uptime INTELLIGENCE

INTELLIGENCE UPDATE

Supply chain exploits: the blind spots operators need to address

John O'Brien 8 Jan 2026

Severe cyberattacks originating from IT and OT supply chains are on the rise. Often these attacks exploit third parties that may be connected to — or have intermittent access to — the operator's internal network. Changing suppliers, systems and personnel is known to introduce new security risks and vulnerabilities; however, many fail to monitor and manage these changes effectively.

Only a handful of third-party suppliers — typically the largest — are considered "Critical" from a regulatory standpoint (see *European cybersecurity regulation and its impact on digital infrastructures*). However, "Non-critical" partners — those often smaller and contracted for shorter terms — are just as likely to pose risks. But they are unlikely to receive the same oversight. Legacy partners present another category of risk, since they may be considered entirely disconnected and therefore no longer monitored.

If any partner (existing or former) remains connected to the network, organizations need to proactively monitor and manage their activity and intervene as necessary. Failing to do so can leave systems vulnerable to supply chain attacks.

The risks have reached a new level of severity following the cyberattack on Jaguar Land Rover (JLR) in 2025, which became the costliest in UK history. The attack cost the company £1.9 billion ($2.5 billion) directly, while the broader supply chain and UK economy suffered an estimated £2.1 billion ($2.8 billion) in damages, according to the Cyber Monitoring Center.

JLR's attackers targeted a former third-party to gain access to its corporate network and ultimately shut down production. Attackers achieved this by reportedly stealing the provider's user login details to JLR's Jira project management system. The exploit was successful because both the system access and user credentials remained live, even after several years. Also in 2025, data center operator and services provider Colt Technology Services was hit by a ransomware attack that initially struck a critical third-party cloud provider (see **Appendix**).

Data center operators have told Uptime Intelligence that they are increasingly concerned about such issues. However, despite this recognition, the Uptime Institute Data Center Security Survey 2025 suggests others may not be concerned enough.

Identifying the blind spots

The Uptime Institute Data Centre Security Survey 2025 found that operators are focused on specific concerns, while remaining unaware of other often-related risks. This is likely to make it more difficult for operators to objectively identify their third-party blind spots and determine the right interventions.

Customer data confidentiality dominates concerns

Nearly two-thirds of operators (64%) consider customer data confidentiality as their top concern, while just over half (54%) cite data loss/corruption and service interruptions as major concerns.

Implication: All of these issues can result from cybercriminals attacking a vulnerable third party, compromising corporate systems and availability, and ultimately targeting customer data, via lateral movement (as evidenced by the JLR attack).

Third-party attacks are significantly underweighted

Only one in five operators (21%) rate attacks via third parties as a top concern, and a similar proportion (18%) do not regularly assess third-party risks. This contrasts with other research indicating that more than half of data breaches are the result of third-party compromises (sources: *LEET Security* and *SecurityScorecard* surveys).

Implication: Many operators are likely underestimating their exposure by failing to monitor all partners. Rather than focusing solely on major suppliers, organizations must monitor all partners, including the long-tail of small and legacy contractors, to ensure secure control of their network perimeter.

Unauthorized access is the leading cause of severe incidents

Unauthorized access is identified as the primary cause of the most serious/severe cybersecurity incidents, by a third of operators (31%).

Implication: Operators report that cybercriminals most often gain unauthorized access to systems through human-targeted techniques, such as exploiting insufficient employee training (44%), social engineering (37%), and stolen or shared credentials (30%). These attacks are frequently delivered via third-party IT and OT system compromises (see *DCIM vulnerabilities increase threat of cyberattacks* and *OT security: rising critical vulnerabilities, widespread risks*).

Sources of risk and their consequences

Customer and operator data face increasing risk from third-party connected systems, which may have multiple vulnerabilities, and produce consequences that are difficult to quantify. Critically, third-party connections to internal networks may be unmonitored or even unknown, resulting from

legacy or unauthorized equipment.

Connected system monitoring failures

Gaps in the inventory of software systems — such as configuration management databases (CMDBs), building management systems (BMS) and data center infrastructure management (DCIM) — can leave operators unable to identify specific weaknesses within their organization. Many small or unvetted supply chain partners may lack adequate cyber credentials. Most, if not all, of these partners require connectivity to internal systems to transact and perform services. A common mistake is leaving user accounts active, passwords unchanged, and APIs or network ports connected after access is no longer required. This appears to have occurred in the JLR incident.

Legacy systems may not be secure or compliant

Many data center facilities continue to use outdated computer hardware and legacy Windows operating systems for industrial control system (ICS)/OT interfaces. While legacy equipment may not comply with international standards such as ISA-99/IEC 62443, NIST or ISO/IEC 27001, modern IT/OT equipment may connect to third-party systems that follow different standards, or which change over time. This inconsistency complicates monitoring, as well as the reporting and remediation of common weaknesses and exposures (CVEs).

Unsanctioned devices

Removable and mobile devices used for on-site maintenance or updates can introduce further risks. For example, compromised USB or other removable media devices have contributed to a steep rise in ransomware incidents affecting ICS/OT systems. In early 2025, US control systems supplier Honeywell discovered 2,472 new ransomware incidents affecting ICS/OT systems — up 46% from the previous quarter (see *Ransomware incidents on OT equipment surge).*

Problems in quantifying contracting risk

When third-party products and connections are unknown or unmonitored, customer and corporate data can be exposed or corrupted, and services disrupted. Beyond this, operators can face unexpected financial exposure when service level agreements (SLAs) and key performance indicators (KPIs) are breached, even though the failure may lie with a third party. In these circumstances, appropriate cyber insurance should be a consideration (see *Cloud outage insurance: assessing policy options*).

Further difficulties arise from resiliency commitments, including recovery time objectives (RTOs), which dictate how quickly a service must be restored after an outage, and recovery point objectives (RPOs), which determine backup procedures to limit the data lost following an incident.

Operators are often concerned that they may be unable to meet arbitrary targets set in standard agreements. For instance, RTOs and RPOs should reflect the reality that even well-understood

cloud services used for active-active failover may take a week or more to fully restore data. In the Colt Technology Services ransomware attack (see **Appendix**), recovery took several months because systems also had to be rebuilt to ensure removal of all compromised code.

The Uptime Intelligence View

Many operators are at the mercy of third parties over whom they have little direct control. However, the security implications often stem from their own failures to properly identify and manage both the internal and external connected systems. Digital infrastructure operators could face serious consequences if they fail to learn from errors in adjacent sectors and do not implement effective monitoring and control of third-party systems and network access.

Appendix

Two high-profile cyberattacks in 2025, affecting Colt Technology Services and Jaguar Land Rover, illustrate the consequences of third-party risk management failures.

- **August 2025:** Colt Technology Services experienced a ransomware attack that took its core business support systems offline. The incident was reportedly caused by a zero-day remote code execution (RCE) attack on a critical Microsoft Sharepoint server, which forced the company to take certain back-office and customer service systems offline. The process of recovery and rebuilding were still ongoing as of December 2025. Attackers reportedly demanded £200,000 ($270,000) for the stolen data, although the likely cost to Colt will be far higher.
- **September 2025:** Jaguar Land Rover suffered a ransomware attack widely reported as the most costly cyberattack in UK history, with losses of £1.9 billion ($2.5 billion). Attackers exploited weak security practices at both JLR and a former third-party partner that still had access and login privileges to the company's Jira project management system dating back to 2021. Attackers acquired login credentials and shut down its global IT systems, stealing hundreds of gigabytes of proprietary (and likely customer) data. The incident halted production and retail operations, as well as financially crippled JLR's supply chain.

The following Uptime Institute experts were consulted for this report:
Antonio Ramos, Founder and CEO of LEET Security, an Uptime Company
Lanre Rotimi, Cybersecurity Program Manager, Uptime Institute

Other related reports published by Uptime Institute include:
OT security: rising critical vulnerabilities, widespread risks
DCIM vulnerabilities increase threat of cyberattacks

Seven fallacies of data center cybersecurity

Cloud outage insurance: assessing policy options

ABOUT THE AUTHOR

John O'Brien

9 Jan 2026

John is Uptime Institute's Senior Research Analyst for Cloud and Software Automation. As a technology industry analyst for over two decades, John has been analyzing the impact of cloud migration, modernization and optimization for the past decade. John covers hybrid and multi-cloud infrastructure, sustainability, and emerging AIOps, DataOps and FinOps practices.

jobrien@uptimeinstitute.com

About Uptime Institute

Uptime Institute is the Global Digital Infrastructure Authority. Its Tier Standard is the IT industry's most trusted and adopted global standard for the proper design, construction, and operation of data centers – the backbone of the digital economy. For over 25 years, the company has served as the standard for data center reliability, sustainability, and efficiency, providing customers assurance that their digital infrastructure can perform at a level that is consistent with their business needs across a wide array of operating conditions.

With its data center Tier Standard & Certifications, Management & Operations reviews, broad range of related risk and performance assessments, and accredited educational curriculum completed by over 10,000 data center professionals, Uptime Institute has helped thousands of companies, in over 100 countries to optimize critical IT assets while managing costs, resources, and efficiency.