NORTHWAVE
CYBER SECURITY

Global Threat Landscape 2026

Threat Intel for Strategic Leadership

Today's Cyber Threats

At a Glance

One shift stands out in 2026: cyber risk is now moving at machine speed. AI is reshaping the attacker–defender balance, with defenders increasingly falling behind.

Threat actors are faster and more adaptive than ever. Exploits are now automated at scale. Attacks are increasingly driven by both identity and vulnerabilities as attackers systematically abuse the trust relationships that modern organisations depend on.

Key Developments We Are Tracking

- AI increasingly enables attackers to act faster than organisations can assess, patch, and respond
- Identity and vulnerabilities are parallel access paths
- Trust is being exploited at scale
- Cybercrime, espionage, disruption and influencing are converging
- Impact is shifting to data, legal, and strategic exposure

43 days median time for an organisation to install a patch after it has become available

7 days average time exploitation occurs before a patch becomes available

How Your Risk is Expanding

From → To

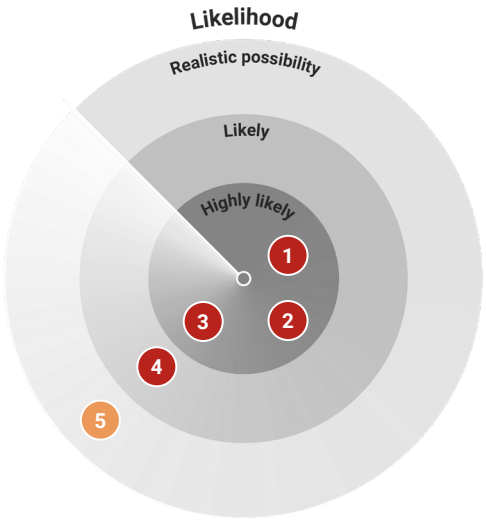
- Systems → Identity
- Incidents → Persistent access
- Disruption → Data and regulatory exposure
- IT risk → Business risk
- Isolated attacks → Strategic consequences

Top 5 Cyber Threats to Prioritise

Exact ranking differs by sector and organisation type

1. **Cyber Extortion**
   - data as leverage
2. **Business Email Compromise (BEC)**
   - identity abuse at scale
3. **Insider Threats**
   - data access without control
4. **Nation-State Attacks**
   - persistent intrusion, data exposure and disruption
5. **State-Aligned Hacktivism**
   - disruption and disinformation

Our threat radar **visualises the likelihood** and the impact of the threats.



Impact of the threat explained

- **Low** Low reputational damage, financial loss, judicial/regulatory consequences and/or business disruption. No additional measures necessary.
- **Medium** Significant reputational damage, financial loss, judicial/regulatory consequences and/or business disruption. Take measures when cost-benefit analysis is significant.
- **High** (Very) severe reputational damage, financial loss, judicial/regulatory consequences and/or business disruption. Mitigate with highest priority and measures until risk is mitigated to an acceptable level.

The following pages provide more insight into what these threats mean for European organisations today and our recommended defence strategies. As always, we advocate for an integrated approach that covers the **business**, **bytes** and **behavioural** aspects of cyber security.

Cyber Extortion

"Impact is now driven by data exposure and regulatory liability, rather than system outage."

Ransomware originally focused on encrypting systems. But today's cyber extortion tactics increasingly prioritise data exfiltration alongside or instead of encryption. Threat actors are using the threat of exposure to increase pressure. As a result, reputational damage, legal risk, and regulatory consequences often outweigh operational disruption.

More than 8,000 organisations worldwide were exposed on leak sites in 2025. In 2026, we've observed the use of AI to accelerate attack timelines, leaving organisations with a narrow window to detect, contain, and respond. The challenge is no longer just recovery, but controlling exposure and making high-stakes decisions under pressure.

Key Defence Strategies

Effective cyber extortion defence is about early detection, constraining and delaying attacker movement, reducing leverage, enabling fast decision making under pressure, and clear crisis communication.

- Establish clear crisis governance across incident response, legal, and communications.
- Run cross-functional crisis simulations so response becomes routine under pressure.
- Align response with regulatory obligations (e.g. GDPR, NIS2) before an incident occurs.

- Deploy MDR/SOC with early detection across identity, cloud, and network, not just endpoints.
- Monitor data exfiltration, backup tampering, and encryption as priority signals.
- Enforce baseline controls: offline backups, phishing-resistant MFA, and network segmentation.

- Train employees to recognise advanced social engineering and MFA bypass techniques.
- Reinforce critical behaviours such as reporting suspicious activity and handling data securely.
- Use scenario-based training aligned with real attack patterns.

Business Email Compromise

“If the identity is trusted, the attacker doesn’t need malware.”

In 2025, BEC accounted for more than 40 percent of all Northwave incident response cases, surpassing cyber extortion. As organisations strengthen defences, attackers are pivoting to session theft and identity-based attacks that bypass traditional controls like MFA.

The threat is expanding across sectors. Manufacturing and business services, especially legal, are among the most affected. Phishing is becoming more convincing and scalable, with messages tailored to language and business context. Combined with AI-driven social engineering, this significantly increases the likelihood of fraud and data compromise.

Key Defence Strategies

Mitigate BEC risk by hardening identity and business processes. Block technical abuse paths and remove reliance on human trust alone.

- Enforce strict payment verification, especially for bank detail changes and urgent transfers.
- Apply the four-eyes principle to high-risk transactions and sensitive operations.
- Define clear approval workflows and escalation paths for financial and access-related requests.

- Include phishing-resistant MFA and conditional access in the identity baseline.
- Detect and restrict OAuth abuse and mailbox manipulation (e.g. forwarding and rule changes).
- Maintain strong email security (SPF, DKIM, DMARC, anti-spoofing, advanced filtering).

- Train employees to verify high-risk requests involving payments or credentials.
- Promote a culture where pausing and checking is expected.
- Train against multi-channel social engineering (email, voice, video) and enable simple reporting.

Insider Threats

“Insider threats are rarely about intent. They are about access without control.”

Most insider incidents involve employees, contractors, or third parties and even AI agents. They are driven by mistakes, negligence, or lack of control rather than malicious intent. These incidents account for roughly one-third of European data breaches and are most common in large organisations, where complexity and employee turnover increase exposure.

The expansion of cloud, SaaS, and AI tools, including autonomous agents, has significantly increased this risk by enabling rapid access and movement of sensitive data. AI-related data leaks are rising in organisations, often driven by a lack of training, governance, and visibility over how data is used.

Key Defence Strategies

Reduce insider risk by controlling access, monitoring behaviour, and enabling employees to make secure decisions by default.

- Implement structured onboarding and offboarding, including timely access provisioning and removal.
- Define and enforce clear policies for acceptable use and negligent behaviour.
- Foster a safe reporting culture with clear escalation paths and whistleblowing mechanisms.

- Enforce least privilege access and require managed, trusted devices for sensitive data access.
- Deploy data classification and DLP to monitor and restrict sensitive data movement.
- Maintain visibility on user activity and unsanctioned tools, including control over AI systems and external integrations.

- Provide continuous, practical training focused on real-world and AI-related risks.
- Reinforce secure daily behaviours for handling sensitive data.
- Create a culture where employees feel safe to report mistakes and challenge unclear situations.

Nation-State Attacks

"Stealthy, long-term, and designed to evade detection."

Nation-state cyber activity now affects almost every major European sector, from defence and energy to manufacturing, logistics and life sciences. Nearly all EU countries are targeted, with Germany, Poland, and France most exposed. These attacks are typically conducted by Advanced Persistent Threats (APTs), well-resourced campaigns backed by governments or their proxies, targeting commercial networks, supply chains, and intellectual property.

For organisations, this represents a persistent business risk. Attackers combine identity abuse, social engineering, insider techniques, and exploitation of cloud and edge environments. These attacks are designed to remain undetected, operate over long periods, and create strategic impact. China conducts persistent and large-scale data collection in Europe, while Russia actively conducts sabotage attempts.

Key Defence Strategies

Defend against persistence by accelerating detection, introducing friction, and preparing for long-term, intelligence-driven response.

- Treat identity, cloud platforms, and edge environments as Tier 1 risk domains, with clear ownership and governance.
- Include supply chain and third-party relationships as part of the internal attack surface, with enforced security requirements and regular review.
- Prepare leadership through adversary simulations and crisis exercises to operate under uncertainty and prolonged threat scenarios.

- Enforce phishing-resistant MFA and risk-based conditional access for critical users and systems.
- Shift detection to behaviour and TTP-based monitoring across identity, cloud, endpoint, and network.
- Reduce attack surface through endpoint and edge hardening and secure baseline configurations.

- Deliver role-based training for high-risk and high-privilege users, focused on targeted social engineering.
- Prepare employees and crisis teams for APT scenarios and prolonged incidents.
- Reinforce response readiness so decision-making and coordination are effective under pressure.

State-Aligned Hacktivism

“The risk is driven less by technical sophistication and more by scale, visibility, and timing.”

Hacktivism remains a persistent threat to European organisations and now is mostly state-linked. Since the start of the war in Ukraine, pro-Russian groups have carried out continuous DDoS campaigns across government, finance, retail, media, logistics, and technology sectors. Individual incidents are often low impact, but their frequency creates sustained operational pressure, especially during politically sensitive periods.

Disruption is often paired with disinformation, amplifying reputational impact even when technical damage is limited. Alleged and confirmed interference with industrial systems are increasing, creating uncertainty and pressure. When hacktivism affects OT environments in critical sectors, even limited access can disrupt operations, raise safety concerns, and trigger regulatory fallout.

Key Defence Strategies

Focus on resilience over prevention. Absorb disruption, maintain trust, and sustain operations under continuous pressure.

- Establish clear crisis governance across incident response, communications, and business continuity.
- Prepare to respond to disinformation and unverified claims quickly and consistently.
- Ensure fallback options exist for critical systems and services during disruption.

- Harden external-facing systems with patching, logging, monitoring, and strong access controls.
- Deploy anti-DDoS protection and web application firewalls to absorb attacks at scale.
- Segment IT and OT environments and restrict direct internet exposure of critical systems.

- Train crisis teams to operate under prolonged disruption and coordinate across security and communications.
- Build awareness of disinformation risks and distinguish between technical impact and narrative pressure.
- Reinforce preparedness for degraded operations and sustained disruption.

Building Defences in the AI era

"Attackers are increasingly operating faster than organisations can assess, patch, and respond."

Cyber threats are shaped by underlying forces–or drivers–that determine why certain threats grow, how fast they evolve, and how much impact they have. Among the key drivers we identified in our 2026 Global Threat Landscape, none act as a greater force multiplier than AI.

Threat actors now use AI to design, execute, and scale attacks much more quickly and easily. AI fine-tunes social engineering, accelerates vulnerability discovery and exploitation, and lowers the skill barrier for attackers. Nation-state actors are at the forefront of this evolution, with criminal adoption following closely behind.

Agentic AI-orchestrated attacks will have the most profound impact on cyber defences. As AI systems become more autonomous, we'll see a significant increase in the speed and volume of attacks. Patterns will become less predictable as AI-assistance makes it easier for attackers to uncover new vulnerabilities and adapt to conditions in real time.

For European organisations, this is not a single tipping point but a steady increase in pressure. **Many organisations still operate on pre AI assumptions, while attackers already exploit these changed conditions.**

What organisations must do now

1. Limit what attackers can reach

Agentic AI-orchestrated attacks will increase pressure on exposed systems, public interfaces, cloud environments, and poorly governed assets. It's critical to know your external attack surface and reduce it where possible.

Focus on:

- Public-facing systems
- Cloud services
- Web applications
- Exposed interfaces
- Network edge devices

What remains exposed must be continuously monitored and patched quickly.

2. Slow attackers down

Agentic AI attackers work at machine-speed, so you must create obstacles to delay their progress. These include:

- Network segmentation
- Identity segmentation
- Just-in-Time (JIT) privileged access
- Tiered admin environments
- Strong controls around cloud and SaaS access

Since these delays only pay off if you use them to trigger your detection, they must be paired with proper detection signals.

3. Accelerate detection and response

Response to an ongoing attack must happen faster. As such, alarm analysis and first active response actions for containment need to be agentic AI-driven as well. Furthermore, SOC and MDR capabilities need visibility across:

- Identity
- Cloud
- Endpoints
- Network edge
- Applications
- Privileges, accounts, keys, and tokens

This visibility delivers the fundamental information for fast, effective decision-making. Lastly, this all feeds into your incident response process, which is still human led. Your process for handling incidents should be clear in terms of communication, responsibilities and process steps. People should receive consistent training to ensure the response feels natural.

How Northwave Can Help

In 2026, cyber risk now sits firmly in the boardroom as a governance and strategic control issue. The ability to take quick, decisive action has never been more important.

We offer our threat intelligence and perspective for action as a starting point. Download the full Global Threat Landscape Report to explore our expert insights in detail.

For tailored guidance, contact us. Together, we can translate these insights into targeted actions for your organisation.

Scan to access Northwave's full Global Threat Landscape 2026 Report

About Northwave Cyber Security

Northwave Cyber Security is a premier European specialist that helps organisations strengthen resilience and respond effectively to cyber incidents. Founded in the Netherlands in 2006, Northwave operates in the Benelux, DACH, and Nordics regions, with offices in Utrecht (Netherlands), Leipzig (Germany), Brussels (Belgium), and Stockholm (Sweden).

Northwave's team consists of over 275 experts in IT security, forensics, psychology, law, criminology, cyber threat intelligence, risk management, and more. Their integrated solutions combine technology, processes, and human behaviour insights for a holistic security approach.

Since 2012, Northwave's certified Computer Emergency Response Team (NW CERT) has been aiding companies globally in responding to and recovering from ransomware attacks, data breaches, and other security incidents.

For more information, visit northwave-cybersecurity.com.

Need help now?
Call day or night: 00800 1744 0000

NORTHWAVE
CYBER SECURITY

E: info@northwave-cybersecurity.com
T: +31 (0) 30 303 1240
W: northwave-cybersecurity.com