MOBIUS APPROACH TO VULNERABILITY GOVERNANCE

A vulnerability is a weakness in an IT system or network that could allow an attacker to exploit the system to compromise the integrity, availability, or confidentiality of the environment and data. These vulnerabilities are the source of constant scrutiny given the exponential increase in breaches, which can be associated with poor vulnerability management on the part of organisations.

One of the key focus areas of vulnerability management is conducting vulnerability assessments by running vulnerability scans and performing penetration tests against the organisations key applications, databases, operating systems and networks. Most organisations have already implemented vulnerability assessment practices either as an internal capability or as an outsourced service from a third party provider. Often, however, the data received from these vulnerability assessments is unable to be used to effectively remediate the vulnerabilities due to the large volumes of vulnerabilities identified, and the organisations lack of vulnerability management processes to support the remediation. This results in the organisation not being able to implement the recommendations from the scans effectively in order to improve their security posture.

Organisations need to recognise that vulnerabilities identified are a symptom of broken governance and management practices and that in most instances vulnerabilities are introduced by organisation itself due to inadequate user access processes, lack of security configuration standards and poor coding practices. Organisations need an approach that seeks to mature the entire vulnerability management practice with a focus on fixing root causes, not merely purchasing a vulnerability testing tool or service and running a scan – Mobius calls this broader approach Vulnerability Governance. Vulnerability Governance is a key component of IT risk management and enables organisations to prioritise risks, drive mitigation efforts, and focus IT asset owners to bolster the organisation's security posture. Organisations should also utilise these processes to increase awareness, drive security priorities and raise the profile of Information Security within the organisation.

Mobius' approach to Vulnerability Governance seeks to assist organisations by identifying the root causes of the security exposure areas and helping to mature the remediation processes to resolve the root causes of vulnerabilities and inadequate management practices, which typically include:

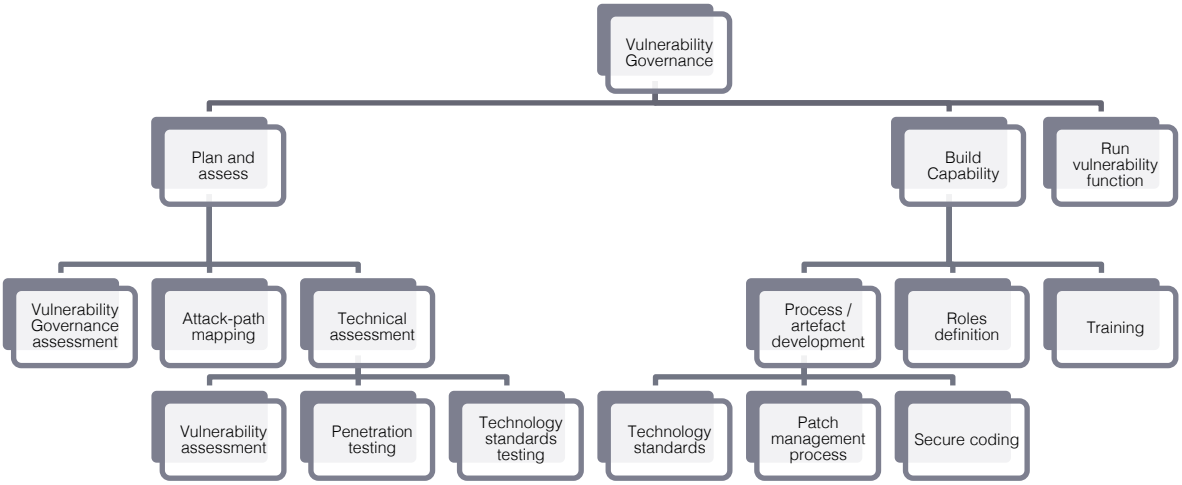
- Inadequate patch management;
- Insecure system / network design and development practices;
- Lack of security standards or misalignment of corporate systems to these; and
- Inadequate user access / permissions management.

Important facets that security managers should incorporate in their Vulnerability Governance programs include:

- Overall Vulnerability Governance design and oversight, including management practices, technologies, capability, roles & responsibilities, and processes required for effective Vulnerability Management;
- Identifying the root causes of vulnerabilities and ensuring remediation processes and accountability are defined to drive mitigation and ultimately improve security; and
- Implementation of technology standards by using a baseline configuration approach for all applications and systems and regular testing against these.

Mobius' Vulnerability Governance services focus on enabling organisations to broaden their vulnerability management practices and to mature from assessment, to management, to governance of their vulnerability management function. This extensive range of services is completely customisable to each organisations maturity and culture and will result in more effective mitigation of IT vulnerability risks.

The diagram below outlines Mobius' services that extend from assisting organisations with planning, governance assessments, building of vulnerability management capability, improving vulnerability practice maturity through to managed services.



Selected services are summarised below:

- Vulnerability Governance assessment – an independent assessment of the vulnerability management posture of the organisation which results in a capability improvement roadmap.
- Attack-path mapping analysis to help organisations prioritise which assets to focus for safeguarding and to test security of critical assets against real world scenarios.
- Vulnerability assessment services, including:
    - Vulnerability Assessments – assessment of the IT infrastructure to determine vulnerabilities in the environment which could be exploited and to determine appropriate remediation plans.
    - Penetration Testing – performing external security assessments.
    - Technology Standards Testing – performing comparative tests to determine if the technology configurations match to those of best practice prescribed by various technology standards.
- Vulnerability Management consulting – a structured approach to improve the vulnerability management capability within the organisation.
- Process improvement and artefact development services, including:
    - Technology standards development and consulting;
    - Patch management process development;
    - Secure coding practice improvement and training;
    - Identity and Access Governance (IAG); and
    - Roles and responsibility definition.
- Vulnerability and Penetration Testing training services – professional training to ensure the organisation's staff are skilled to combat the latest threats.
- Vulnerability Management Managed Service – a service whereby organisations outsource their vulnerability identification and management to Mobius to enable them to focus on core operations.