February 2026
Info Snapshot
Sponsored by Logicalis

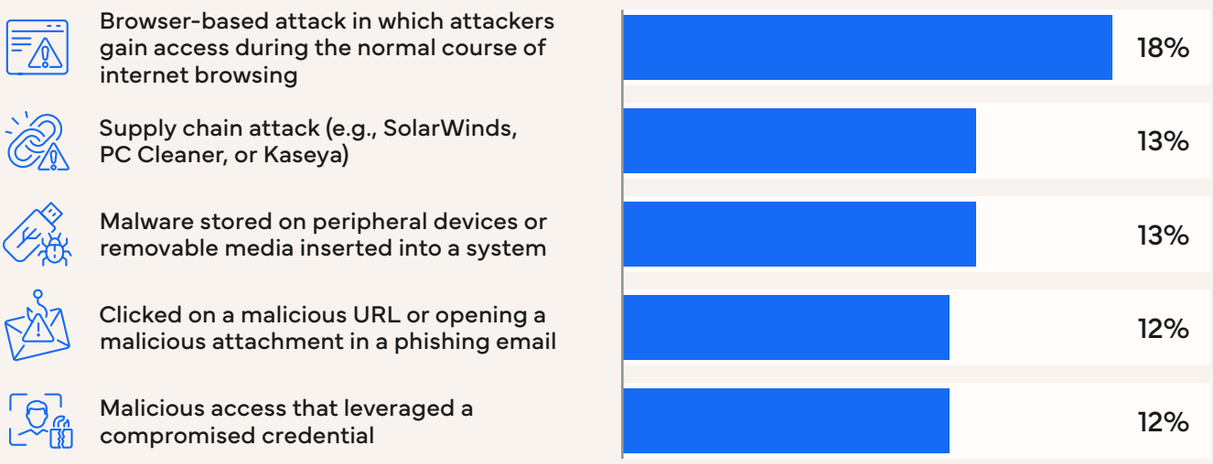
Human Identities: Cybercriminals' Easiest Route Into Your Organisation

David Clemente
Research Director,
European Security, IDC

The threat landscape continues to diversify, but human identity remains at the centre

In recent global research, we found that human identities remain the easiest target for attackers. As demonstrated by the data below, people and their identities feature in all 5 of the top sources of initial ransomware compromise, as they are the most accessible and least protected routes. For attackers with time on their hands, ease – not speed – is key.

The most significant sources of ransomware compromise



[1]Source: IDC's *Future Enterprise Resiliency & Spending (FERS) Survey, Wave 5,* June 2025, worldwide (N = 885). These are the top five responses and will not total 100%.

These results highlight that **people are the primary target** for ransomware attackers – not just within organisations but also in their wider supply chain. While this may not come as a surprise, it does confirm that human identities must be a significant focus area when developing an organisation's security strategy.

This identity threat is accelerating as **AI use becomes widespread.** AI tools enable attackers to industrialise commodity attacks (e.g., mass phishing) and craft more effective personalised attacks. This takes advantage of human weakness and preys on the identities of trusted suppliers.

As a result, ransomware is ramping up with no signs of slowing, causing record levels of business disruption (including time lost due to essential IT being blocked) and loss of revenue or critical services during attacks.

Specific capabilities are needed to address identity security

The data shows numerous ways attackers gain access using human vulnerabilities. However, organisations can take certain steps to mitigate these risks:

Browser-based attack (18%): Begin with using secure web browsers, web browser isolation and end-user behaviour monitoring.

Supply chain attack (13%): Implement vulnerability management and use cyberthreat intelligence to assess supplier risk while considering managed secure firewall, SSE, and zero trust network access.

Malware on devices (13%): Consider an XDR platform – with optional SIEM – to monitor endpoint activity and detect anomalous user behaviour and data exfiltration.

Phishing email click (12%): Use phishing tests with automated user training and apply XDR policies to monitor endpoint and user behaviour.

Compromised credentials (12%): Use cyberthreat intelligence to identify stolen credentials on the dark web and SIEM to identify suspicious accounts and correlate authentication, command and control, and endpoint activity.

Key actions to close the easiest routes for cybercriminals

Reviewing the list of suggested tactics, it can often be overwhelming and difficult to decide which strategic direction to take first. Concerns also exist around resource availability to execute these tactics and experience to ensure correct execution. Key actions include the following:

- **Prioritise the right tactics:** Organisations can choose their tactics or take advantage of external providers that can advise on which tactic will have the most effective impact.
- **Access practical experience:** Organisations need access to experts who have dealt with many cyberattacks and can bring knowledge from working across multiple companies and industries.
- **Strengthen incident responsiveness:** Organisations need access to experts who are on-call and available. When an incident happens, it is already too late to create a response plan and allocate responsibilities.

Ransomware is prevalent, and even the best-protected organisations can suffer an incident. However, this does not have to be intimidating for organisations with a plan and people in place. Preparation can mitigate the immediate impacts of an incident and alleviate longer-term damage (e.g., customer churn, reputational damage, and regulatory sanctions).

Most importantly, having the right capabilities provides invaluable peace of mind for business executives and security leaders – and even better if these capabilities are flexible, adaptable and scalable to meet any need.

LOGICALIS
Architects of Change

Message from the sponsor

As a leading Global Security Managed Services provider, we see firsthand how Human Identity vulnerabilities can weaken an organisation's defences. This Info Snapshot highlights how attackers exploit these gaps while also demonstrating that effective security solutions are within reach. Visibility is essential — we offer a simple assessment to uncover human-centric vulnerabilities and provide practical recommendations to strengthen your security posture.

Learn more.

IDC Custom Solutions

February 2026 | #EUR254250526-IS | Sponsored by Logicalis