imprivata® | Ponemon INSTITUTE

Unpacking the perils of third-party access risk in manufacturing

PONEMON REPORT 2025 | Manufacturing

Manufacturing Spotlight

From underestimation of inherent risks, to overconfidence in vendor security practices, to resource constraints and more, manufacturing organizations are clearly challenged by third-party access risks. Given their pivotal position in the supply chain, **manufacturers can be significantly vulnerable when risks impact the efficiency and security** of business-critical equipment they use to manage and control operations.

For perspective on these challenges for manufacturers, here are key findings from the 2025 Imprivata State of Third-Party Access in Cybersecurity report.

Key takeaways

The cybersecurity risk posed by third-party access is significant, and it's not going away

While they're trying, manufacturing organizations are struggling to address the threat due to limited budgets, lack of resources, and no centralized control or ownership

Manufacturers need to refine and mature their strategies for securing third-party access

Breach prevalence and impact

42% of manufacturing organizations experienced a data breach or cyberattack involving a third party accessing their network.

35% said the attack or breach was the result of the vendor having too much privileged access

Biggest breach consequences

Loss or theft of sensitive and confidential information **(50%)**

Regulatory fines **(45%)**

Loss of revenue **(45%)**

46% think third-party remote access is becoming the organization's weakest attack surface.

Risk management challenges

47%

of manufacturing organizations spend more than 50 hours per week (and 31% spend more than 100 hours) analyzing/investigating the security of third-party access.

43%

of manufacturing organizations don't have a comprehensive inventory of all third parties with access to their network. The biggest reasons cited are lack of resources (46%) and no centralized control over third-party relationships (37%).

45% of respondents said their organization provides third parties with only enough access to perform their designated responsibilities.

Lack of a comprehensive, consistent access strategy

29%

say their strategy to address privileged access risk is applied consistently across the organization (the lowest of any industry in the survey), with 18% saying they have no formal strategy at all.

27%

use enhanced identity and access management techniques to ensure appropriate access to high-value data assets.

Too much confidence in vendor security practices

54%

of manufacturing organizations say they don't evaluate the security and privacy practices of third parties before they engage them to access sensitive information.

The primary reasons are a lack of internal resources to verify, and confidence in the third party's ability to secure information (both cited by 64% of respondents).

59%

of manufacturing organizations say third parties with access to their sensitive information are not monitored. Of those that don't monitor, the overwhelming top reason was confidence in the third party's ability to secure information.

Barriers to reducing risk

The biggest barriers cited in reducing third-party access risk are:

- Complexity of compliance and regulatory requirements **(61%)**
- Insufficient resources and budgets **(33%)**

Ultimately, manufacturers are as susceptible as any other industry to third-party cyber risk, and while they recognize the threat, they struggle to fully address it. A winning game plan starts with a comprehensive strategy, and then requires putting the right budget, expertise, resource capacity, and technology controls in place.

For additional insights on the challenges of third-party access and how organizations are trying to manage risks, **see the full Imprivata State of Third-party access in Cybersecurity report.**

Learn more

View manufacturing data