THREAT LANDSCAPE CHART

ATTACK ACTOR
Who is attacking

Attackers can range from individuals to national governments. Who the attacker is can define their likely objective(s) and capabilities. For example, nation-states are likely to have more resources than criminal opportunists and may pursue political goals over financial gain.

Attack Actor Examples:
- Individuals
- Hacktivists
- Criminal Opportunists
- Organized Crime Syndicates
- Terrorists & Affiliates
- Corporations
- State-Sponsored Actors
- Nation States

INTENT
Attackers' Objective(s)

Attack actors are motivated by different goals. Who they attack and the assets they target will depend upon their objective(s). Broadly speaking, attackers' objectives are often either economic and/or political in nature.

Threat Objective Examples:
- Infiltration
- Espionage
- Disruption of Services
- Data Theft
- Data Manipulation
- Data Destruction
- Financial Theft
- Physical Destruction

For more information, please view the Likelihood spider graph.

CAPABILITY
Attackers' available resources and methods

Attackers range in sophistication. The intelligence, reconnaissance, and technical means available to an attack actor will determine the types of cyber attacks they can launch. More targeted cyber attacks generally require more resources.

Attack Method Examples:
- Malware
- Denial of Service
- Drive-by Downloads
- Spam & Phishing
- Botnets
- Worms & Trojans

For more information, please view the Likelihood spider graph.

RISK
Vulnerability to cyber attack

Vulnerability to cyber attacks depends on an organization's attack surface—all points attackers can exploit to launch an attack—and the technical and operational defenses in place.

Attack Surface Examples:
- Insiders
- Poor cyber hygiene
- Technical vulnerabilities existing in hardware, firmware, and software
- Exploitation of public-facing websites and/or social media
- Exploitation of third-parties such as suppliers, vendors, or partners

For more information, please view the Risk spider graph.

IMPACT
The extent of possible damage

The costs incurred by a cyber attack and the extent of possible damage can range from immediate, direct costs to long-term consequences affecting the targeted organization and external actors.

Attack Impact Examples:
- Direct cost of the attack (investigation, disruption of operations, mitigation of damages)
- Second- and third-order effects on business operations and key stakeholders
- Damage to long-term strategic interests

For more information, please view the Impact spider graph.