OSTENDIO

Third Party Risk Real Talk

Partnering with third parties and vendors is essential to your success, but these partnerships may also be your greatest risk. What if you could secure your ecosystem and turn your greatest risk into your greatest asset?

The real world facts every serious security pro should know:

71%

of organizations say their third party network has grown in the last three years.
(source: Gartner)

91%

of breaches were linked to a third party vendor in 2021.
(source: CyberRisk Alliance)

83%

of executives report that third party risks were identified after initial onboarding.
(source: Gartner)

51%

of businesses have suffered a data breach caused by a third party.
(source: Ponemon Institute)

74%

of data breaches experienced by organizations in the last 12 months were a result of giving too much privileged access to 3rd parties.
(source: Ponemon Institute)

The Real World Impact

As a serious security professional, you know that monitoring your ecosystem is a lot of work. From accessing your cloud providers and apps to your purchasing vendors and supplies, there's a lot at stake. But when weaknesses go undetected, the impact can be felt across the organization.

2013 — TARGET

Breach
Hackers stole 40 million credit & debit card records, & 70 millions customer records.

Impact
18.5 million in fines, $10 million class-action lawsuit in 2015 and $10,000 to consumers who suffered losses from the breach. Ordered to develop and maintain better information security.

2020 — zoom

Breach
Attackers accessed confidential records, source code, trade secrets & highly sensitive information, including 500 million usernames & passwords.

Impact
Zoom banned across organizations. Compliance & reputational damage.

2021 — Microsoft

Breach
Microsoft Power Apps breached due to a default configuration that could be findable via search engine, which affected 38 million records containing personally identifiable information (PII).

Impact
47 organizations affected, including American Airlines, Ford & governmental health agencies. Time lost due to recoding product configuration & reputational damage.

Challenges You Can Overcome

Challenge #1
Vendors don't have the staffing to answer your questionnaires, so questionnaires go unanswered.

What you can do
Eliminate manual evidence mapping for your vendors, and simplify your assessments by creating questionnaires vendors can answer without external staffing. To accomplish this, use a security software that allows your vendors ease of access to your questionnaires where they can easily map evidence to relevant questions.

Challenge #2
Centralized Vendor Assessment Repositories can quickly become outdated or don't have sufficient information requirements for questionnaires.

What you can do
Leverage a solution that stores data in real-time so questionnaires have the most up-to-date information. For example, if a SOC 2 audit is already completed, evidence and documentation from that security audit can be mapped to the questions in a vendor risk assessment, saving you money and effort on vendor risk.

Challenge #3
Completing vendor assessments in spreadsheets and forms is a time-consuming and unreliable process.

What you can do
Make sure no vendor questionnaire goes unanswered again by leveraging a security software that involves everyone. Rather than relying on manual questionnaire completion, save time and resources by using a tool that includes your people and your vendors in championing your security, ultimately replacing manual spreadsheets and forms with simplified workflows.

Three Steps to People-First Vendor Risk Management

1

Track your organizational vendors & third parties.

Leave nothing to chance with a system that adequately tracks your third parties and vendors. Keep up-to-date data on your vendors' security capabilities and what data access they have.

2

Assess risk level with third party assessments.

Pay close attention to each risk level of your third parties and assess by risk category. Use a security platform to send third party assessments to your vendors and set the appropriate mechanisms and responses in place based on risk level.

3

Invest in people-first solutions for serious security pros.

Find an integrated risk management solution that protects everyone. Your people, your vendors, and your auditors. Third party risk management is more than an independent process. It's more than systems. It should identify weaknesses, give you complete visibility, and fully integrate into your security and compliance programs.

Everyone Secure.

How-to Guide: Building a Third Party Risk Management Program

Download this free eBook

to begin safeguarding your organization by building a third party risk management program that secures your ecosystem.