Cyber threat landscape & 2026 priorities

Sarah Armstrong-Smith

Key Trends

More complex, highly adaptive, and aimed at the human

01

State Actors

National, international. Use of proxies, and influence operations to sway public opinion

02

Ransomware

More elusive, higher stakes, willing to take more risk. Targeting critical infrastructure

03

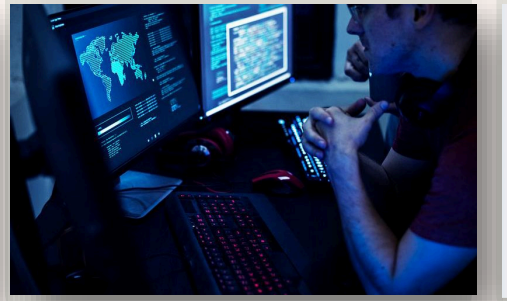
Supply Chain

Interconnectivity across trusted channels, broad scale attacks, crippling the economy

04

Cyber Mercenaries

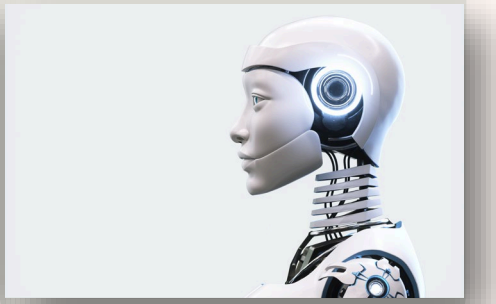
Custom-made services, highly specialised weapons of mass disruption / destruction



05

AI

Becomes a force multiplier for attackers and defenders, in an information war



Operating in the grey zone

- Persistent, low-cost scalable influence operations
- Synthetic media used to desensitise and disseminate
- Deep fakes, disproportionately impact women and children
- AI slop exhausts detection and alerting tools
- Destabilise government, reshape policy, change the long-term outlook

Cyber is a geopolitical weapon of war and influence

Cyber Mercenaries: crimes against humanity

- Commercial spyware for mass surveillance
- Packaged intelligence on targets
- Tracking and location data
- Predictive algorithms
- Comms interception
- Mass sabotage

Now combine, and put them in the hands of criminals

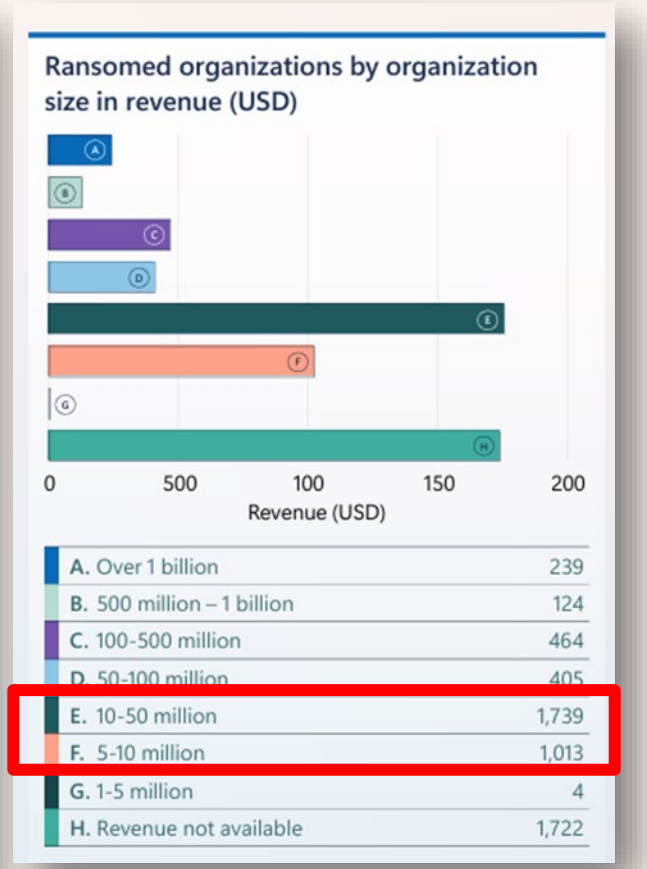
Scaling for impact

Downstream - niche and specialist vendors

Midstream - the sweet spot for extortion

Upstream - managed service providers

- Abuse remote infrastructure management
- Disconnecting updates and pipelines
- Intercept and disrupt backup and comms



Source: Microsoft Digital Defense Reports 2025

Subversion & Evasion

- Building resilience into underpinning infrastructure
- Use of proxies to hide attribution
- Multi-layering of command and control
- Redistributing workloads
- Multi-stage attack paths over extended period

Not breaking in, but blending in

Insiders – the soft target

Home grown

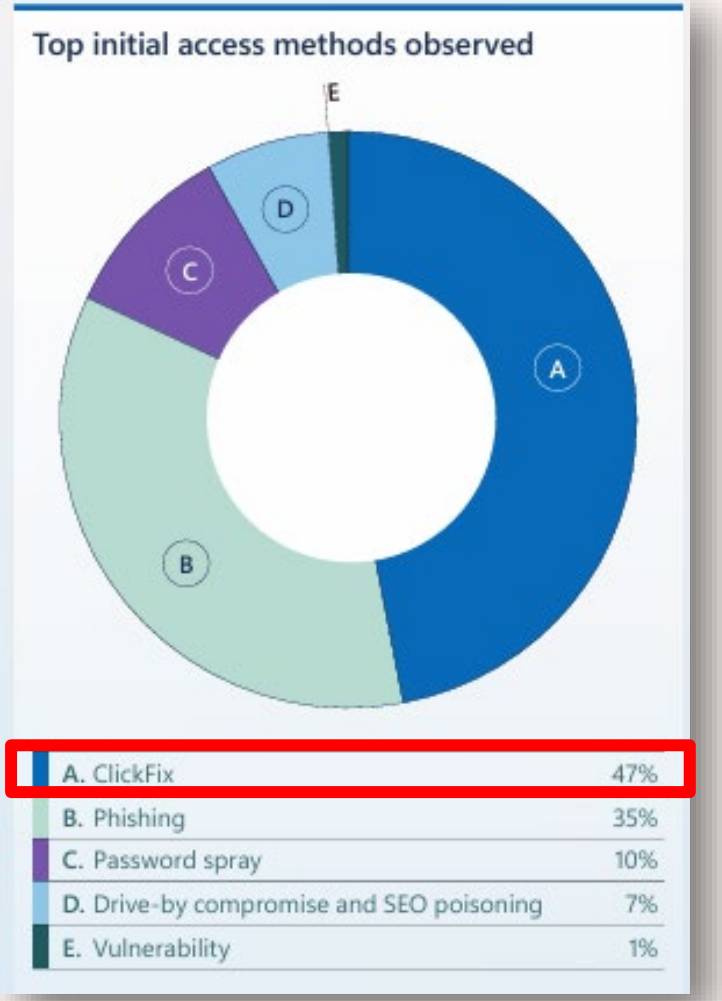
- Mass layoffs in government and industry
- Disillusioned middle management
- Employees primed for sabotage
- Overriding suspicious alerts
- Enabling backdoors
- Transaction approvals
- Executive blackmail

Planted

- Using insiders to access to infrastructure and intelligence over the long term
- AI-generated and stolen identities
- Obtaining legitimate credentials
- Actual target, or jump through?

Initial access – the prime target

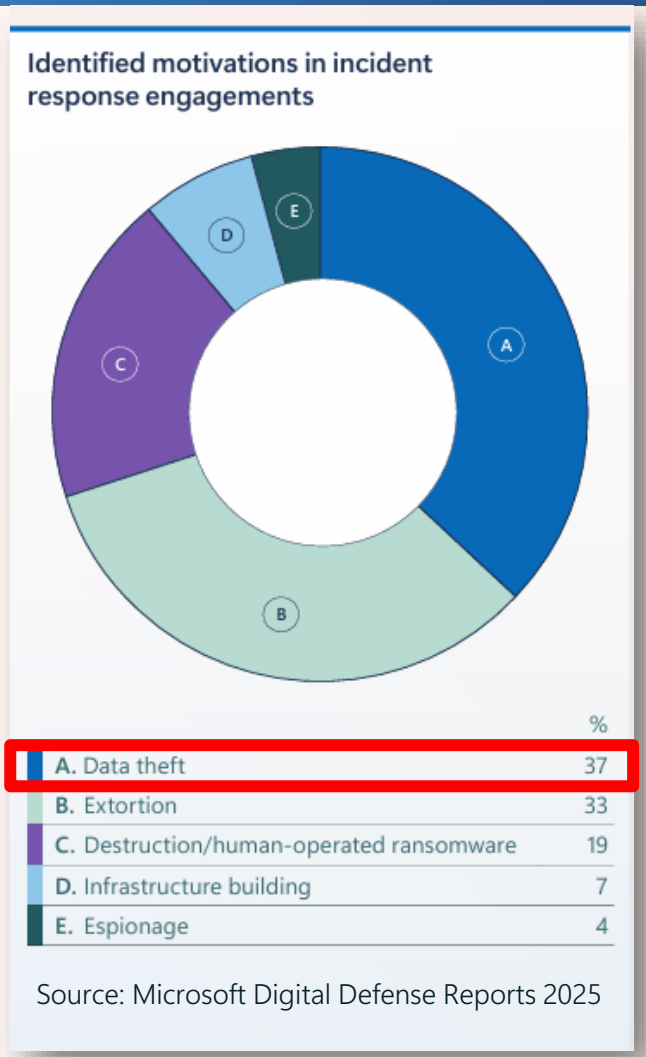
- **Cloud identity – the one to trump them all**
- Click-fix overtaken phishing as primary access
- AI-generated emails receive 50% higher click rate
- Email bombing to bypass critical alerts
- Info stealers as initial pay-load
- Location proximity emulation
- Bots for high-scale fraud



Source: Microsoft Digital Defense Reports 2025

Data – the consistent objective

- Data access versus exfiltration
- Mass dump, versus slow and steady
- Same data, different actor motivations
  - **Ransomware** – opportunistic / high volume
  - **State** – espionage, secrets, intellectual property
  - **Activist / insider** – reputation damaging



Agentic AI – the equaliser

- Action-taking AI agents directly interface with infrastructure & data
- Make decisions autonomously
- High levels of adaptability
- Conduct research
- Generate content
- Emulate empathy

Without a human interface

Agentic AI – the offensive advantage

- Deliver speed and efficiency, with no human fatigue
- Reconnaissance to identify vulnerable targets
- Adapting real-time by making lateral movement decisions
- Rerouting command and control channels
- Ransomware built with evasion and recovery overrides
- **Agent2Agent attacks** – prompt injections, hijacking, misdirecting

As defenders harden, threat actors engineer

Agentic AI – the defensive advantage

- Anticipate, adapt and respond with speed, scale and precision
- Detection engineering to scan for vulnerabilities, and take decisive action
- Identify path of least resistance and add layers of segmentation
- Deploy decoys, re-route traffic, modify and update security configs
- Digital twins for testing and modelling high risk scenarios

Can you detect and respond quicker than an adversary?

Safe and secure AI Adoption

- Human validation for all high-stakes decision-making
- Resilience, redundancy and safety controls
- AI agents treated same as human agents
- Identity-based access controls
- Information protection
- Ethical oversight

Human always in the loop

Protecting AI Models

- AI secure-by-design and default
- Strict data governance and control
- AI Agents in guardian mode
- Scenario planning at scale
- Chaos engineering
- Reversion

Its software, so it’s still vulnerable

Opportunities: Board accountability

The *methods evolve, the mission remains consistent*

01

Geopolitical Risk

Understand how external events, shifts the will and motivation of bad actors. Prepare for the long game

02

Culture

Top-down leadership to embrace psychological safety, to protect from exploitation

03

People & Data

Understanding the value in different hands, determines long term strategy for protection

04

Crisis Leadership

Building effective resilience, that reflects the toughest decisions and stakeholder preparedness

Opportunities: Tech responsibility

Anticipate, and defend for tomorrow

01

Dynamic Defense

End-to-end visibility on attack path exposure, and dynamic detection and response

02

Secure by Design

Choosing and deploying innovative tech that combines utility, security and productivity.

03

Identity & Data

The highest protection and risk oversight levied on the most vulnerable and valuable assets

04

Resilience

Predictive and adaptive preparedness to deliver stability in times of extreme uncertainty