



CYBER SECURITY TRENDS FOR 2023

WHAT TO EXPECT, WHAT TO DEFEND AGAINST

BARNOWL ONLINE INFORMATION SHARE

Michael Davies

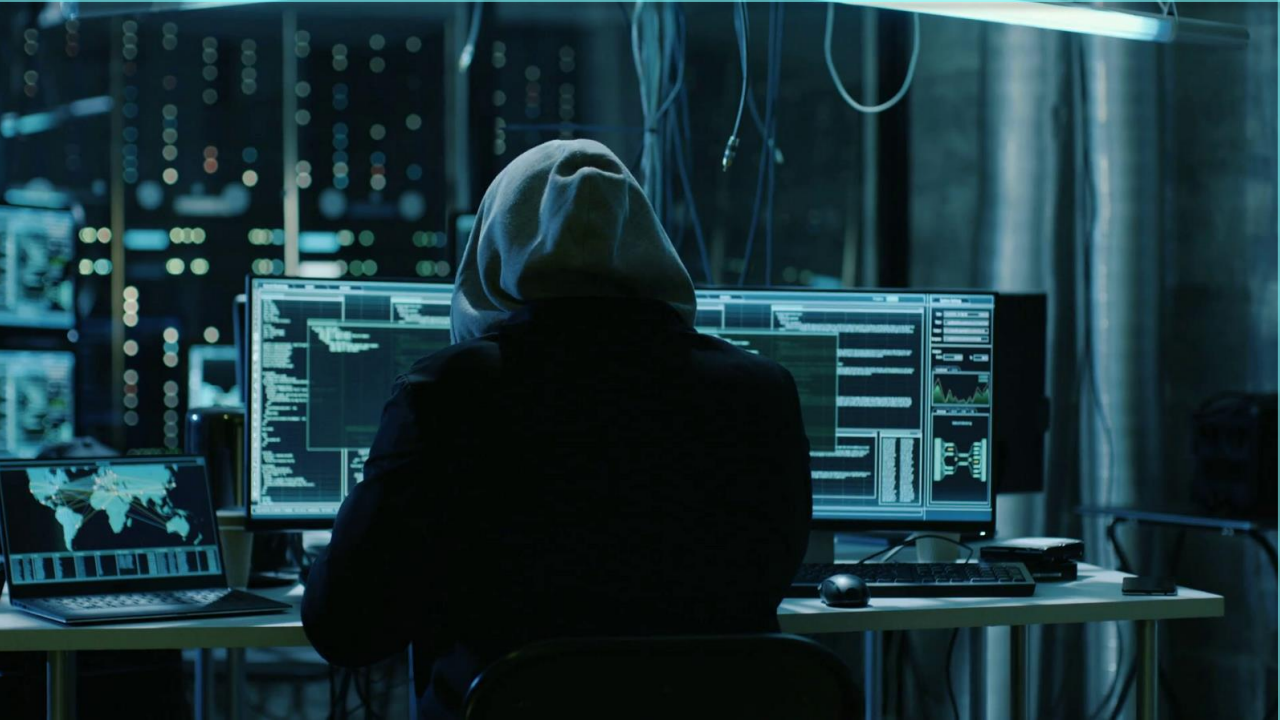
Pax Resilience

<https://www.paxresilience.io>

Tim Gilman

Cyber Armed Security

<https://cyberarmedsecurity.com>



Cyber Insurance market hardening
Increasing premiums
Increasing excesses
Less cover

THE AVERAGE DATA BREACH COSTS A SOUTH AFRICAN COMPANY R46M AND TAKES EIGHT MONTHS TO DETECT AND CONTAIN, IBM SECURITY STUDY 2021

Data breaches in SA are on the rise
Almost nine in 10 organisations in South Africa have suffered a ransomware attack, with a third of the data unable to be recovered.
(IT-Online April 2022)

Ransomware
Phishing
Business email compromise
Vulnerability in third party software
Stolen or compromised credentials
Malicious insider
Brute force attack
Distributed denial of service (DDoS)



Data is a significant
organisational asset

DATA PROTECTION HAS LED TO CHANGES
IN STRATEGY, GOVERNANCE, OVERSIGHT
& COMPLIANCE IN ORGANISATIONS TO
PROTECT:

Intellectual Property & 'Secret Sauce'

Know-how

NDA's & Contracts

Personal and Company Information of:

Customers

Employees

Suppliers

STANDARDS

ISO 27001 – Info Sec

ISO 27032 – Cyberspace

ISO 21434 – Automotive Cyber Security

NIST

SOC 2

COMPLIANCE

GDPR

POPIA Act 2013

National Cyber Security Policy
Framework 2015

NDA's

Contracts

10 CYBER SECURITY TRENDS FOR 2023

builtin.com/cybersecurity/cybersecurity-trends-for-2023

- Securing both remote and hybrid workers
- Adapting security for increased cloud dependency
- Visibility, control, protection and remediation in response to supply chain attacks, IoT attacks and ransomware
- Preventing ransomware attacks
- Increased popularity of SaaS security solutions
- Spotlight on chief information security officers' liability
- Building cyber resilience
- Governments prioritizing critical infrastructure
- Government and industry collaboration across countries and industries
- **Realization that people are and will remain the main causes of attacks**

CYBER: THE WEAKEST LINK THE HUMAN FACTOR

- Phishing
- Smishing
- Vishing
- Social Engineering



- TRAINING
- AWARENESS
- SIMULATIONS
- KEY CYBER SECURITY CONTROLS

KEY CYBER SECURITY CONTROLS

Multifactor authentication for remote access

Endpoint detection and response

Secured, encrypted and tested backups

Cyber incident response and management, planning & testing

Cyber security awareness and phishing testing

Remote desktop protocols

Privileged Access Management

Email filtering and web security

Patch management and vulnerability management

Logging and monitoring / network protection

End-of-life systems replaced or protected

Vendor / supply chain management

EVERYONE IS RESPONSIBLE



The Board
Risk & Audit Committee
The Executive Team (not just CISO, CIO and CRO)
Management
Employees



Integration with;
Suppliers
Partners
Other
Stakeholders



THANK YOU

PLEASE FEEL FREE TO CONTACT US FOR MORE INFORMATION

Michael Davies

Pax Resilience

<https://www.paxresilience.io>

Tim Gilman

Cyber Armed Security

<https://cyberarmedsecurity.com>