TECH TITAN

PREPARE · CONTAIN · RECOVER

Gun Chun Len

Resilience begins before ransomware strikes

Managing Director & CEO · Tech Titan Group

Connecting people, endpoint visibility, incident response and recoverable data into one readiness programme.

Connect on LinkedIn

THE PERSPECTIVE

Minutes matter. Preparation matters more.

PREVENT | DETECT | CONTAIN | RECOVER

Practical security leadership connects technology decisions to business outcomes.

THE STRATEGIC CONTEXT

Ransomware is an operational crisis, not only a malware event

An attack can disrupt services, compromise identities, expose data and place leadership teams under immediate pressure.

No preventive layer is perfect. Readiness depends on recognising suspicious behaviour early, containing movement and restoring trusted operations.

Gun Chun Len's resilience perspective brings technology, specialist response and business preparation into the same plan.

01

THE OPERATING AGENDA

The ransomware readiness cycle

01

REDUCE

Close common entry paths

Strengthen endpoints, identities, email security, patching and user awareness.

02

DETECT

See attacker movement sooner

Monitor endpoint and user behaviour for activity that traditional signatures may miss.

03

CONTAIN

Limit operational damage

Isolate affected systems, protect privileged access and coordinate incident decisions quickly.

04

RECOVER

Restore trusted services

Use protected backups, tested procedures and clear priorities to return critical operations safely.

02

THE LEADERSHIP LENS

Leadership decisions before an incident

AUTHORITY

Know who can make urgent decisions

Define technical, legal, communication and business owners before pressure arrives.

EVIDENCE

Preserve what investigation needs

Plan logging, forensics and documentation alongside containment.

CONTINUITY

Agree what must recover first

Business priorities should determine recovery sequence and acceptable downtime.

FROM STRATEGY TO ACTION

Run a readiness programme, not a checklist

Ransomware preparedness improves when controls and people are exercised together under realistic conditions.

Explore Managed Detection & Response

01

Review the most likely entry routes

Assess endpoint, credential, remote access and social-engineering exposure.

02

Test isolation and escalation

Confirm teams can contain affected assets and reach decision-makers quickly.

03

Validate clean recovery

Ensure backups are protected, usable and aligned to critical-service priorities.

04

Exercise executive communications

Rehearse internal, customer and regulatory communication responsibilities.