imprivata | Ponemon INSTITUTE

2025 third-party risk report: vital statistics

The Ponemon Institute's report, "The state of third-party access in cybersecurity," provides eye-opening statistics on the risks and challenges that arise when vendors and other outsiders access organizations' networks. Here are key findings from that report.

Organizations across all industries are aware of, and have been affected by, third-party risks.

47%
of organizations experienced a breach or attack that involved third-party network access in the previous 12 months

64%
say third-party data breaches will either increase or stay the same over the next 12-14 months

48%
believe third-party remote access is becoming the organization's weakest attack surface

Organizations are trying to address the risks, but it remains a challenge to do so, lacking a consistent/ mature strategy.

47%
say IT / security makes ensuring the security of vendors' remote access to its network a priority

73%
say they have a VPAM solution, but only 52% expressed confidence that it's effective in reducing privileged access abuse

Organizations have an average of 20 vendors with access to their organization's network, with

- 25% reporting that they have more than 30 vendors that do
- But only 50% of organizations have a comprehensive inventory of all vendors with access to their network

Why does it remain a challenge?

Limited internal resources, a reliance on manual processes, and no centralized control.

44%

say that managing third party permissions and remote access to their network can be overwhelming and a drain on internal resources, spending an **average of 134 hours per week analyzing and investigating the security of third-party and privileged access**

59%

do not monitor third-party access due to confidence / reliance on the vendor's security and/or a lack of internal resources to do so (44%). Among those that do monitor access, **59% are doing so manually.**

The most significant barriers to reducing third-party and privileged access risks were

Lack of oversight or governance (50%)

Complexity of compliance and regulatory requirements (48%)

Insufficient resources or budget (41%)

The result is limited visibility into vendor access.

Good news:

Organizations are getting better at providing the right amount of access to third parties with only **34% saying the attack involved the third-party having too much privileged access, down from 70% in 2022.**

But...

BUT **35% said they were unsure how the cyberattacks were perpetrated**, up from just 2% in 2022

Third-party access remains a prevalent threat that organizations need help addressing.

Consequences of an attack:

Loss or theft of sensitive and confidential information (53%), regulatory fines (50%) and severed relationships with the vendor (49%)

58%

of organizations said their strategy to address privileged access risks is inconsistent or non-existent

To gain further insight on the risks and challenges of third-party access, see the full report. To learn about purpose-built third-party access solutions from Imprivata, visit our website.

Read the full report

Visit our website

imprivata®

Imprivata delivers access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. Imprivata's platform of innovative, interoperable access management and privileged access security solutions enable organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership. For more information, visit www.imprivata.com

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0)208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +613 8844 5533