

STRATEGIC CYBER RESILIENCE

.....

A QUICK GUIDE FOR
BUSINESS LEADERS





Security incidents are inevitable, but successful businesses prioritise being **CYBER RESILIENT instead of scrambling to recover. Strategic cyber resilience involves several elements.**



1

PROACTIVE DEFENCE



Neutralise threats before they can do any harm. Treat regular assessments, threat intelligence and strong policies as your first line of defence.

QUICK RESPONSE



A well-structured incident response plan allows for quick detection and mitigation of risks. This ensures you are back to business in no time.

2



3

BUSINESS CONTINUITY

.....

Don't leave room for cyber attacks to disrupt your operations. Implement a strategic business continuity plan that includes backup and disaster recovery steps as well.



STAYING AHEAD OF THE CURVE

.....

Evolve with the threat landscape. Stay updated on the latest trends, learn from past incidents and continuously strengthen your defences.



4



5

SECURITY- CONSCIOUS CULTURE

.....

Train your employees to identify and manage risks. Foster a security-first culture.

COMPLIANCE

.....

Failing to meet regulatory requirements can attract hefty fines, lawsuits and damage to your brand's reputation.



6



**If a cyber incident struck today,
would your operations continue
uninterrupted?**

WE CAN HELP you build a security
plan based on the core elements of
strategic cyber resilience.

CONTACT US NOW!