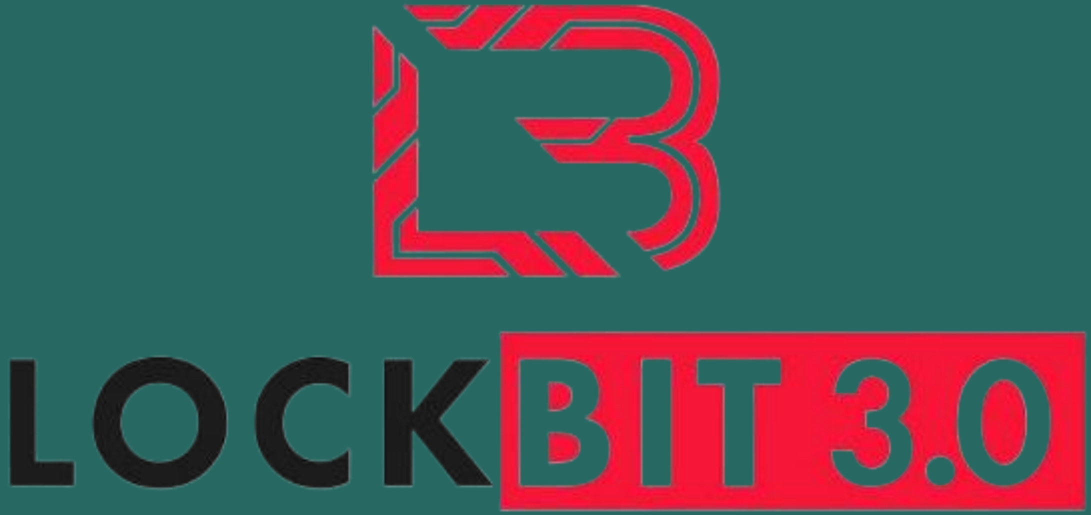
evolvenorth

Prepare to fail

evolvenorth

Why build a Cyber Incident Response Plan?

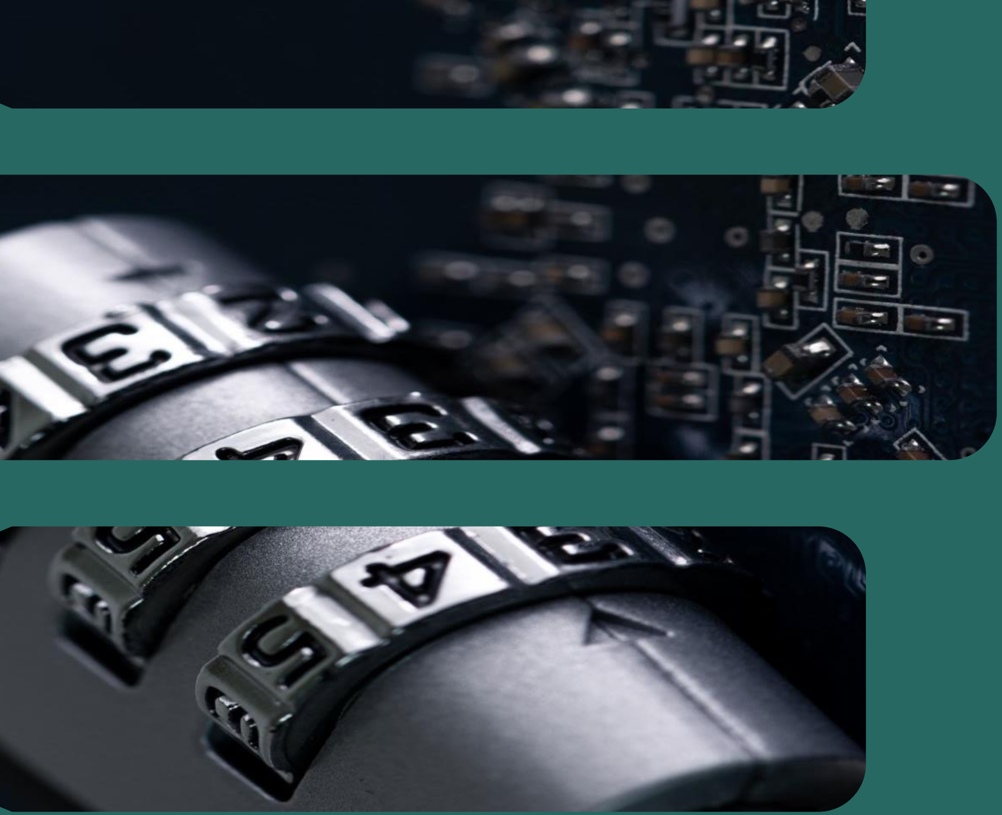
Because of this lot



Firewall Daily

BlackCat Ransomware Data Exfiltration Tool Upgraded

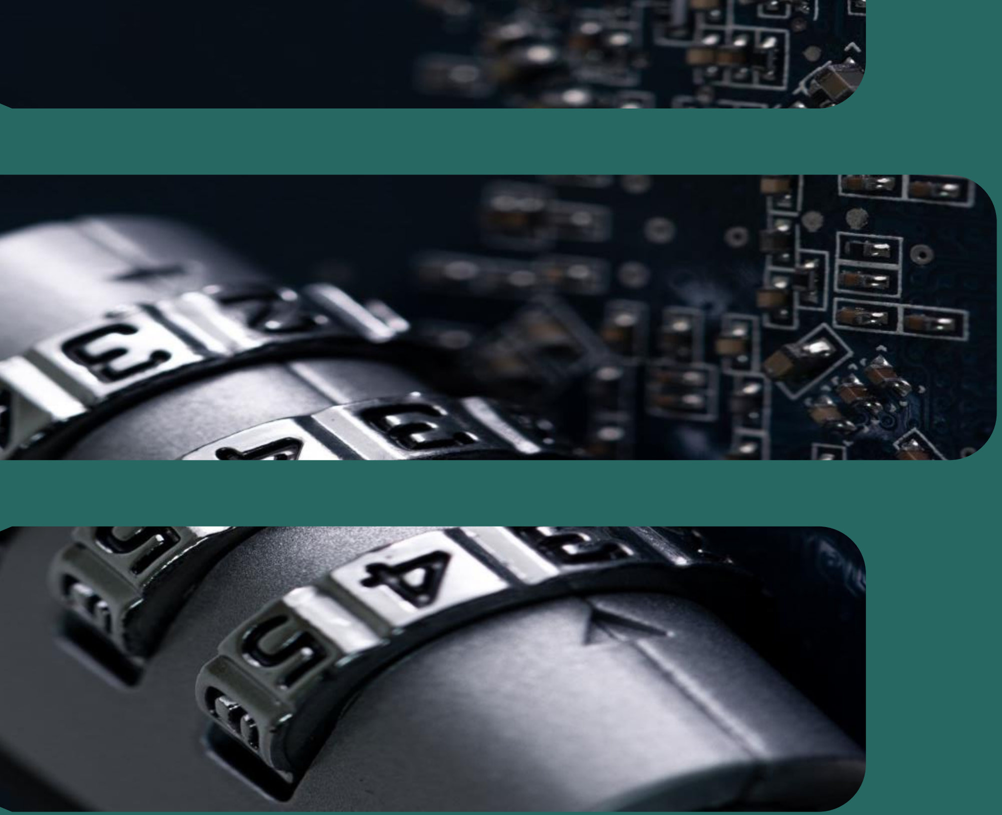
THE CYBER EXPRESS



You are more likely to sustain a Ransomware incident via your third-party supply chain that directly on your business.

All you may have left to manage that incident is your communications tools............

You need a whole business response plan.



What does a CIRP deliver –

- Clear ownership of response tasks
- Pre-defined lines of communications
- Pre-set “back channel” communications
- Communications plans (all stakeholders)
- Functional Department response plans
- Playbooks (how you cope)
- Defined systems dependencies.
- Risk acceptance

A business that understands its risks.

Cyber Incident Response Plan - Build Process

evolvenorth

Assemble the CIRP Team

Appoint CIRP Team Leader

Kick Off Meeting

Whole Business Team

Functional Department Representation

Review System Dependencies

Create Systems Register

Risk Assess

Capture Actions inc.
Department CIRP
Remediation
Due Diligence
Contract Review
Risk Acceptance

Draft CIRP

Identify Stakeholders (third parties etc)

Add System Dependencies

Draft Department Level CIRPs

Agree Response owners

Link to BCP/DR/Breach Procedure etc

Tabletop Test

Revise CIRP

Revise Department CIRPS

Repeat Annually

Update CIRP

> "The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved."

Confucius

evolvenorth