ESENTIRE

Guard Against Third-Party Risk to the Nth Degree

PROTECT YOUR DATA FROM THE UNKNOWNS AND **COMPLEXITIES OF VENDOR ECOSYSTEMS**

In January 2019, eSentire commissioned Spiceworks to conduct an online survey of 600 information technology and security decision makers in the U.S., Canada, U.K., Ireland and Scotland with purchase influence over security solutions and familiarity with third-party risk.

For many, cost-effective scalability usually means outsourcing some or all of your business functions to a complex web of third-party vendors. Do you have formal procedures to manage the potential web of cyber risk that comes with outsourcing? Have you thought about the nth number of parties in your vendors' ecosystems who also may have access to your data?



PERCEPTION

Most organizations report they have effective third-party risk policies in place.



74 percent are confident their third parties have adequate protections in place against a breach and would notify them if a breach occurred involving their data.

An organization typically has many vendors and those vendors have vendors. This creates a hidden web of potential data risk. You are responsible for third parties and you must consider fourth and fifth parties who may have access to critical information without providing direct consent.



59 percent have a risk policy in place

81%

81 percent say their risk policy is effective

WHY DOES MANAGING THIRD-PARTY **RISK TAKE A BACKSEAT?**

Prioritization

Only **35%** say managing third-party risk is a priority

Lack of Resources

32% lack internal resources to audit third parties

TRUSTING BLINDY



20% trust their third-party vendors' privacy







CONSEQUENCES

The cost of a third-party breach is not just measured in short-term dollars and lost productivity, but long-term reputational damage and abnormal client churn.





44%

44 percent experienced a breach in the past 12 months involving a third party

15%

Only 15 percent were notified of the breach by the third-party responsible



27%

reduced productivity/efficiency

19%

reputational damage



14%

lost business from abnormal client churn

THE RISING TIDE: **A THIRD- AND NTH-PARTY WEB THAT DEFIES DIRECT**



Only 28% of respondents are confident their vendors notify them when data is shared with **nth parties**

YET

60% say they are confident they have full visibility into **nth parties** accessing their data





KEEP A WATCHFUL EYE ON NTH-PARTY VENDOR SPRAWL AND KNOWING WHERE YOUR DATA MIGHT LIVE

A comprehensive third-party risk management program is essential. eSentire can help you with:

- Reviewing and assisting in either the development or improvement of an ongoing Third-Party Risk Management program
- Conducting questionnaire-based risk assessments on specific third parties based on the core 15 areas of eSentire's Security Framework
- Interpreting and communicating the findings and develop a pragmatic plan for changes to reduce risk



eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than \$6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit www.eSentire.com and follow @eSentire.