8Depths

The State of Cybercrime

Cybercrime has evolved dramatically from early 2000s till present day, shifting from relatively isolated, low-level attacks carried out by individual hackers into a highly organised, global industry. Before then, threats were largely limited to basic malware, website defacement, and small-scale financial fraud, often requiring technical expertise.

By contrast, today's cybercrime ecosystem is professional and commercial, with "cybercrime-as-a-service" model, cybercriminal education and support services, and AI-driven attacks enabling even low-skilled threat actors to launch sophisticated campaigns.

At the same time, the rapid expansion of cloud computing, Internet of Things (IoT), Industrial Control Systems (ICS), mobile devices, and remote work has widened the attack surface, while social engineering and identity-based attacks are now dominant.

Overall, cybercrime is now more scalable, automated, and financially motivating for criminals than ever before, posing a far greater global threat.

www.8depths.com



Cybercrime at scale:



Ransom payouts and stolen funds have surged

escalating from millions to billions in dollars and cryptocurrency, fuelling a rapidly expanding criminal economy

---



The financial impact of cyber attacks has exploded

growing from billions to trillions in dollars globally, and now representing one of the most significant business risks

---



Threat actors are scaling operations faster than enforcement can respond

with ransomware groups and criminal networks proliferating at a pace beyond the abilities of law enforcement

---



Attack methods are constantly evolving

with cybercriminals continuously refining tactics and techniques to outmanoeuvre even the most advanced security controls

Types of organisations successfully compromised by cybercriminals include:

- Cyber security vendors
- Cyber security managed service providers
- Cloud service providers
- Secure government agencies
- Law enforcement agencies
- Cyber security threat intelligence agencies
- Organisations with highly accredited security certifications
- Organisations with advanced security measures

There is now, no clear line between the secure and the vulnerable. Organisations with limited security controls continue to be breached—and so too are those with mature, well-funded cyber security programmes.

This raises a sharp question. Despite increased investment in tools, frameworks, and controls, cybercrime continues to advance at a pace that often outstrips traditional defences. Attackers are proving not only persistent, but highly adaptive—consistently finding ways around even the most robust security environments.

So, as cybercrime continues to evolve, the real question is clear:

At what point will your cyber security be positioned to effectively meet the challenge?



What has influenced the state of cybercrime?

Cybercrime is not just a technology problem—it is a human one. Today's threat landscape is shaped by a combination of motivation, psychology, economic opportunity, low perceived risk, commercialisation and rapidly evolving capability.

Cybercriminals are not acting randomly; they are making calculated decisions, influenced by incentives, accessibility, and the ease with which attacks can be executed at scale—attracting a broader range of actors with increasingly sophisticated intent.

To understand why cybercrime will keep evolving and how to respond effectively, it is critical to first understand the key drivers that are fuelling its growth.

Key drivers of cybercrime

1 Strong financial incentives (low risk, high reward)

$23.84 trillion

Cybercrime is now a multi-trillion-dollar economy (~$23.84 trillion by 2027).

Attacks like impersonation, ransomware, and fraud generate billions in direct losses.

Compared to traditional crime, cybercrime offers:

Lower physical risk | **Global reach** | **Anonymity** | **High scalability** | **Profitable rewards**

The Outcome:

Cybercrime is economically attractive and growing exponentially

2 Rapid advancement of Artificial Intelligence

AI enables:

Automated reconnaissance, phishing and scams | **Deepfakes and impersonation** | **Faster malware development**

Change of malware signature in real-time to avoid detection | **Vulnerability exploit development for malicious use**

AI lowers the skill barrier
→ less-skilled attackers can launch advanced attacks.

Automation allows mass-scale targeting
→ millions of victims targeted concurrently.

The Outcome:

Cybercrime is becoming faster, cheaper, and more accessible

3

Industrialisation & professionalisation of cybercrime

Cybercrime now operates like a business ecosystem:

"Cybercrime-as-a-service" (ransomware kits, phishing kits, etc)	**Organised cybercrime groups with specialist roles**	**Recruitment through affiliate programs**
Organised crime groups collaborating globally	**Mass exploitation worldwide**	**Profit sharing system**

Reports show industrialised, multi-victim attacks through high-volume, scalable operations.

The Outcome:

Attackers operate like corporations, increasing efficiency and scale

4

Human element

70%

Threat intelligence indicates that over 70% of breaches still rely on people, not tech:

Social engineering | **Human error** | **Privilege misuse**

Users are exploited through trust, urgency, fear, or lack of awareness, a problem which cyber awareness training does not always prevent.

The Outcome:

Humans remain the weakest link in cyber security

5

Expanding digital attack surface

More connected systems = more vulnerabilities:

Cloud services	**Service partners and contractors**	**APIs and AI Agents**
IoT devices	**Remote work environments**	**Bring Your Own Device (BYOD)**

Supply chain attacks and third-party risks increase the number of blind spots and weaken security perimeters.

The Outcome:

More entry points
→ harder to defend everything

6

Weak or uneven global cyber security governance

Cybercrime is borderless, but law enforcement is not.
Differences in:

Laws | **Enforcement capabilities** | **International cooperation**

Joint operational policing resources lag behind cybercrime growth (e.g., number of new cybercriminal groups is rising faster than takedowns by law enforcement).

The Outcome:

Attackers exploit legal and jurisdictional gaps

7

Geopolitical tensions & State involvement

Nation-state attackers increasingly engage in:

Espionage | **Infrastructure attacks** | **Cyber warfare** | **Hacktivism**

Global instability has shown to increase cyber activity against businesses, not just government institutions.

The Outcome:

Cybercrime overlaps with cyber warfare and political conflict

8

Legacy systems & poor security practices

Many organisations rely on:

Outdated software | **End of Life devices** | **Misconfigured systems** | **Unmaintained open-source codes**

Known vulnerabilities remain unpatched for long periods of time leaving room for exploitation.

The Outcome:

Basic security failures enable large-scale attacks

9

Knowledge gap & underinvestment in defence

Many organisations cyber security capabilities lag behind threats, mainly because they:

Lack cybercrime knowledge and expertise	**Accept the security risk**	**Procrastinate on taking action**
Underestimate the cyber risk	**Overestimate their cyber security**	**Shift responsibility to outsourced providers**

This combination of factors results in underinvestment in security, leading to volume of attacks growing faster than defensive capacity.

The Outcome:

Defenders are consistently outpaced

10

Shift to identity-based attacks

The focus of attacks has moved from networks to people and credentials.

Credential theft, account takeover, and identity fraud are rising.

Trust is now the primary vulnerability.

The Outcome:

Identity is the new attack surface

A recipe for cybercrime

Cybercrime today is driven by a combination of economic, technological, and human factors:

Economics

Huge profits + low risk

Technology

AI + automation scale attacks

People

Human error and trust exploitation

Systems

Expanding, insecure digital infrastructure

Governance

Challenges with global enforcement

Together, these create a perfect storm from which cybercrime grows faster than our ability to stop it.



Cybercrime prevails...
So, is cyber security working?

The issue now is no longer about how much security you have in place... but whether you are approaching cyber security in the right way at all?

Contact Us

Reach out to an 8Depths team member to uncover how leading organisations are rethinking cyber security investment – and how you can do the same.

8depths.com/contact

+44 (0) 20 4617 9888

info@8depths.com

*Note: The views and opinions included in this report belong to 8Depths and are based on current, subjective assessments. They do not necessarily mirror the views of any external entity. While we aim for accuracy, these viewpoints are for informative purposes only and do not constitute a guarantee of future outcomes.