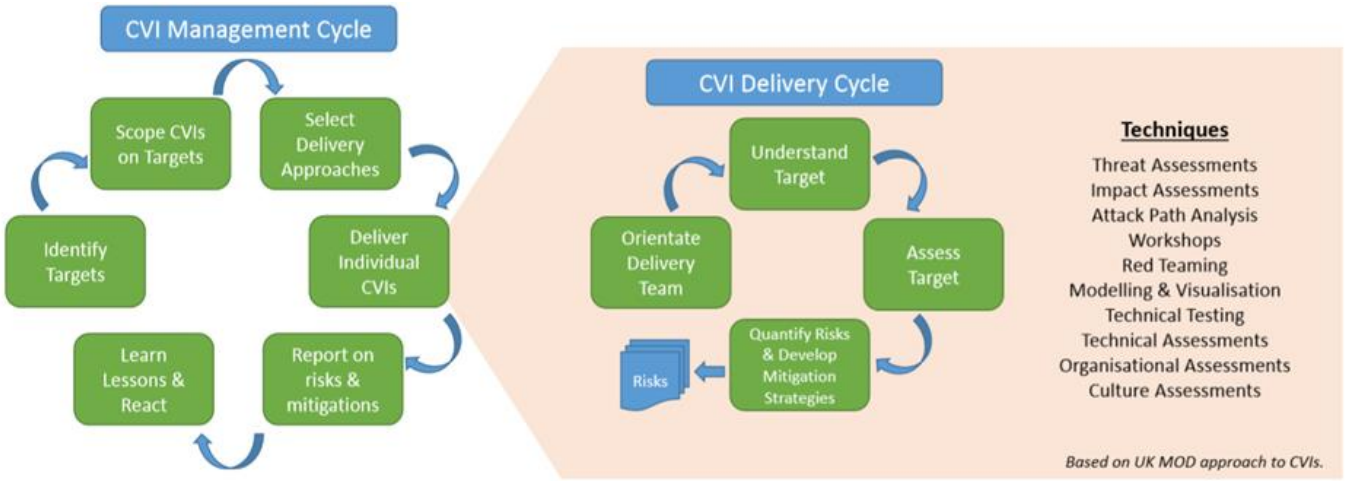
As socio-technical investigations, close attention is paid to how people, processes and technology work together and the potential vulnerabilities this creates, which are often key to an attacker being able to exploit a vulnerability. CVIs therefore consider human elements relevant to cyber (behaviours, culture) in parallel with traditional 'harder' technical cyber assessments.

CVI Frameworks

As CVIs can be complex, investigations are best undertaken using a structured methodology, ensuring CVI activity focuses on desired outcomes with a consistent approach. In some organisations with few CVI activities a simple framework is sufficient. Larger organisations may need a more robust framework to support an enduring programme of CVIs.

Case Study: UK MOD's CVI Programme

The UK Ministry of Defence (MOD) has developed its own framework for CVIs which is now in its 5th iteration. It sets out the management and delivery activities required to conduct CVIs in a Defence setting. It provides guidance on techniques which can be employed, tailored where appropriate to the Defence environment.



An example CVI Framework, based on the UK MOD's

Meta Mission Data (MMD) supported UK MOD in developing its framework and delivering its CVI programme:

- **As a Delivery Partner** MMD delivered individual CVIs on air and maritime platforms, deployable IT systems and establishments.

- **As its Operations and Delivery Specialists (ODS)** MMD supported MOD's CVI Operations Cell in scoping and managing its CVI portfolio. This included oversight of CVI teams, technical assurance of CVI outputs, portfolio analysis and improvements to the CVI Framework.

- **As a Training Provider** MMD delivered training in MOD's CVI framework for both UK Industry Delivery Partners and MOD CVI practitioners from its training facilities and at customer sites, providing interactive sessions with realistic scenarios to exercise the CVI process.

Our team's appropriate skills and expertise included:

- **Systems engineering** for complex systems (including people, organisations, technology and processes) to rapidly develop understanding and representations.
- **'Soft skills'** to facilitate interactions with a wide range of CVI stakeholders.
- **Domain experience** for core defence domains (Air, Land, Maritime, Space, Cyber).
- **Cyber threat understanding** across both Industry and MOD sectors.
- **CVI techniques** including attack path analysis, technical, organisational and cultural assessments).
- **Risk assessment**, including quantification and identification of themes, mitigations and interventions and
- **Risk management**, including specification and implementation of mitigations.

Outputs from UK MOD's CVIs have benefited military operational communities, which are able to make more informed risk decisions (i.e. a capability will be deployed at *x* degree of cyber risk). Findings have also allowed interventions to be made in capability acquisition alongside adjustments in enterprise risk posture, validating the approach

Value of CVIs (To all sectors)

Conducting CVIs within a structured framework can benefit organisations across many sectors, providing:

- **Holistic and realistic assessments**, taking an attacker view which considers the full extent and interaction of an organisation's people, processes and technology.
- **A scalable approach** which is well suited to investigating complex organisations, as well as specific systems or sites.
- **A methodical approach** which leads to effective (cost and impact) interventions.
- **An adaptable approach**, which can examine organisations/systems/capabilities in early stages of implementation as well as those which are already fully mature.

- **Rich outputs**, which integrates with enterprise risk management and provides reports at appropriate levels for multiple audiences (technical, management, board level).
- **Established techniques,** proven to deliver valuable findings while being sufficiently flexible to accommodate novel assessment approaches for unique circumstances.
- **Evidence for scrutiny,** validating ‘secure by design’ approaches and boosting the likelihood of achieving approval/investment gates.

For further information on how CVIs can support your organisation, please contact cyber@mmd.meta.aero .