mobius consulting
actualising change

CYBERSECURITY

No modern business is immune to cyberattacks. Which means the key to your defence lies not in evasion, but in preparation.

And that means having all the right controls and processes in place to respond to threats quickly and effectively. If you don't, an attack could have serious impacts on your business, and response could take too long – if it happens at all.

The good news is, Mobius is perfectly positioned to help you prevent, detect and respond to cyberattacks. That's because we're not an audit company whose role ends with telling you what your risks are. Nor are we a technology vendor with a narrow, product-specific focus. Instead – and far more usefully – our skill set enables us to unite people, processes, technology and compliance in a single, cohesive solution ideally geared for your environment.

First, we help you understand your current risks and readiness, ensuring realism by deploying simulated attacks to probe your systems for unknown vulnerabilities. Then, assessment in hand, we develop your cybersecurity improvement plans and response processes, and provide a full suite of services to help you implement both. Destination reached, you'll be fully equipped to respond to cyberthreats.

THE MOBIUS ADVANTAGE

EXPERTISE

- Assessment against NIST CSF and ISO 27000 standards
- Vulnerability and penetration testing
- Full development and implementation of incident response processes
- Cybersecurity Fundamentals (CSX)
- Offensive Security Certified Professional (OSCP)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- ISO 27001 Lead Implementer

APPROACH

- Holistic and realistic assessment via ethical hacking
- Determine cybersecurity control improvements required for detection and prevention
- Implement response processes that work best for you
- Intuitive for all stakeholders, with detail to guide response teams
- Hands-on assistance with internal adoption of the processes

RESULTS

- An improved cybersecurity posture
- The ability to respond to cyberattacks
- Processes that are adapted specifically for your needs

Contact Mobius Consulting:
+27 21 201 1120 | +27 10 590 6111 | info@mobiusconsulting.co.za
www.mobiusconsulting.co.za

CYBERSECURITY APPROACH

STEP ONE
UNDERSTAND THREATS AND CRITICAL ASSETS

- Identify critical data and system assets
- Identify potential cyber-related threats
- Develop a threat profile

STEP TWO
ASSESSMENT OF CURRENT AND FUTURE STATES

- Assess how prepared the organisation is to deal with a cyberattack
- Decide on a desired state of cybersecurity capability
- Determine remediation across people, process and technologies

STEP THREE
ROAD MAP AND PRIORITISED PLANS

- Prioritise remediation projects
- Develop project plans and overall road map
- Allocate responsibilities

STEP FOUR
INCIDENT RESPONSE

- Develop incident response processes
- Consider integration of the processes across organisational functions
- Develop playbooks

STEP FIVE
IMPLEMENT IMPROVEMENTS

- Implement and embed the incident response processes
- Implement projects according to defined road map
- Improve organisational and security capabilities required

>> Let us help you avoid becoming a cybersecurity statistic.

---

mobius consulting
actualising change

Contact Mobius Consulting:
+27 21 201 1120 | +27 10 590 6111 | info@mobiusconsulting.co.za | **www.mobiusconsulting.co.za**