THREAT
LANDSCAPE

Attacks against countries, organisations and individuals are on the increase

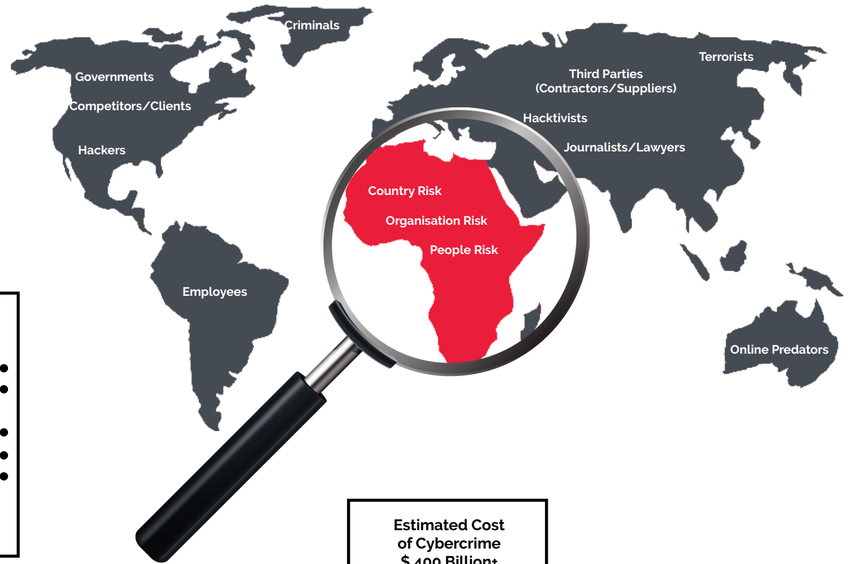
Cybercriminal Code of Ethics

"If what you put on the Internet is worth anything, one of us will try to hack or steal it."

"If we can't sell it, we'll just encrypt it or erase it so you can't use it either, or simply post it online to ruin your reputation."

"If you don't care about protecting your stuff from the likes of us, don't worry: You're our favourite type of customer!"

Estimated Global Spend $ 120 Billion+



Estimated Cost of Cybercrime $ 400 Billion+

ORGANISATIONAL RISKS

- ORGANISED CRIME SYNDICATES
- OPPORTUNISTIC CRIMINALS
- ONLINE PREDATORS
- THUGS
- HACKTIVISTS

- MALICIOUS SCANS
- THEFT OF SENSITIVE INFORMATION
- FRAUD
- BUSINESS DISRUPTION
- INFORMATION LEAKS

COUNTRY RISKS

- STATE SPONSORED ATTACKS – MILITARY / INTELLIGENCE
- MERCENARY / BLACK HAT HACKERS
- TERROR GROUPS
- HACKTIVISTS

- INTELLIGENCE GATHERING
- INTELLECTUAL PROPERTY THEFT
- PROPAGANDA & MISINFORMATION
- REPUTATIONAL HARM
- CRITICAL INFRASTRUCTURE DAMAGE
- DISTRIBUTED DENIAL OF SERVICE
- FUNDRAISING

PEOPLE RISKS

- DISGRUNTLED EMPLOYEES
- RECKLESS EMPLOYEES
- HACKTIVISTS
- UNAWARE EMPLOYEES
- INFORMATION PARTNERS

- COLLUSION
- SCAMS
- SOCIAL ENGINEERING
- SPEAR PHISHING
- INFORMATION LEAKS
- EXTORTION
- DARK WEB ACTIVITY
- RANSOMWARE