UD 24

Secure and Compliant

A guide to mitigating the latest cyber threats

James Rentoul

Security Manager

"Security is not a product, but a process." –

Bruce Schneier Fellow at Berkman Klein Centre of Internet and Society

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." –

Stephane Nappo Global CISO Groupe SEB

“The only secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards”- Gene Spafford – Professor at Purdue University and US Government advisor

Cost of Breaches Globally

£6.3Tn

Cost to the world in 2023

£99Mn

2019 fine to Marriott International for GDPR

£8.2Tn

Cyber cost to the world in 2025

£3.51Mn

Average global cost of data breach

£13Mn

Fines to the UK corps in 2023 imposed by ICO

Threats

What are the threats the SOC are seeing

- Business Email Compromise
- Teams phishing
- Data theft
- Third party compromise

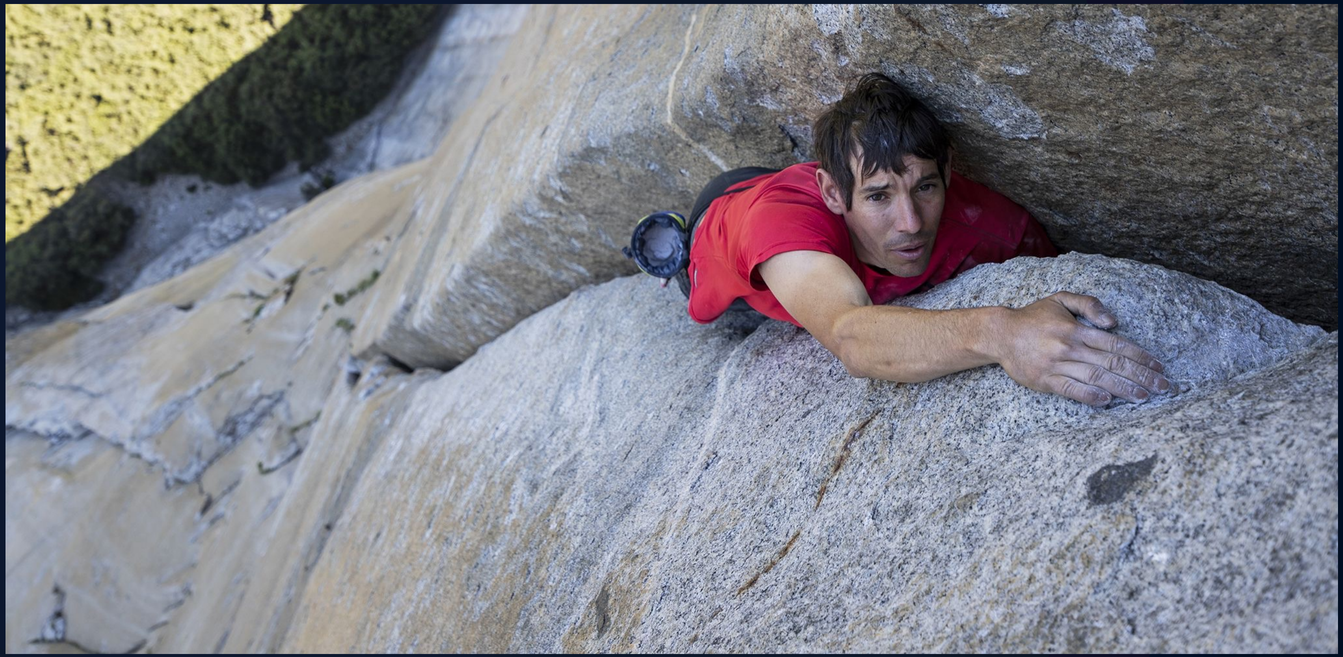
- Malware
- Ransomware
- Vulnerability Exploitation
- Code

Where are these threats coming from

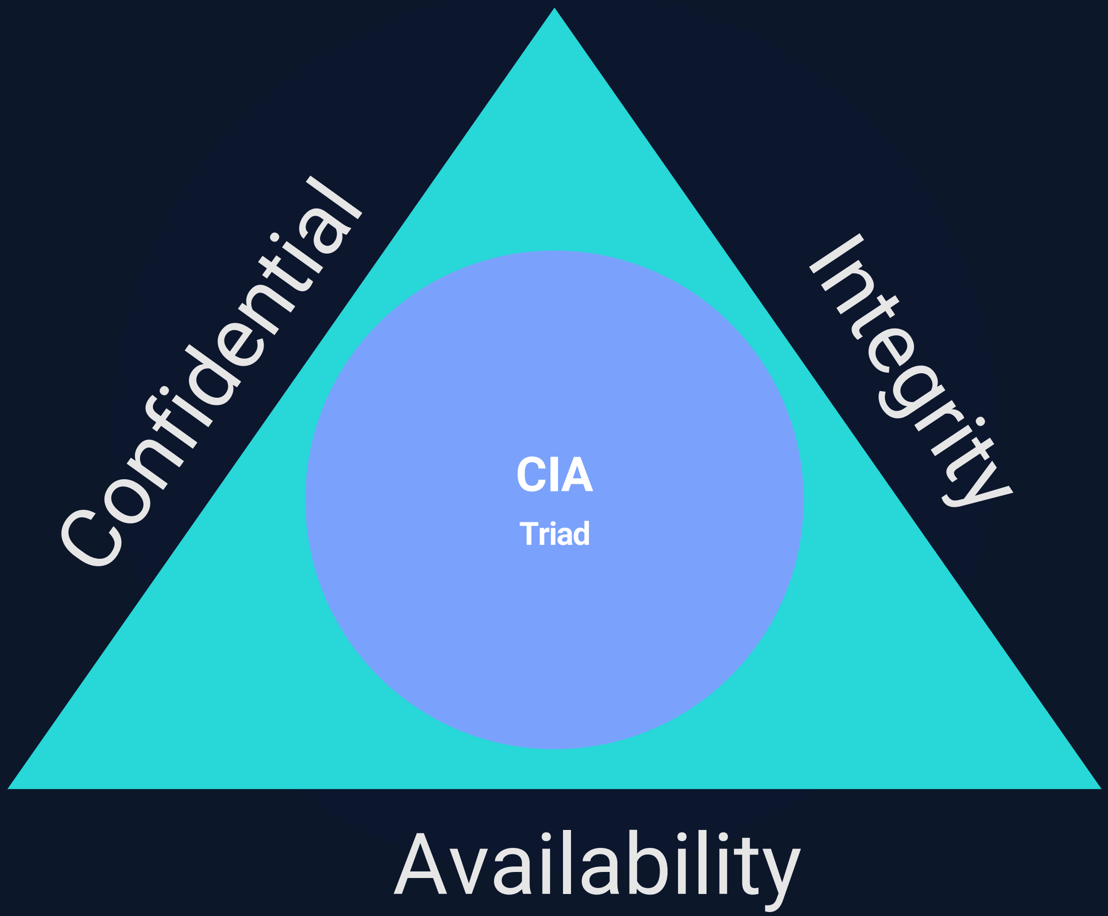
- Russia
- India
- Africa – Nigeria
- US
- UK

- Process
- Environmental
- Insider

Risk



Information Security



Frameworks

01

Cyber essentials

02

ISO:27001:2022

03

ISO:27002:2022

04

NIST 2.0

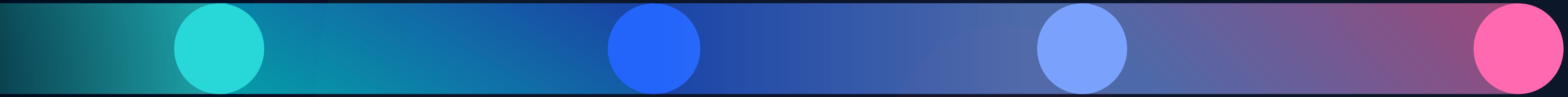
05

SOC 2

06

PCI

Pilers of Cyber security



Prepare

How do you prepare for an attack? What tooling and policy do you have in place

Detect

How do you detect an attack. This will require Tooling and Staff

Respond

How do you respond to an attack, how do implement your policies

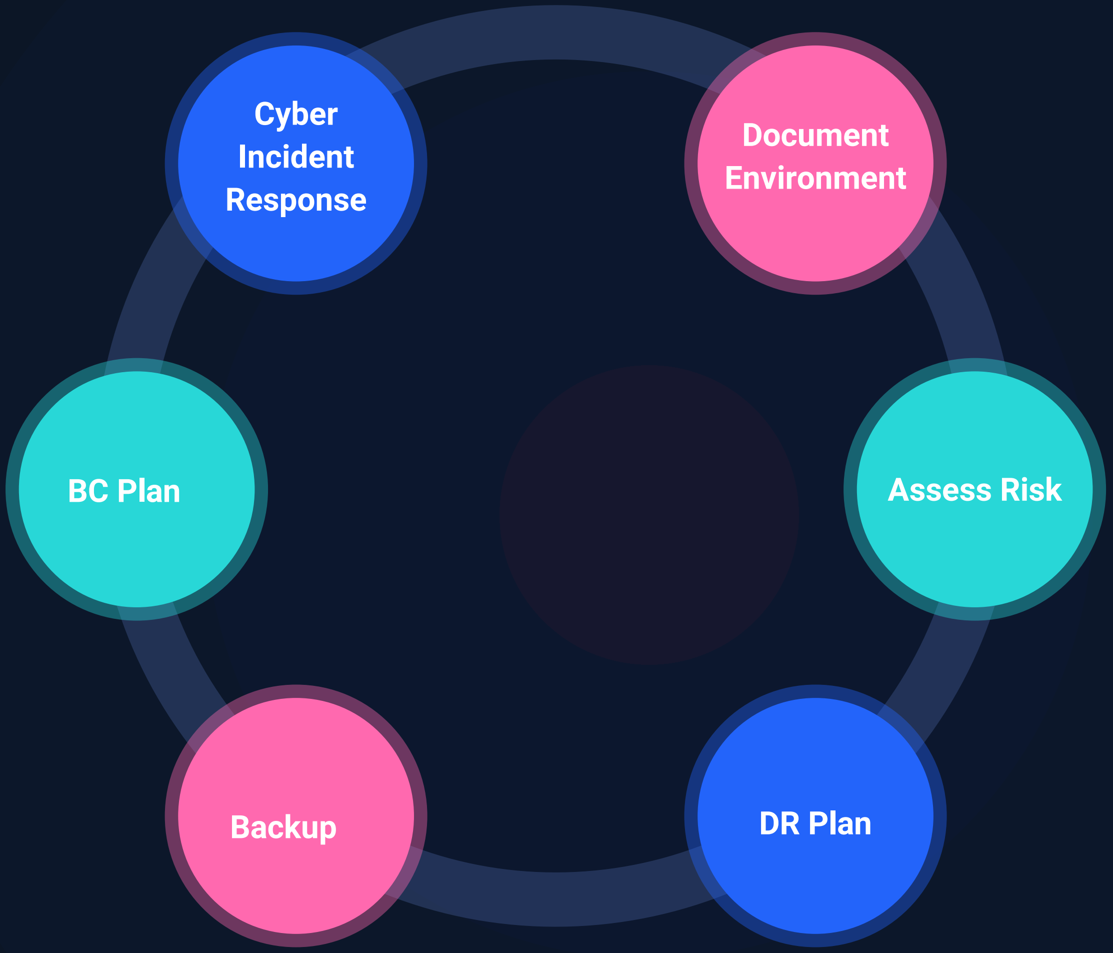
Recover

Implementing the policies defined in the Prepare stage.

Prepare

What is required to be prepared for a cyber attack

Prepare


Cyber Incident Response
Document Environment
Assess Risk
DR Plan
Backup
BC Plan

Layered approach

Edge Security

Email filtering

MFA

Firewalls

Vulnerability

Patch for security updates

Monitor for new Vulnerabilities

Reduce attack surface where you can't patch

Data Protection

Know your data and its Sensitivity.

Create RBAC

Data Loss Prevention

Detect

How do you know an attack is happening

Layered approach

NDR

Network Detection

Canary tokens

XDR

Tooling that allows greater visibility of Users, Devices, email and access

SIEM

Monitor your estates Logs

Full visibity of your estate

Alert to unusual behaviour

Ingest and utilise threat intell

Respond

How do we get rid of the attacker

Respond

Step 1

Step 2

Step 3

Incident Management

- What’s happened
- What playbook are we using

Incident Analysis

- Forensics
- What is the breach
- Log review

Communicate

- Staff
- Clients
- Partners

Recover

How do you get back up and running

Recover

Step 1

Step 2

Incident Recovery Plan Execution

- DR Plans
- Access
- Secure clean network
- Scan

Incident Recovery Communicate

- Staff
- Clients
- Partners

Cyber News

Lockbit

- RSAAS
- Affiliate Program
- Taken down by NCA and 10 partners
- A large take down of Infrastructure
- Backup within 1 week

Medibank Private

- Australian Government response
- 9.7 Million personal details
- Sanctions
- Financial fines and jail time for dealing with Aleksandr Ermakov
- Photo published

Questions

Thank You.