Protect against the **cyber kill chain**

7 steps to proactively protect your business

Cybersecurity threats can feel overwhelming, but understanding the **Cyber Kill Chain** — a widely recognised model illustrating the typical progression of cyberattacks — can help your IT team **proactively** minimise risks.

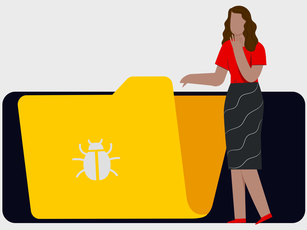
While not every attack strictly follows these steps, this framework gives you valuable context on how cyber threats typically unfold and provides practical actions you can take to strengthen your defences.

Step 1: Reconnaissance

Attackers gather information about your business to identify vulnerabilities.

Protect yourself:

- Limit publicly available sensitive information.
- Regularly audit your digital footprint.
- Educate your team on oversharing online.



Step 2: Weaponisation

Attackers craft malicious payloads specifically tailored to exploit discovered vulnerabilities.

Protect yourself:

- Deploy advanced threat detection solutions.
- Regularly update and patch software.
- Monitor threat intelligence feeds for emerging threats.

Step 3: Delivery

Malicious payloads reach your organisation, often through phishing or other deceptive methods.

Protect yourself:

- Implement robust email security solutions.
- Train staff regularly on recognising phishing attempts.
- Set strict email filtering policies.

Step 4: Exploitation

Attackers execute the malicious payload to breach your defences.

Protect yourself:

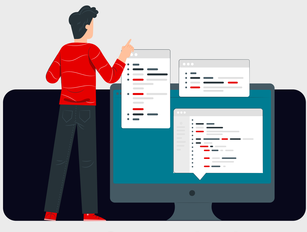
- Use endpoint detection and response (EDR) tools.
- Restrict admin privileges to limit possible damage.
- Regularly conduct penetration tests.

Step 5: Installation

Malware or backdoors are installed to maintain persistent access.

Protect yourself:

- Deploy advanced antivirus and anti-malware software.
- Establish endpoint security measures.
- Monitor network activities for unusual behaviours.



Step 6: Command and Control (C2)

Attackers establish communication channels to control compromised systems.

Protect yourself:

- Implement network segmentation.
- Use firewalls and intrusion detection systems.
- Regularly analyse network traffic for anomalies.

Step 7: Actions on objectives

Attackers execute their final goals, such as data theft or disruption.

Protect yourself:

- Encrypt sensitive data both at rest and in transit.
- Ensure frequent backups and recovery procedures.
- Conduct regular security audits and response drills.

Conclusion

While this framework equips your internal IT team with some sort of strategy, some protections listed require specialised software or external expertise.

If you need assistance with any step listed, you can click here to request a call. **Vodacom Business** is ready to help secure your business.

vodacom business