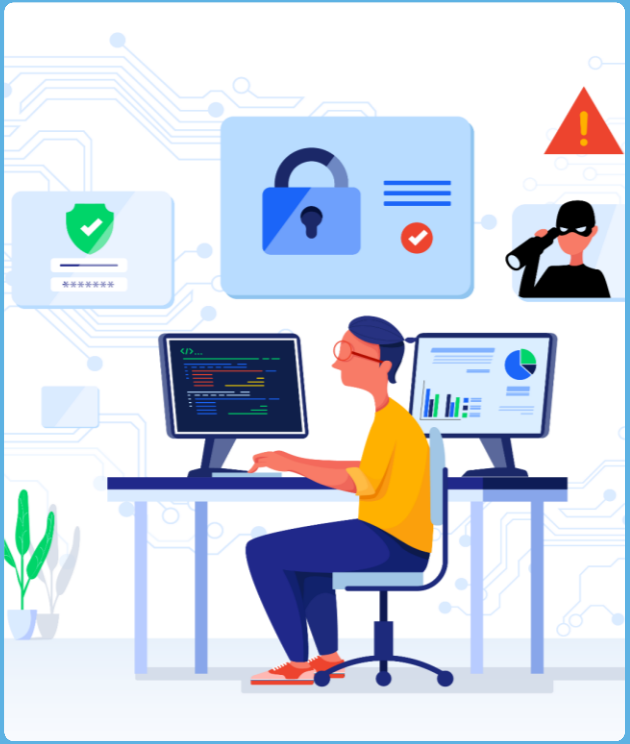
UNISYS | Securing Your Tomorrow®

Increasing cyber resilience

Gergana Winzer



COVID19 has created many concerns for employees and changed the way we work and we weren’t exactly ready…

- 68% of Australians were WFH in the midst of the pandemic
- 42% of Australian businesses expect to permanently maintain WFH workforce

Cyberattacks will still happen
Regulators will still regulate

Recent victims of cyber attacks

BLUESCOPE
STEEL

Service
NSW

Have I been hacked?

How to stop it?!

1. Do your research

2. Take an attack based approach to Security

3. Incident Response Planning

1. Cover the Basics

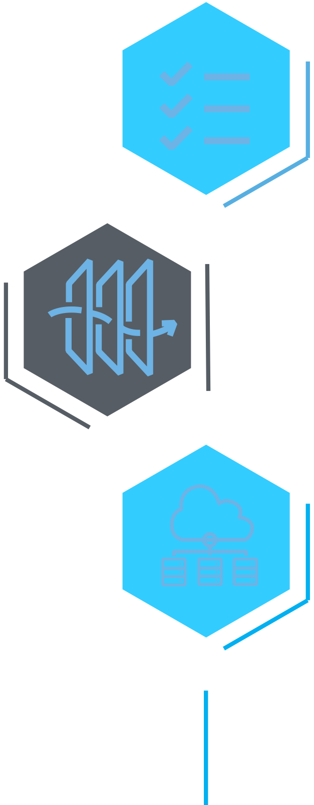
2. Perform a Compromise Assessment

Perform Threat Hunting and Red Teaming. Monitor the Dark Web and Obtain Targeted Threat Intelligence

3. Get Strategic

UNISYS | Securing Your Tomorrow®

Anatomy of a cyber attack



Data Exfiltration

Once found the data, the attacker will copy it to another location under their control outside the network.

Local machine takeover + Privilege escalation

The Attacker will look at taking over control of the infected device. Once obtained the attacker will look to move laterally in the network to search for data.

Email/ Web attack + malware download

Email with a link or an attachment that will either contain or direct a user to malware. The user opens or clicks and downloads the malware

The path to resilience can be zero trust

Know your network

Know & control your network

Visualize, model and design informed security

Easy Zero Trust

Reduce your attack surface across cloud, on-premises, devices and things

Encrypt data in motion

Protect communications with strong encryption

Cloak critical assets

Cryptographically hide critical assets from adversaries

Irrefutable identity

Authenticate with physical and behavioral biometrics

Enable adaptive security

Integrate existing security tools to correlate, detect and respond

Thank You

Any Questions?