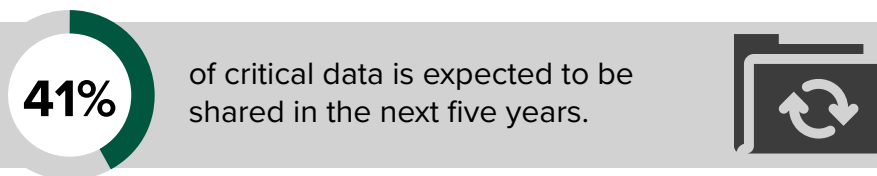
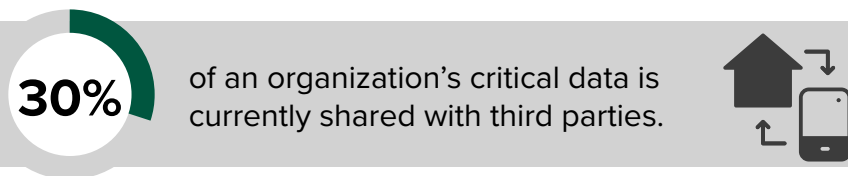
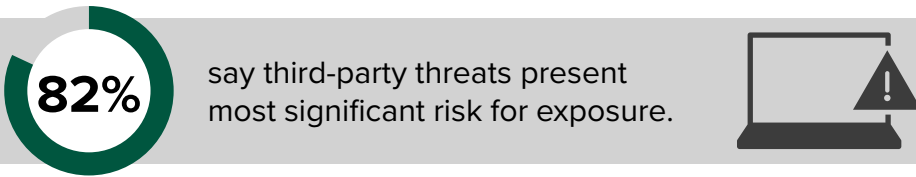


# Organizations Don't Prioritize Third-Party Risks

Key Process Gaps Demonstrate How Businesses Are Increasingly Vulnerable To Security Breaches

## CONFIDENTIAL INFORMATION IS CONSTANTLY EXCHANGED WITH THIRD PARTIES

Both organizations and third parties are exposed to significant cyber risk.



Critical data may include customer information, sales data, or other forms of intellectual property.

## INEFFECTIVE THIRD-PARTY RISK-PREVENTION STRATEGIES

This is due to both the lack of prioritization and the matter of approach.

24% of new vendors are unassessed.

40% of current vendors remain unassessed.

48% of organizations aren't intent on improving how they manage third-party risks.

74% of organizations do not utilize risk intelligence feeds.

95% of risk management efforts are impeded by poor collaboration, classification, and strategic guidance.

## VICTIMS OF THIRD-PARTY CYBER INCIDENTS DON'T CHANGE

Despite experiencing incidents, organizations aren't readily embracing risk management.

67% have experienced a third-party cyber incident in the past year.

30% of companies with an incident continue to share their critical data with third parties.

46% of organizations suspend risky third-party relationships only after an issue is resolved.

22% of firms, which have not experienced a cyber incident, share their critical data with third parties.

## MITIGATING THIRD-PARTY RISK REQUIRES CHANGE BUT IT BRINGS REWARDS

New assessments, processes, and technology solutions are recognized for yielding customer and business benefits.

57% want deeper internal and external assessments of current third parties.

50% seek streamlined/standardized processes.

56% anticipate increased trust from customers.

51% expect an improved customer experience.

