VCRI
THE VALUE CHAIN RISK INSTITUTE

VCRI LEARN · THIRD-PARTY RISK

Third-Party Risk 101: why vendor questionnaires fail

What third-party risk management is, why the spreadsheet approach breaks, and what better looks like.

Joshua Marpet and Cairn Viktor

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHY YOU CARE

Their breach becomes your breach

Target, 2013

Attackers first got in with credentials stolen from an HVAC and refrigeration vendor that had remote access to Target's network.

Kaseya VSA, 2021

Ransomware went through a flaw in IT management software used by managed service providers, reaching their downstream customers.

SolarWinds Orion, 2020

Attackers slipped a malicious file into a software update, signed with SolarWinds' own legitimate code signing certificate.

MOVEit Transfer, 2023

The CL0P ransomware gang exploited a flaw in a file transfer product and stole data from the databases behind it.

Sources: CBS News on the US Senate Commerce staff report (2014); CISA Kaseya guidance (2021); CISA alerts AA20-352A and AA23-158A.

valuechainrisk.org/learn · CC BY 4.0

THE BASICS

What third-party risk management is

- A third party is anyone outside your organization who touches your data, your systems or your operations.
- That includes suppliers, software and cloud services, IT providers, contractors, and the open-source code inside your products.
- Third-party risk management (TPRM) is the practice of knowing who they are, how much you depend on each one, and what happens if one fails.
- Your vendors have vendors too. Risk flows down the whole chain, not just one link.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

THE USUAL PROCESS

How most programs work

Most of the effort lands in one step: the assessment. And most assessments are a spreadsheet.

Inventory
List every third party you use.

→

Tier
Rank them by how much they can touch or break.

→

Assess
Ask about their security, usually with a questionnaire.

→

Contract
Write security terms into the agreement.

→

Monitor
Check again, usually once a year.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

THE QUESTIONNAIRE

“Do you require multi-factor authentication?” Yes.

The vendor types the answer. Nobody checks it. It goes in a folder until next year.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHY IT FAILS

Four structural problems

Self-attestation

The vendor grades its own homework. The incentive is to check every box, not to tell the truth.

Point in time

An answer is true, at best, on the day it was written. Systems and people keep changing.

No evidence

A “yes” is a claim, not proof. There is no setting, log or report behind it.

Every customer asks differently

Each customer sends its own form, so vendors spend their time on paperwork instead of security.

valuechainrisk.org/learn · CC BY 4.0

A CASE STUDY

What the Target report found

The risk lived in the access Target gave the vendor, not in anything the vendor wrote on a form.

The way in

A phishing email stole the HVAC vendor’s credentials.

That vendor had remote access to Target’s network for billing and project work.

The missed checks

The Senate staff report says Target rarely required two-factor authentication from its low-level contractors.

It also says alerts fired when the malware arrived.

Source: CBS News, “Senate report details Target’s missed chances to stop data breach,” March 25, 2014.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

YOUR VENDORS' VENDORS

Even the numbers need a definition

Change the definition and the answer moves by a factor of two to three. A single number on a form hides that choice.

13.1 million

open-source packages classified in VCRI's Q3 2026 State of the Supply Chain report.

36% or 52%

npm's risk-weighted rate of packages that are abandoned, archived, deprecated or superseded, depending on how you define "still maintained."

Source: VCRI, State of the Supply Chain Q3 2026, "Abandoned Is a Range," valuechainrisk.org/state-of-supply-chain/

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHAT BETTER LOOKS LIKE

Four upgrades

Evidence

Ask for what systems produce: settings exports, scan results, software bills of materials, not typed answers.

Continuous

Check on a rhythm that matches how fast things change, not once a year.

Shared

Answer once, share with every customer, in a format anyone can check.

Consequence-based

Spend the most effort on the vendors whose failure would hurt the most.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

QUESTIONS BECOME EVIDENCE

Swap the claim for the proof

INSTEAD OF ASKING	ASK TO SEE
Do you require MFA?	An identity provider export showing MFA enforced, including for contractors
Do you patch promptly?	Recent scanner results with dates
Do you track your software components?	The SBOM file itself
Do you have an incident plan?	The date and findings of your last exercise

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHAT TO DO MONDAY

Start small, start with access

- List the vendors that have accounts or remote access into your systems.
- Pick your top five by what they could reach or break.
- For each one, replace one questionnaire item with a request for evidence.
- Check that a second factor is actually enforced on every vendor account.
- Try a free, open scorer, such as VCRI's BeaconScore, to see what evidence-based grading looks like.

valuechainrisk.org/learn · CC BY 4.0

VCRI

THE VALUE CHAIN
RISK INSTITUTE

Free to use, teach and share.

This deck is part of the VCRI Learn series. Use it in your class, your team meeting or your chapter, with credit to The Value Chain Risk Institute.

valuechainrisk.org/learn

valuechainrisk.org/learn · CC BY 4.0