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 cost of cybercrime $400 Billion+”

THREAT LANDSCAPE

Estimated Global Spend $120 Billion+

COUNTRY RISKS

- State Sponsored Attacks – Military / Intelligence
- Mercenary / Black Hat Hackers
- Terror Groups
- Hacktivists

PEOPLE RISKS

- Disgruntled Employees
- Reckless Employees
- Hacktivists
- Unaware Employees
- Information Partners

ORGANISATIONAL RISKS

- Organised Crime Syndicates
- Opportunistic Criminals
- Online Predators
- Thugs
- Hacktivists

MALICIOUS SCANS  THIEF OF SENSITIVE INFORMATION  FRAUD  BUSINESS DISRUPTION  INFORMATION LEAKS

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

DISGRUNTLED EMPLOYEES  RECKLESS EMPLOYEES  HACKTIVISTS  UNAWARE EMPLOYEES  INFORMATION PARTNERS

www.wolfpackrisk.com