CYBERGEN®

Cybergen Threat Intelligence Brief

Date: 09 February 2026
Audience: Board, CISO, Security Operations, Incident Response

Tasmiha Arif
CISO

+44 (0) 1865 950 828
www.cybergensecurity.com

2026

Executive overview

Cybergen Threat Intelligence Teams analysed recent public victim disclosures linked to extortion-led ransomware operations. The findings show clear industry concentration, with a small number of sectors accounting for the majority of the impact.

Across 837 publicly disclosed victims:

- The top 3 industries account for ~44%
- The top 5 account for ~59%
- The top 10 account for ~80%

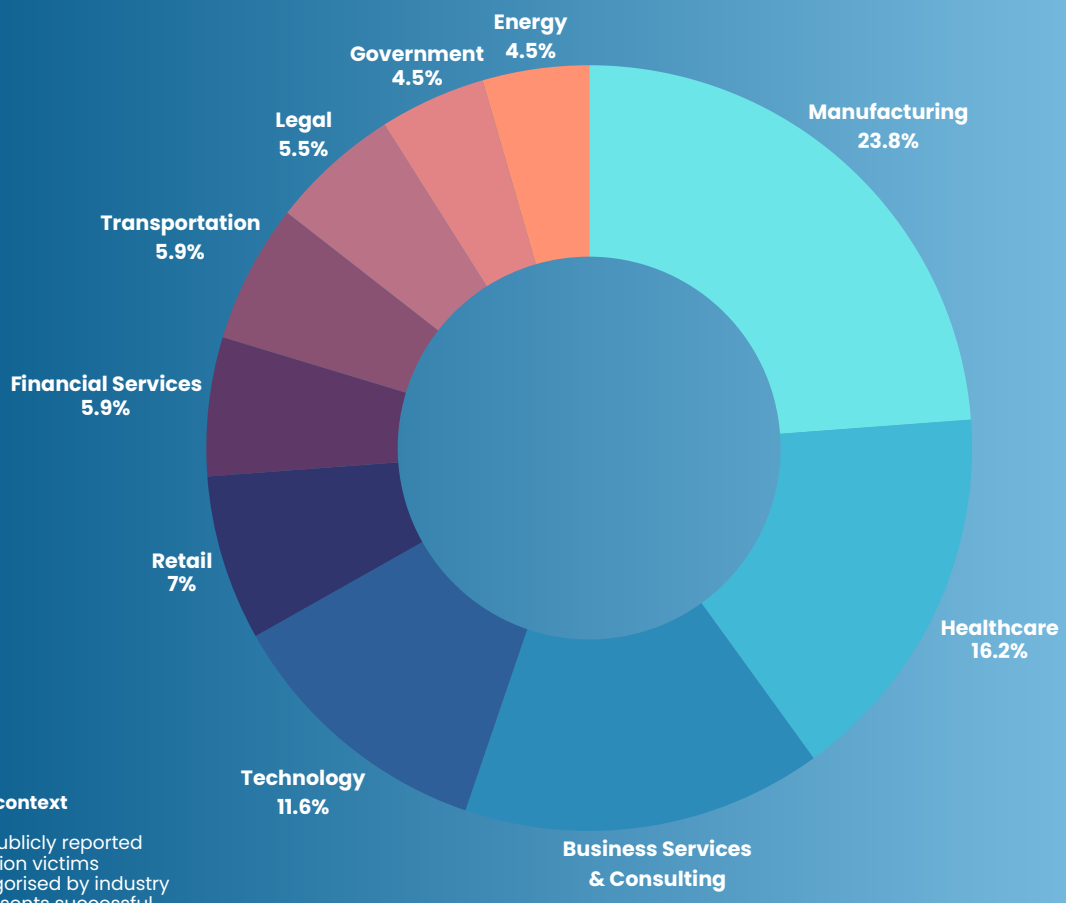
This is not random cybercrime. It reflects deliberate targeting based on business leverage.

Threat actors consistently prioritise organisations offering:

- Rapid operational disruption
- High regulatory or reputational pressure
- Scalable downstream access

Public victim posting represents successful coercion outcomes, not just technical compromise.

Industries Most Impacted by Ransomware



Dataset context

- 837 publicly reported extortion victims
- Categorised by industry
- Represents successful coercion outcomes

Cybergen analysis focuses on business impact mechanics, not threat volume.

*Original data acquired from Flashpoint Ignite

Cybergen interpretation: Extortion is a business model

Cybergen analysis shows public victim disclosure usually follows a predictable operational sequence:

1. External foothold (identity abuse, exposed services, remote access)
2. Privilege escalation
3. Data staging
4. Operational disruption
5. Public coercion

Threat actors are optimising for:

- Speed to business impact
- Systems that halt operations
- Systems that enable disclosure

44%

Manufacturing, healthcare, and business services & consulting account for 44% of all industry ransomware incidents.

Not exploit sophistication.

Most extortion methods are succeeding because:

- Identity pathways are permissive
- External exposure is poorly prioritised
- Data staging is not detected early
- Critical business dependencies are unmapped

These are structural risk issues.

Sector-specific extortion scenarios

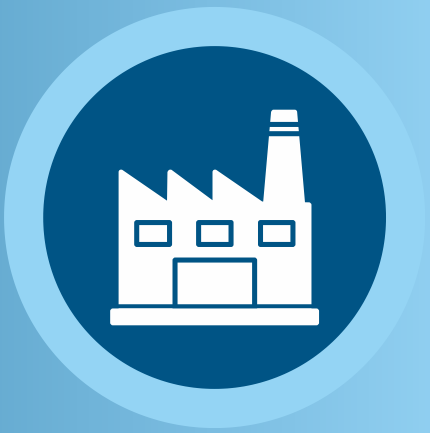
Manufacturing / Energy / Transportation

Primary leverage: Operational downtime

Typical scenario:

- Initial access via exposed remote services or compromised credentials
- Rapid movement into production scheduling or visibility systems
- Partial disruption used to force negotiation
- Encryption often secondary to business interruption

Board impact: Revenue loss begins immediately.



Healthcare / Legal / Financial Services

Primary leverage: Data sensitivity + service disruption

Typical scenario:

- Entry via identity compromise
- Fast access to patient, client, or financial records
- Data staged before encryption
- Dual-track extortion (operations + disclosure)

Board Impact

Regulatory exposure plus service continuity risk.

Business Services / Technology

Primary leverage: Downstream access

Typical scenario:

- Compromise of shared platforms or admin credentials
- Lateral movement into client environments
- One breach becomes multiple victims

Actor behaviour alignment by industry

Cybergen Threat Intelligence Teams observe consistent behavioural patterns:

- Operations-heavy sectors face rapid-impact attacks prioritising disruption over stealth
- Regulated sectors see early data staging before encryption
- Service providers are targeted for credential harvesting and tenant hopping

30–90-day forward risk outlook

Based on current targeting patterns:

- Manufacturing and healthcare will remain primary extortion targets
- Professional services' compensation will continue rising due to access scaling
- Identity-led intrusion will dominate over exploit-led attacks
- Public victim disclosures will increasingly involve partial encryption combined with data coercion

Organisations with exposed remote access, weak identity segmentation, or limited visibility into data movement remain at the highest risk.

Show to the Board

Current Threat Landscape Overview

Cyber extortion activity is increasingly concentrated on a small number of industries where attackers can rapidly disrupt operations, access sensitive data, or gain downstream leverage.

Recent intelligence shows:

- 80% of publicly disclosed ransomware victims fall within just 10 industries
- Manufacturing, healthcare, and professional services are most impacted
- Attacks are structured business operations, not opportunistic crime

Threat actors are no longer focused solely on technical compromise. They target business pressure points.

What This Means for Our Organisation

Cyber risk is now operational risk.

Successful attacks typically involve:

- Compromise of identities rather than malware
- Early data staging before encryption
- Use of legitimate tools to avoid detection
- Fast escalation to business disruption

The decision window between intrusion and executive-level impact is shrinking.

Board-Level Issues to Consider

1. Do we know our fastest path from internet exposure to business disruption?
2. Can we detect sensitive data staging before it becomes extortion leverage?
3. Are our most critical systems mapped to identity and access dependencies?

If these cannot be answered with evidence, extortion risk is largely unmanaged.

Key Takeaway

Ransomware is no longer primarily a technical problem.

It is an intelligence-driven business threat designed to exploit operational pressure, data sensitivity, and trust relationships.

Resilience now depends on understanding how attackers monetise environments, not simply how they enter them.

Tasmiha Arif
Chief Information Security Officer
Cybergen® Security

CYBERGEN®

Get in touch with Cybergen to strengthen your security through intelligence-led defence

Cybergen delivers threat-led security built on real adversary behaviour, not theoretical risk. While most providers focus on controls and compliance, we focus on how attackers actually compromise organisations: through identity abuse, misconfiguration at scale, and weaponised trust relationships. Our intelligence-driven approach connects threat data directly to operational defence, helping organisations prioritise what truly matters, reduce breach impact, and build security strategies aligned to modern attack realities.

Cybergen Security
Hexagon House
Avenue 4
Station Lane
Witney
Oxfordshire
OX28 4BN

+44 (0) 1865 950 828

sales@cybergensecurity.co.uk

www.cybergensecurity.co.uk

Join Our Social Community

LinkedIn