imprivata® | Ponemon INSTITUTE

The state of third-party access in cybersecurity

PONEMON REPORT 2025 | United Kingdom

01 Introduction

The modern enterprise relies on third parties – including vendors, contractors, suppliers, partners, and broader supply chains – to operate effectively and to be successful. But it can often be those same third parties at the source of cyber incidents. In fact, 51% of organisations in the UK experienced a breach or attack that involved third-party network access in the previous 12 months. That's higher than the global average of 47%.

The Ponemon Institute surveyed 398 IT professionals from UK organisations from healthcare, the public sector, financial services, manufacturing, and other industries. Here are the key findings based on what they told us:

- The cybersecurity risk posed by third-party access is significant, and it's not going away.
- Organisations are trying, but struggling, to address the threat. Reasons why include limited budget, lack of resources, and no centralised control or ownership.
- Organisations need to refine and mature their strategies for securing third-party access.

The remainder of this mini report will focus on key takeaways from the UK environment, presented with supporting data, related to the prevalence of the third-party risk. For full discussion on context about the global figures, and further insights on other takeaways, check out the full ***"State of third-party access in cybersecurity"*** report.

02 Key takeaways: Prevalence of the third-party threat in the UK

The third-party risk is significant, and attacks can have meaningful business, financial, and operational impact. The threat is expected to remain at current high levels – or get worse – and organisations recognise that the third-party access threat is one they must address.

51% of organisations in the UK have experienced a data breach or cyberattack over the past 12 months involving third-party access

32% said the attack or breach was the result of the vendor having too much privileged access

36% where unsure of the cause, likely due to a lack of visibility

Biggest breach consequences

Loss of sensitive information **(54%)**

Regulatory fines **(49%)**

Severed relationships with third party **(47%)**

65%

of organisations think data breaches caused by third parties will remain the same or increase in the next 12-24 months

47%

of organisations say that third-party remote access is becoming their weakest attack surface

£70,000 is the average cost to restore access after a breach in the UK

03 More on the third-party access threat

Organisations in the UK face an uphill battle when it comes to third-party access risk. When more than half of organisations reported a third-party access-related attack or breach, and when 65% think those type of attacks are likely to stay the same or increase, the need for a better access strategy is clear. With proper prioritisation and funding, organisations can elevate their strategy for protecting against third-party access risk.

Download the global report, *"The state of third-party access in cybersecurity,"* for full insights into the third-party threat, how organisations are trying to combat it, why they're struggling, and what types of strategies are being deployed.

Download now