MOBIUS CYBERSECURITY TESTING AND IMPROVEMENT

There are media reports on a daily basis of organisations that have been attacked by cyber criminals resulting in defacement of websites, theft of confidential information and denial of service attacks to name a few. Not only is the number of hacking incidents increasing, but also the net effects on organisations are worsening. A report by the Centre for Strategic & International Studies estimates that cybercrime in South Africa is costing the country approximately R5.8 billion a year – not to mention the added impact of brand and reputational damage. Ensuring the security of information assets ought to be high up on the agendas of organisations.

Given that new vulnerabilities are discovered on a daily basis it is essential that organisations have an adequate technical vulnerability testing capability to test web sites and web applications on a frequent basis. Once identified, an effective vulnerability management capability is required to ensure that vulnerabilities are remediated and root causes (such as insecure coding practices or an ineffective patch management process, among others) are addressed. Failing to address vulnerabilities in a timeous manner allows an attacker a window of opportunity to exploit vulnerabilities, resulting in an increased risk of the information systems being compromised.

Technology vulnerabilities are not the only means of attack - cyber criminals also use social engineering techniques such as phishing attacks that exploit the lack of employee awareness. It is essential that adequate information security awareness programmes are run on a frequent basis, and that phishing exercises are performed to assess the effectiveness of employee information security awareness training.

Building on the expertise, experience and technology toolsets of the Mobius vulnerability governance team, we have developed a cybersecurity testing and improvement managed service to address some of the common challenges faced by many South African organisations, including the lack of skilled and experienced cybersecurity resources, budgetary constraints on the information security function and the lack of access to vulnerability assessment technologies and resources required to manage the output reports of these technologies.

The service incorporates both the technology and people aspects of cybersecurity and aims to test and improve organisational cybersecurity capability:

	Testing	Capability improvement
Technology	Vulnerability scanning and web presence analysis	Vulnerability Management
People	Phishing, surveys, and cyber incident response testing	Information security awareness

CORE SERVICE OFFERING

- **Quarterly website/web application vulnerability scanning** - scanning up to 20 IPs per year using industry-leading commercial web vulnerability scanning technology. This includes analysis, root-cause identification, reporting and recommendations for effective, risk-based vulnerability remediation.
- **Monthly (ongoing) vulnerability management** - maintaining a log of current vulnerabilities, monitoring of vulnerability remediation efforts, following up with responsible personnel, trend analysis and reporting.
- **Annual phishing exercise** - conducting annual phishing test and assessing user responses.
- **Monthly information security awareness material** - provision of email awareness material to address the areas of improvement noted during vulnerability scanning and phishing.
- **Annual cyber incident response simulation exercise** - facilitating a simulated cybersecurity incident to test your cybersecurity incident response plan and personnel.
- **Semi-annual external visibility/web presence analysis** - analysing cyber threat networks to determine whether your organisation or industry may be at risk of cyber-attacks.

SUPPLEMENTARY SERVICES:

In addition to our standard services, Mobius offers supplementary services to further improve your organisation's cybersecurity capability on an as-needed basis:

- **Attack path mapping** - an analysis of the path a real-life attacker would follow to gain access to your organisation's "crown jewels", which serves as input into remediation planning.
- **Penetration testing** - testing whether identified vulnerabilities are, in fact, exploitable by means of specialised manual technologies and expertise.
- **Internal network and infrastructure vulnerability assessments** - testing the internal network and infrastructure for security vulnerabilities.
- **Access to the Mobius team to supplement resources during an incident response** - the team that understand your environment can be available during a cybersecurity incident if needed.

COST

The core service is priced at R30 000 per month (excl VAT) over a minimum 12-month period for organisations employing no more than 500 employees. This price is valid for all organisations signing on during 2016. Should any of the supplementary services be required, these will be priced separately.