

CYBERSECURITY ESSENTIALS

For BUSINESSES



ARMATA

CYBER SECURITY

www.armata.co.za

Now, more than ever, we all rely on the Internet to live, work and communicate. If you're online in any way, you're vulnerable to cybercrime. Sadly, thanks to the dark web and the rise of Malware-as-a-Service, it's only becoming cheaper and easier for cyber criminals to attack businesses of every size.

ARMATA Cyber Security is here to help you fight back. Forming part of the Vivica Group of companies and powered by Vox, we deliver a comprehensive set of cybersecurity products and services to over 1000 businesses across South Africa to prevent breaches and protect critical data.

WHAT IS CYBERSECURITY?_

Cybersecurity combines essential technology, people and processes to protect systems, networks, and data from cyber-attacks.

When it comes to cybersecurity, the challenge for businesses is threefold:

- **Assessing cybersecurity risk areas accurately and cost-effectively**
- **Matching cybersecurity needs within the company IT budget**
- **Maintaining a simple, effective and affordable cybersecurity programme on an ongoing basis**

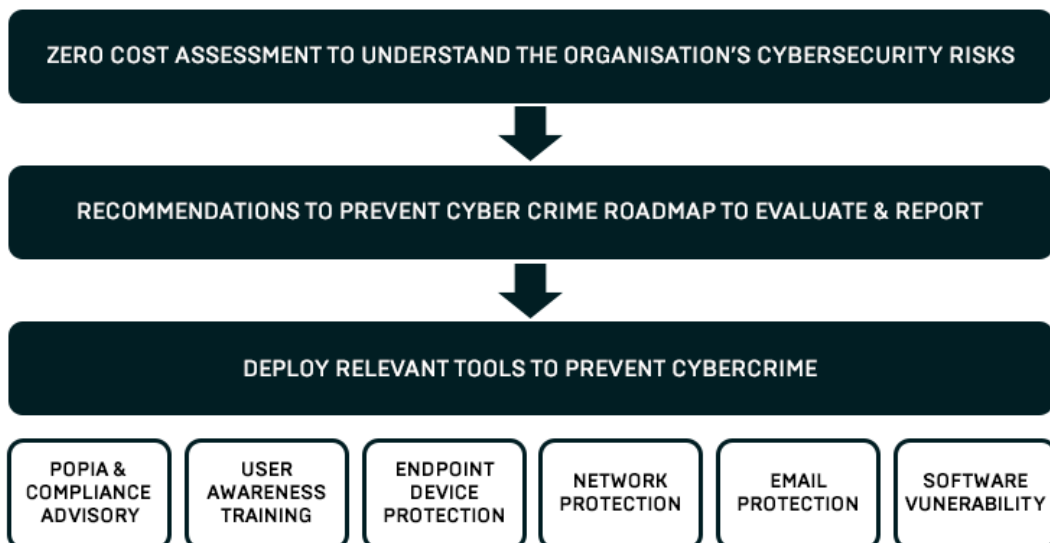
WHY IS CYBERSECURITY SO IMPORTANT?_

At the moment, South Africa is one of the Top 5 most targeted countries in the world when it comes to cybercrime. According to insurance companies, local businesses pay R4 million on average to cover the costs of a breach. With POPIA (Protection of Personal Information Act) now in place, those responsible for keeping personal data safe within their organisation could also face additional fines or even jail time.

- **Over 80% of cyber-attacks are due to stolen or weak passwords**
- **In 2021, 96% of companies acknowledged facing some form of phishing attack**
- **Ransomware rose by 42% in 2021**
- **280 days is the average amount of time most companies take to detect and respond to cyber-attacks in their environment**

_HOW CAN ARMATA HELP?

We understand cybersecurity resources can be costly and are in short supply. That's why we've adapted best practice frameworks to suit organisations with limited budgets and access to IT skills. And it all starts with our FREE Cybersecurity Assessment.



THE ARMATA CYBERSECURITY ASSESSMENT

HOW IT WORKS

ASSESSMENT METHODOLOGY:

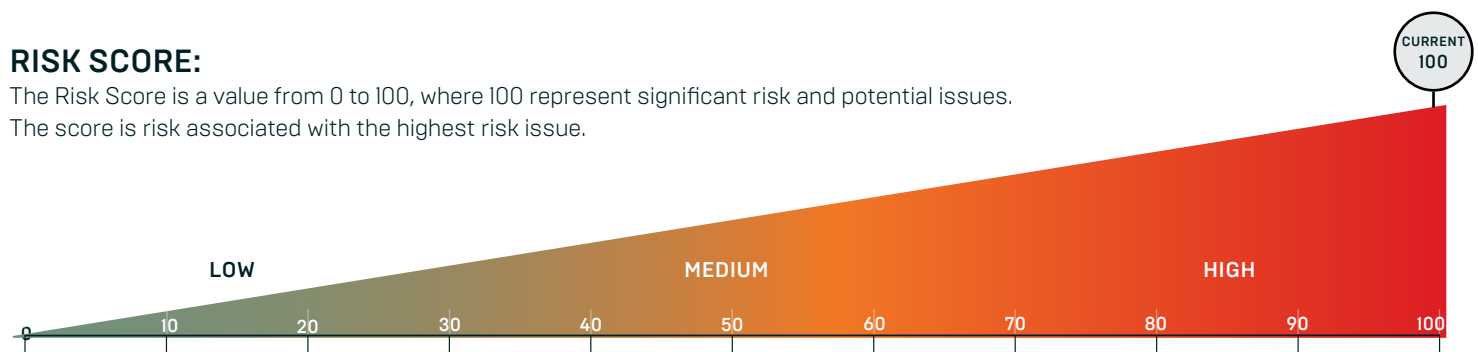
It involves a software deployment, for a period not exceeding two weeks, which is non-intrusive and presents no risk to your company.

VALUE DELIVERED:

A report card that definitively assesses cybersecurity risk and baselines the risk into a risk score – allowing you to see which areas to prioritise first.

RISK SCORE:

The Risk Score is a value from 0 to 100, where 100 represent significant risk and potential issues. The score is risk associated with the highest risk issue.



CRITICAL IT AREAS ARE INVESTIGATED:

The status of the following key cybersecurity areas / tools:



Antivirus and Anti-spyware

Endpoint software on laptops, desktops, mobile devices and servers to detect and destroy known viruses and spyware.



Firewall (presence and effectiveness)

Used to protect a network or system against unauthorised access. Next-Gen Firewalls can also control users' data in and out of a network.



OS Patching

Used to fix software vulnerabilities that may be exploitable by hackers.



Insecure Listening Ports

Open ports that can be exploited by hackers to gain access to a company's network.



History of Failed Logins

These can point to a hacker's attempt to gain access to an environment.



User Safety Settings

Walking away from a PC and not locking the screen can allow unauthorised users quick and easy access to a PC.






ASSESSMENT REPORT CARD:

Once scanned, the Assessment will produce a report card with results per user - using a grading system from A to F.

Computer	Overall Grade	Anti-Virus	Anti-spyware	Local Firewall	Missing Critical Patches	Insecure Listening Ports	Failed Logins	Network Vulnerabilities	Screen Lock with Timeout	System Aging	Supported OS
AABOURIZK-NB (19#.##.###)	C	A	B	C	-	A	B	-	F	A	A
ACRONJE-NB (10.##.###)	A	-	-	-	-	-	A	-	-	-	A
ADAWSON (192.###.###)	B	A	A	C	-	A	B	-	-	A	A
ADAWSON-NB (1#.##.###)	C	A	B	C	-	-	A	-	-	A	F
ADORO-PC (192.###.###)	B	A	A	A	A	A	A	-	F	A	A
ALSOFFICE-PC (1#.##.###)	F	A	B	C	C	A	B	-	F	A	F
AJACOBS-PC (1#.##.###)	C	A	B	A	B	A	A	-	F	A	A

OUTCOME IF CYBERSECURITY VULNERABILITIES ARE FOUND

ARMATA will propose solutions that address one or all of the following risk areas – these could be, but are not limited to:

-  **Network Security** – protects the environment from attacks externally as well as controls how users utilise the Internet connection.
-  **Email Security** – stops spam and potential phishing or malware attacks in emails.
-  **Endpoint Security** – protects laptops, desktops and servers from virus or malware attacks – preventing loss of company data.
-  **User Awareness Training** – trains staff to be more cyber aware and to act more securely.
-  **Data Backup** – protects it against loss and makes it easier to recover a system from a breach or failure.

ASSESSMENT FREQUENCY – MANAGED SECURITY SERVICE

When these Assessments are conducted on a regular basis, you'll not only become aware of the cybersecurity areas to prioritise in terms of risk and budget spend, but you'll also receive a roadmap to make continuous improvements to your IT environments to ensure your scores remain healthy.

ARMATA DELIVERS INTELLIGENT CYBER SECURITY SOLUTIONS

ARMATA Cyber Security is a company powered by Vox Telecom. ARMATA was established to create a cyber security identity for Vox and allow for a more focused business. Our vision is to deliver cyber intelligent solutions, that help achieve zero interruption to your business systems, whilst maintaining the highest level of protection for your data.