imprivata

A Continuing Crisis: Third-Party Access

Third-party vendors are an inevitable part of a business environment, which means third-party remote access is a necessity. But this privileged, third-party access and specifically, the risk involved, is a growing problem — and it's a problem every single organization needs to solve.

Third-Party Risk Needs To Be Taken Seriously

Organizations still aren't taking third-party vendor remote access seriously. Year over year, no new progress has been made in reducing third-party risk or increasing third-party specific security effort.

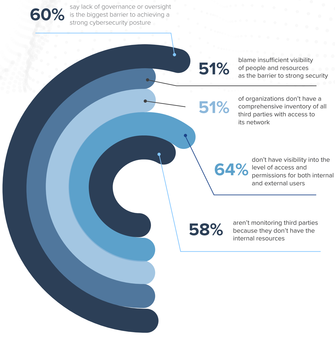
In this year's research 70% of respondents say it was the result of giving too much privileged access to third parties — a slight decrease from 74% of respondents in 2021.

Those numbers might not account for every single vendor-caused attack.

39% of organizations say they aren't confident their third parties would notify them of a data breach.

53% say that less than half of their third parties are aware of their industry's data breach reporting regulations — which is concerning considering that several of the newest federal mandates and orders require cyber incident reporting and response plans.

Organizations are having trouble gaining visibility over vendors and third-party activity...



...and controlling or restricting access, even though access controls are proven and effective methods to limit vendor access (and therefore risk).

- 57% of organizations are unable to designate only enough access to perform designated responsibilities (and nothing more)
- Only 36% of respondents say their organizations have visibility into the level of access and permissions for both internal and external users.

And it's no wonder why — finding and retaining cybersecurity talent is the biggest challenge of IT and security teams across industries.

49% don't have individuals dedicated to managing third-party access

60% don't inventory third parties because there's no centralized control over third parties

48% aren't inventorying or managing vendors because of the complexity of the third-party relationship

67% feel managing third-party permissions and identities is overwhelming and a drain on internal resources

This is why 59% of respondents say their organizations are not evaluating third parties' privacy and security practices or they are unsure if they do. They just don't have the manpower or resources.

60% continue to rely on the reputation of the third party instead of evaluating security

58% percent of respondents say it is because the third party is subject to contractual terms

57% say they don't do security checks because they don't have the internal resources to check or verify

As a result...

- 64% say third parties are becoming an organization's weakest attack surface
- 67% believe the number of cybersecurity incidents and data breaches involving third parties is increasing
- 50% don't rank as highly effective in mitigating remote access threats
- 47% aren't highly effective in detecting remote access threats
- 48% aren't effective in responding to third-party incidents
- 48% aren't highly effective in controlling third-party access to network
- 53% aren't highly effective in achieving compliance with security and privacy regulations
- Most (66%) don't have confirmation that basic security protocols are in place or (67%) check for vulnerabilities in hardware or software

So what?

Organizations have made some progress when it comes to third-party security, but it's not enough to move the needle. Considering the rapid rate at which cyberattacks are progressing — and the hefty price tag that comes with the cleanup of an attack — organizations must do more to secure their systems from third-party threats.

Automate third-party remote access. It needs to be handled differently from internal access. Streamline remote access specifically for third parties to effectively and successfully secure the connection.

Integrate security technologies. To fully secure third-party identities and access, cybersecurity tech needs to sync and communicate with each other to fill in all security gaps.

Create a third-party risk management program that uses these automated and interconnected technologies to predict, detect, prevent, and respond to any third-party risks.

52% say their organization's IT team doesn't prioritize third-party risk