imprivata

Manufacturing's third-party access challenges: Best practices to build a security-focused culture

There's no doubt that digital transformation has created significant opportunities for manufacturers to boost operational productivity and efficiency. But growing connectivity with and reliance on third-party vendors to keep the wheels turning has also brought increased security vulnerabilities.

The risks to manufacturers include loss of intellectual property, the compromise of OT systems, and downstream impacts to the supply chain or customers.

The resulting damage can be devastating. Attackers targeting manufacturers often aim to steal proprietary designs or cause chaos by shutting down machinery or production lines. Approaches include ransomware, data theft, user impersonation, and threats to expose sensitive information. These attacks not only damage infrastructure and revenue but can also erode an organization's trust and reputation.

The real-world impact of these vulnerabilities is troubling. According to the IDC InfoBrief, sponsored by Imprivata, "Manufacturing's Digital Transformation Dilemma" (IDC #US53662525 July 2025), 57% of manufacturers experienced a ransomware attack in the past year. The IDC InfoBrief also found the cost of one hour of unplanned downtime to be over $125,000.

A foundational problem is that too often, too many vendors have too much access to manufacturers' sensitive data, with too little oversight. In addition, manufacturers often place far too much faith in their vendors' security practices without the benefit of due diligence and adherence to zero trust principles. Essential to successfully managing vendor access risk is the use of purpose-built solutions that enable simple, secure access to networks and sensitive data. Importantly, these solutions need to be an integral part of a comprehensive strategy focused on safeguarding data.

What does that look like? **The IDC InfoBrief highlights best practices** manufacturers are employing to help build a culture and foundation for superior security, including:

- ☑ Establish cross-functional teams responsible for developing an Industry 4.0 roadmap that balances security, operational performance, and corporate goals.
- ☑ Create and enforce standardized security policies and network access.
- ☑ Utilize a formal escalation process for critical network performance or security issues.
- ☑ Regularly review and evaluate the security policies in place. Security is a dynamic process that must be adapted as necessary.

To learn more about manufacturers' digital transformation challenges and opportunities, read the IDC InfoBrief.
For information on how Imprivata helps manufacturers and other organizations manage third-party access, click here.