Cyber resilience and cyber security

A holistic approach to digital security for medium-sized businesses

Recent security reports show an increase of cyber-attacks on African businesses. Amidst these threats, cyber resilience stands out as a proactive defense, helping businesses withstand, respond to and recover from security incidents.

Cybercriminals, including hacktivists and hackers, often act opportunistically unless they're executing a targeted or sponsored attack. Globally, many medium-sized businesses remain unaware of cybersecurity threats. This is due to their size and the assumption that, governments and medium to large-scale enterprises are the primary targets due to their perceived profitability and robust security measures.

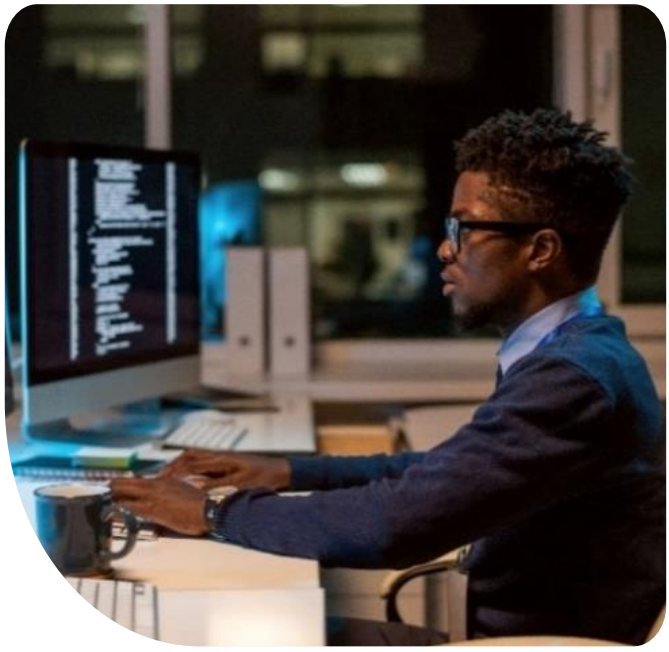
However, medium-sized businesses are vital to the economies of developing countries, representing the backbone of commerce. Despite their size, they possess valuable data that cybercriminals covet, including employee and customer records, financial information, and insights into business trends. As digital payment methods like mobile payments become increasingly integral to medium-sized businesses, cybercriminals are keen to exploit these vulnerabilities.

Most medium-sized businesses lack sufficient cybersecurity resources, sophisticated infrastructure and training to effectively manage and respond to cyber threats. This makes them appealing targets for cybercriminals.

"While threats are imminent to businesses and blocking them is critical, it is also essential to respond to an attack."

Cyber resilience

Cyber resilience is the ability of businesses to anticipate, withstand, respond, adapt, recover and limit the impact of security incidents. This involves deploying and optimising appropriate tools and processes. Cyber resilience also refers to strengthening cyber defense capabilities in the face of a cyber threat.



Key elements and attributes of cyber resilience

- Aligning business processes with information security and business continuity measures.
- Ensuring that business objectives prioritize the protection of Confidentiality, Integrity, and Availability (CIA Triad) of ICT infrastructure.
- Implementing swift response and recovery processes to effectively manage disruptions.

“According to studies by Grant Thornton eminent cyber advisors, most firms evaluate cyber posture based on the National Institute of Standards and Technology (NIST) cybersecurity framework. While 80% of the framework focuses on identification, protection and detection, only 20% is on response and recovery.”

Investing in cyber resilience

Recent security research reports show a rise in cyber-attacks on African businesses, impacting firms significantly. Medium-sized businesses, in particular, face breaches resulting in financial losses, disruptions, and reputational damage. This raises the question: why invest in cyber resilience?

Having a cyber resilience program helps businesses in numerous ways by addressing key questions such as:

- **Is our perimeter and network safe?**
- **Do we have a last line of defense in a cyber attack?**
- **What is our critical and sensitive data?**
- **What is our risk exposure?**
- **Are our backups safe and recoverable?**

Benefits of a cyber resilience program

It helps in blocking threats, early reconnaissance, and building and strengthening internal processes by defining roles and responsibilities in the organisation.

It enhances overall security strategy for improving governance.

With governments enforcing data protection privacy policies, there's a growing importance to safeguard data.

It focuses more on IT security resources and generates trust across clients, partners and vendor systems.

Improves compliance and governance while ensuring the safety of sensitive data.

Enhances business continuity during cyber-attacks, optimizing IT response and ensuring smooth daily operations.

Improving cyber resilience

Cyber resilience is a continuous process, and it comprises of numerous steps. The first is to ensure clear visibility into the business’s cybersecurity posture. Understanding cybersecurity posture through risk analysis is the key. This starts by identifying the assets, assessing individual risks associated with the asset and assessing vulnerabilities. Businesses need to quantify the risks from a monetary perspective, allowing the board or the stakeholders to prioritise risk mitigation actions based on the business impacts.

Cyber resilience will also involve significant investments in budgets, people, technology, training etc. Awareness of the cyber risks to the enterprise management and board helps buy into the overall strategic objectives.

Focus on cyber security fundamentals

Focusing on small but powerful security fundamentals through best practices is essential.

The key to security is being proactive and this can be achieved through investment in:

- Asset Inventory
- Endpoint Security
- Risk Quantification
- Email Security
- Ransomware Protection
- URL Filtering

Preventive measures that can be adopted include:

- Backup and DR Plans
- Security and Awareness Training
- Encryption

It is essential to have security management systems in place to mitigate the attack surface by incorporating:

- Data Leak Prevention Mechanisms (DLP)
- Identity and Access Management Solutions
- Multi-Factor Authentication
- Vulnerability and Patch Management tools
- Security Information and Event Management tools.

While some of the above are costly, minimum-security baseline configurations depending on the business, could help mitigate cyber threats.

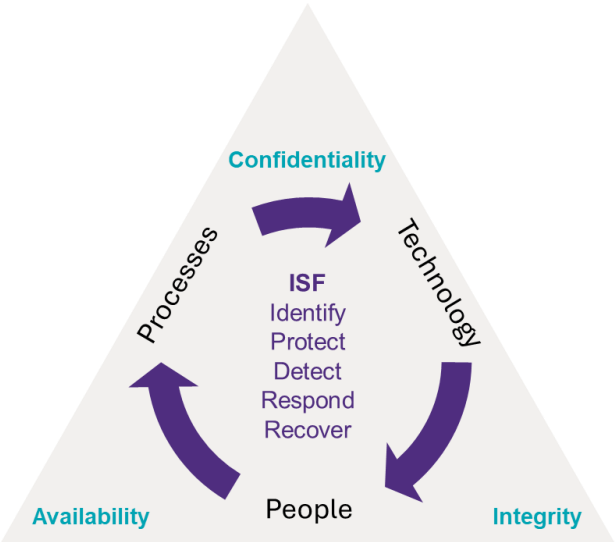
Why build a cyber resilience strategy?

A comprehensive cyber resilience strategy helps address security at all levels and proactively protect the firm's environment.

To protect the business environment, it is critical to develop a cybersecurity framework. The framework can be based on standards like NIST, ISO 27001, COBIT, etc.

The critical elements of an Information security framework include the following components:
Governance, Asset Management, Encryption, 3rd Party risk management, physical and environmental security, Security and Awareness training, Business Continuity Management, Incident Response, etc.

Information Security Framework



The core of the cybersecurity information security program is the People. Effective cybersecurity defense consists of a combination of people, processes and technology.

The difference between cyber resilience and cyber security

Cyber resilience is not cybersecurity but is complementary to cyber security. Cyber resilience combines operational resilience and cybersecurity, while cybersecurity is a defense strategy consisting of people, processes, and technology designed to protect people and systems.

How we can help

If you are seeking to enhance your organisation's cybersecurity or ensure regulatory compliance, consider partnering with us. Our team of dedicated IT professionals can help safeguard your organisation and mitigate cyber threats through several methods:

Assess Current Capabilities	
Risk analysis	1. Cyber Risk Analysis. 2. Risk Quantification
Cybersecurity Gap Assessments	3. Control Gap Assessment 4. Risk Assessment based on current and future use 5. Bridging Gaps and Control Testing
Design	
Program Design	6. Information Security Framework Program Development and Strategy
Implement Design	7. Governance – Development of Policies, Processes, Procedures etc. 8. Policy Management 9. Asset Management
Implement Security Controls	10. Information Security 11. Security Incident Management 12. Technical Controls Development 13. Security Awareness and Training
Monitoring, Response and Recovery	14. Monitoring Implementation Program. 15. Compliance testing. 16. Policies and Procedures

Key contacts

Aswin Vaidyanathan
Partner, Assurance
T (+267) 3707 107
E aswin.vaidyanathan@bw.gt.com

Sampath Kumar
Associate Director, IT Advisory
T (+267) 3707 136
E sampath.kumar@bw.gt.com

Leteng Basiamisi
Assistant Manager, IT Advisory
T (+267) 3707 160
E leteng.basiamisi@bw.gt.com