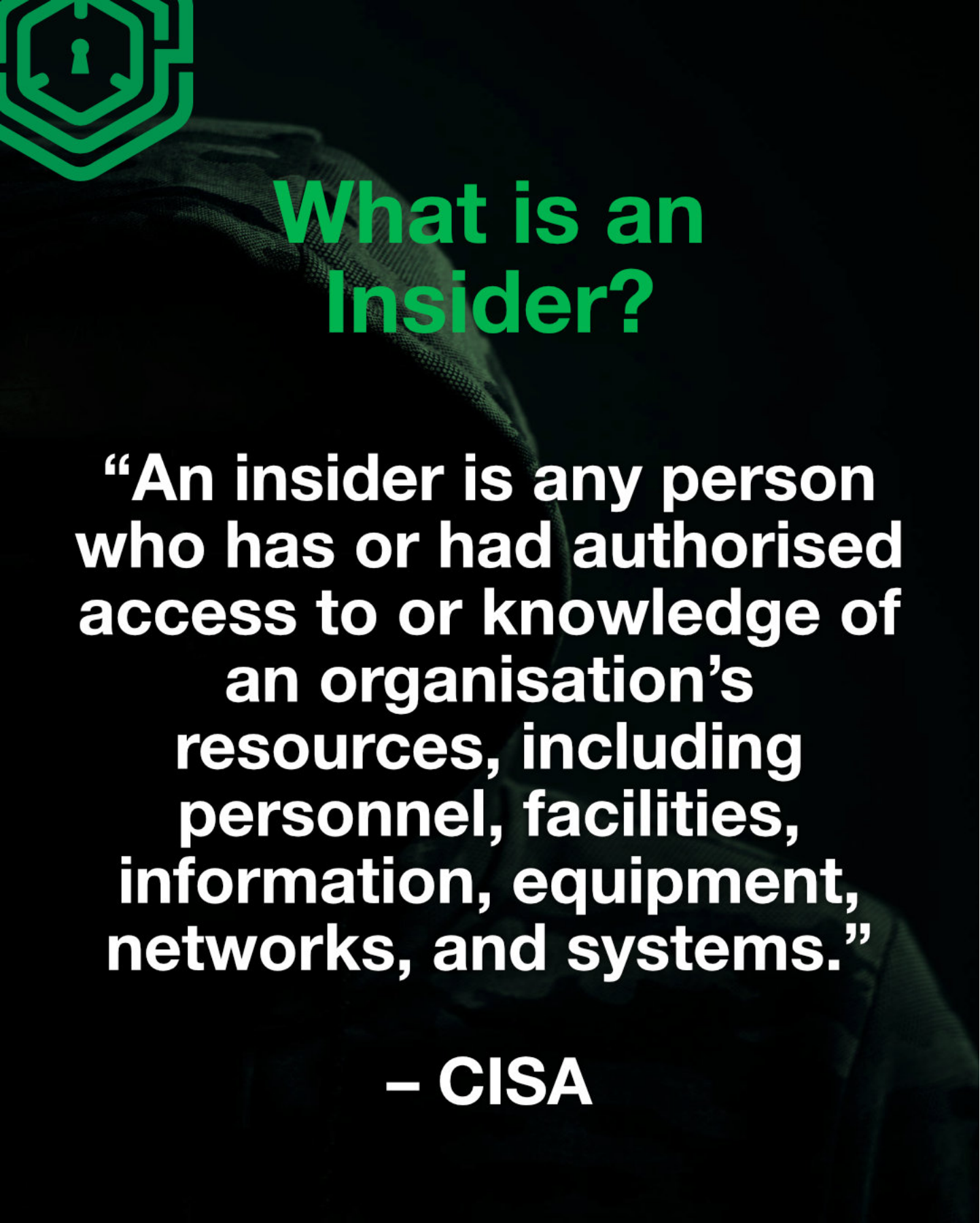
What is an Insider Threat?

Unintentional, intentional, negligent, accidental, malicious, collusive... Know your risks!


Insider Threats
Insider threats are on the rise and its critical to know exactly what they are so you can defend against them.

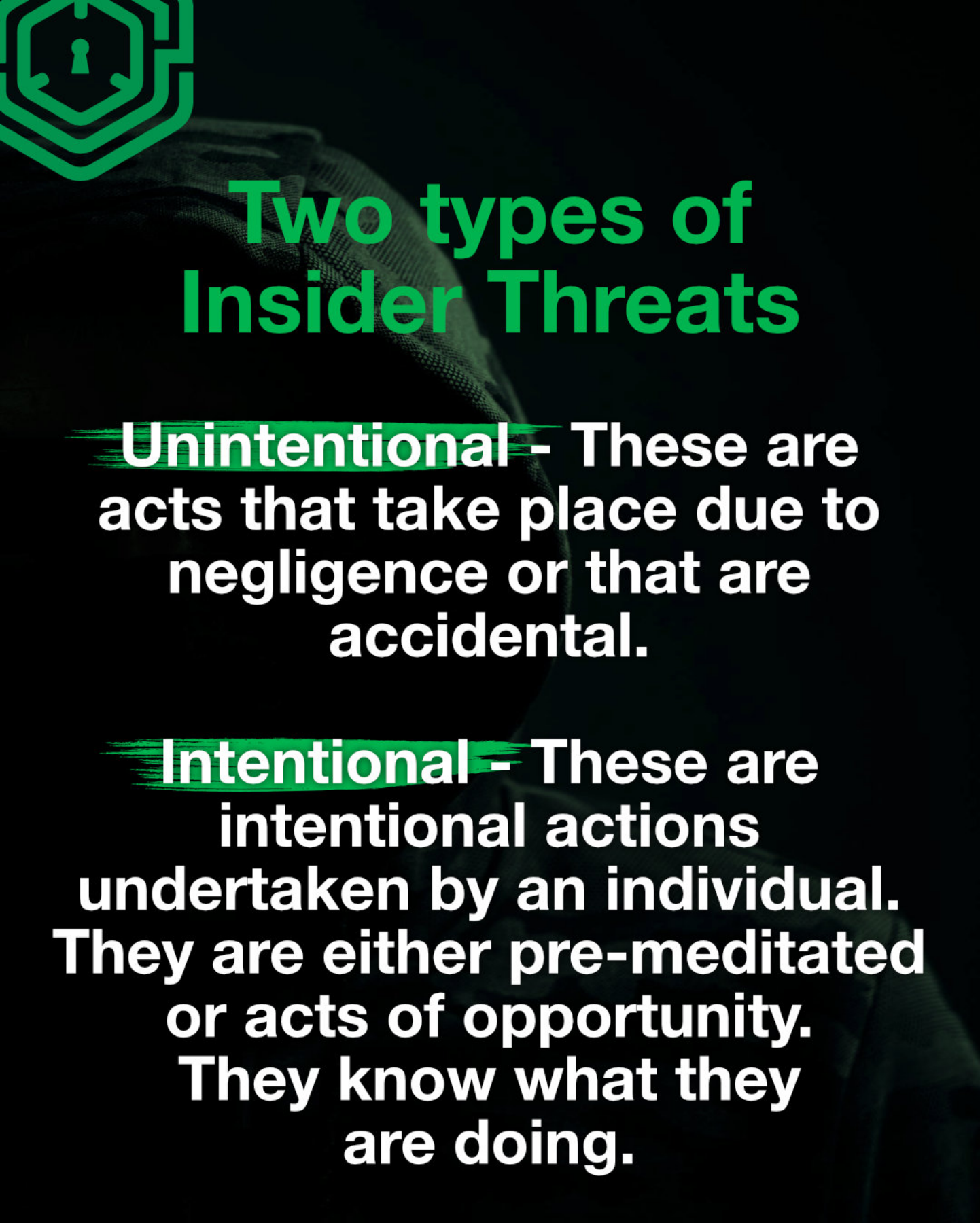


What is an Insider?

"An insider is any person who has or had authorised access to or knowledge of an organisation's resources, including personnel, facilities, information, equipment, networks, and systems."

– CISA


What is an Insider Threat?
“the threat that an insider will use their authorised access, intentionally or unintentionally, to do harm to the department’s mission, resources, personnel, facilities, information, equipment, networks, or systems.”
- CISA


Two types of Insider Threats
Unintentional - These are acts that take place due to negligence or that are accidental.
Intentional - These are intentional actions undertaken by an individual. They are either pre-meditated or acts of opportunity. They know what they are doing.

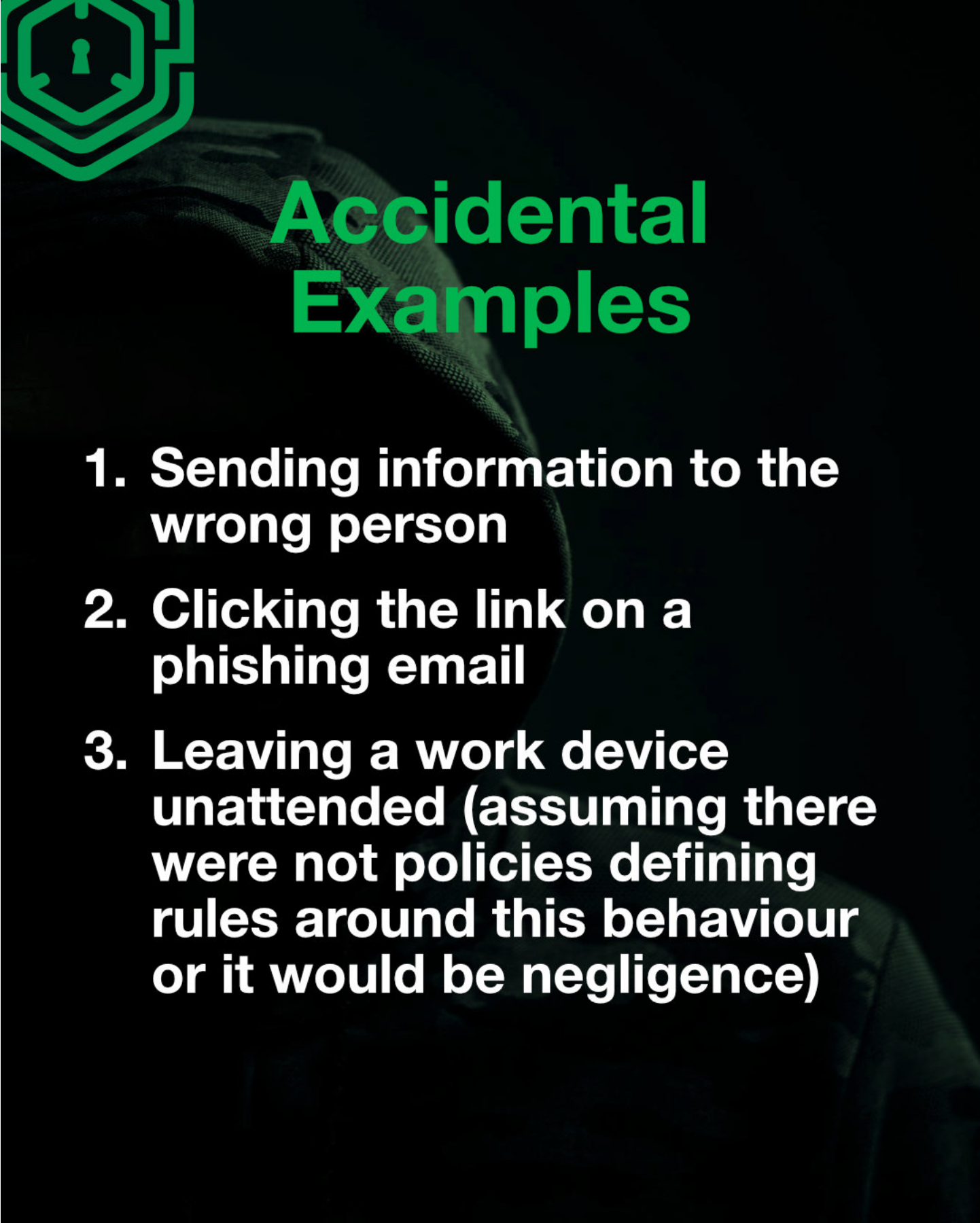
Unintentional Insider Threats

Negligent - Covers actions where an individual was either careless or disregarded policies, processes, or procedures.

Accidental - When an individual unintentionally causes a security incident - it was purely accidental.

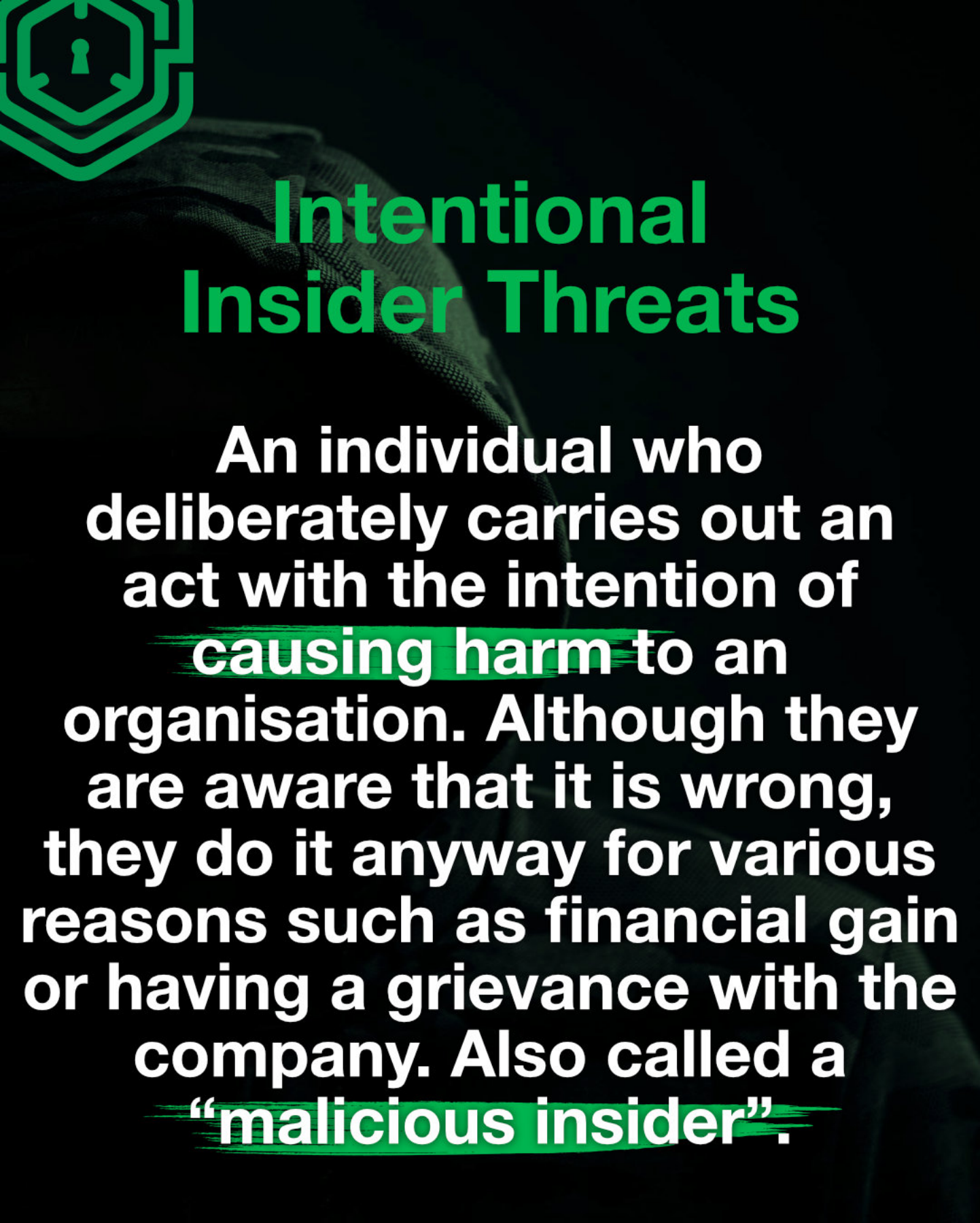
Negligent Examples

1. Letting someone into a restricted area
2. Not reporting a lost device containing business data
3. Unsanctioned cloud services or applications - 'Shadow IT'
4. Not installing updates or patches when requested
5. Allowing someone else to use your credentials



Accidental Examples

1. Sending information to the wrong person
2. Clicking the link on a phishing email
3. Leaving a work device unattended (assuming there were not policies defining rules around this behaviour or it would be negligence)



Intentional Insider Threats

An individual who deliberately carries out an act with the intention of causing harm to an organisation. Although they are aware that it is wrong, they do it anyway for various reasons such as financial gain or having a grievance with the company. Also called a "malicious insider".

Intentional Examples

1. Motivation to 'get even' because of some grievance
2. Theft of information for financial gain
3. Theft of information for career progression - to a competitor
4. Theft of information for social reasons - whistleblowing
5. Sabotaging equipment
6. Collusive threats - nation state


So how do I
defend against
insider threats?

1

Asset Register

With a documented asset register in place, you know what you are protecting, can define controls to ensure each asset is adequately protected, and can monitor critical assets for data exposure or exfiltration.

2

Threat Landscape

Knowing what threats you face is critical in being able to defend against them.

You also need to identify threats that could target specific assets or data you hold.

3

Detection Strategies

Based on your defined assets and threat landscape, what do you need to monitor for and how will this be achieved?

This will speed up response time and help reduce any data exposure.

4

Incident Response

What happens if or when you have an incident?

You must know what to do if your data is breached, but also when an issue is detected, its critical to be able to respond in a timely manner to reduce exposure time or data being exfiltration.

5

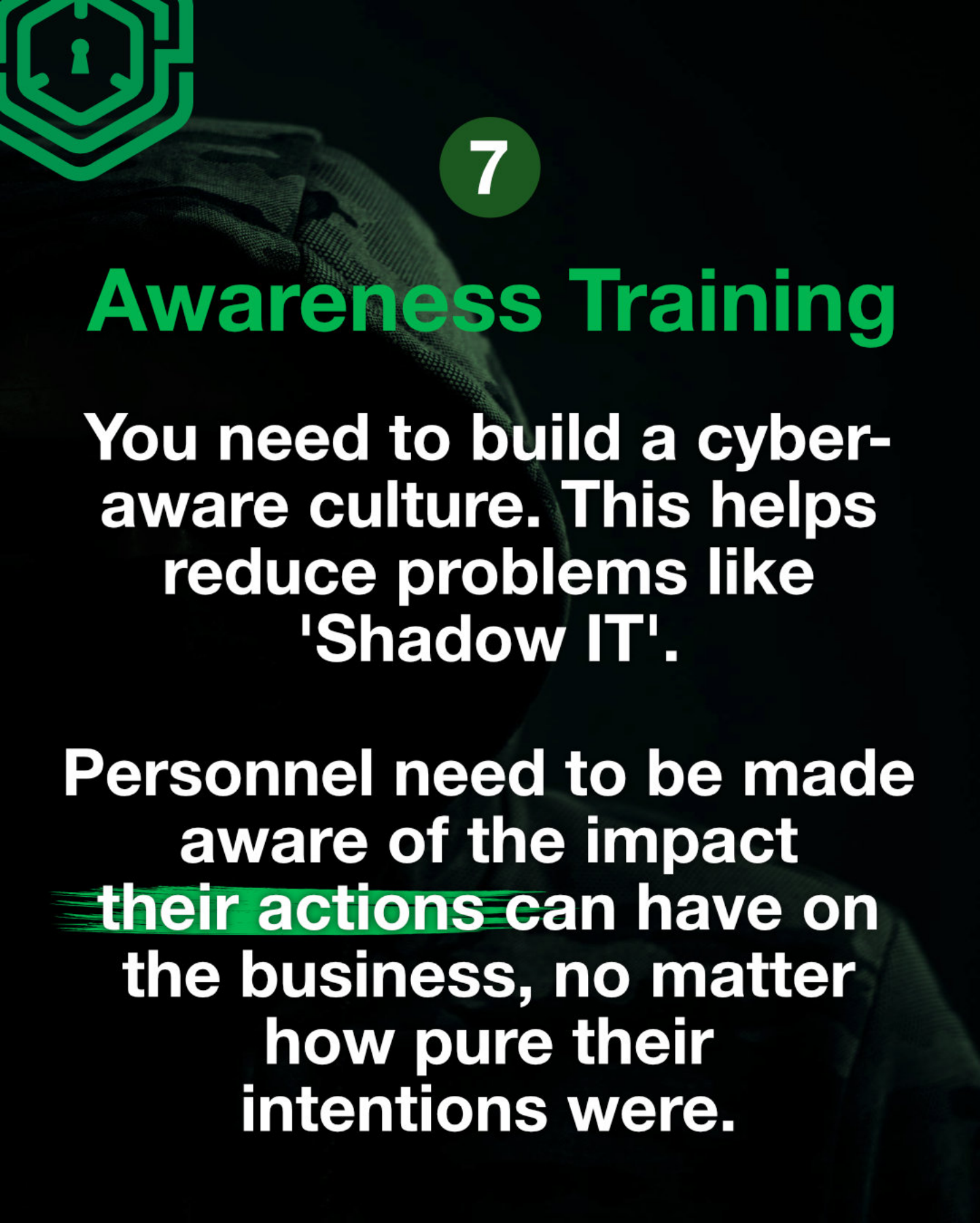
Reporting

Develop a culture that encourages reporting of potential threats, weaknesses in security controls, indicators of a potential insider threat, or any other relevant concern, and have clear and easy processes for personnel to report them.

6

Threat Management Team

This could be the same team that is part of your incident response planning and management, but needs to be able to assess and respond to actual and potential insider threats.



7

Awareness Training

You need to build a cyber-aware culture. This helps reduce problems like 'Shadow IT'.

Personnel need to be made aware of the impact their actions can have on the business, no matter how pure their intentions were.

Want More Information?

Read more on our blog about insider threats, their motivations, how they exfiltrate information, and how to defend against them!

https://morrisec.com.au/insights

MORRISEC