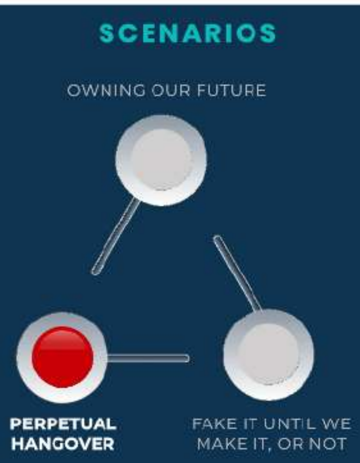
3.11
CYBER RISK

As the digital age accelerates, cybersecurity is more critical than ever. New working patterns raise concerns about the security of networked technologies and increase the risk of cyberattacks and data fraud. Cyber risk is no longer just an IT problem; it is an extremely serious threat to the well-being of a country, organisation and the individual.

SCENARIOS



FLAGS

COUNTRY FLAGS	C	F
1. LEADERSHIP	🟨	🟩
2. INSTITUTIONAL CAPACITY	🟥	🟨
3. POLITICS	🟨	🟨
4. SOCIAL COHESION	🟥	🟨
5. NATIONAL POLICY	🟨	🟨
6. SERVICE DELIVERY	🟥	🟨
7. INEQUALITY	🟥	🟥
8. ECONOMY	🟥	🟨
9. GLOBAL TRENDS	🟩	🟩
10. CLIMATE	🟥	🟥

C – CURRENT (2020/21) **F – FUTURE (2030)**

SUCCESS STORIES

The South African Banking Risk Information Centre (SABRIC), a Non-Profit Company formed by major SA Banks to initially assist the Banking and Cash in transit industries combat organised bank-related crimes. They have adapted to become Africa's trusted financial crime risk information centre leveraging on strategic partnerships.

It was no small feat to bring financial competitors together to share sensitive incident information in the spirit of collaboration. While there have been challenges along the way, I believe the benefits are now realised by the financial sector and the country as a whole.

Cyber-attacks and data breaches are on the increase. Covid-19 has been the catalyst forcing countries, organisations and individuals to embrace digitisation to a far greater extent in a short time frame, thus making us more dependent on technology and far more susceptible to cyber-crime. Rapid rollouts and dramatic surges in the use of technological solutions increase risks of cybercrime, infrastructure overload and breakdown, privacy violations and inequality.

TOP 5 CHALLENGES TO ACHIEVING TARGETS

1. Vulnerable Services: Expanded use of potentially vulnerable services, such as virtual private networks (VPNs) that lack adequate safeguards due to increased working from home.
2. Legislation: Ineffective legislative and regulatory processes, as well as poor and often delayed implementation.
3. Sophisticated cyber-criminal operations run like large corporates, with specialised divisions targeting governments, companies, NGOs and individuals for considerable amounts of money.
4. Poor cyber security awareness and implementation, specifically exposing sensitive information.
5. Increased complexity, dependency and larger footprint, as more organisations make use of third-party service and shadow IT (cloud services).

TOP 5 RISK TREATMENT OPTIONS AND OPPORTUNITIES

1. Identify appropriate technology and process interventions in order to optimise preventive, detective and investigative controls in your environment.
2. Allocate adequate funds and resources to implement much needed legal and regulatory reform measures and reduce bureaucracy to ensure that critical legislation is implemented timeously. Introduce legislation in South Africa compelling organisations to declare cyber attacks/ incidents
3. Public and private organisations will need specialised skills dealing with cybersecurity. Not just an IT responsibility. It is much wider.
4. Monitor and report cyber-attacks and breaches at senior levels rather than just being an IT incident and an IT problem. Set up an incident response team. Invest in detective controls detect and remove attackers from networks and systems as soon as possible.
5. Holistic approach to security, which includes due diligence on third party contractual obligations, accountability and liability.

FACTS AND FIGURES

Overall, global fraud rates have hit a near-20-year high, with 47% of companies reported to have experienced fraud over the past two years.

SonicWall Capture Labs Threat Researchers' key findings:

39% decline in malware (4.4 billion YTD); volume down for third consecutive quarter.

- 40% surge in global ransomware (199.7 million).
- 19% increase in intrusion attempts (3.5 trillion).
- 30% rise in IOT malware (32.4 million).
- 3% growth of encrypted threats (3.2 million).
- 2% increase in crypto jacking (57.9 million).

Attackers sit on a network for 60-130 days without being detected.

The Alert Africa team has assisted over 100 victims of cybercrime and harassment to date. The top scams reported are:

Internet fraud: sextortion, threats of sharing sensitive photos and scamming via online ads & other services.

Hacking/computer-intrusion scams: business emails compromised, social engineering and hacked PC accounts.

Source: Alert Africa (www.alertafrica.com), SonicWall Capture Labs Threat Research