17-July-2024

How GSK is building NextGen TPRM Program

gsk.com

What we will discuss today?

Marek Jakubczak

Supplier Cyber Security Risk & Assurance Director

https://www.linkedin.com/in/marekjakubczak/

1. About GSK
2. Cyber threat landscape
3. Current state of play
4. What's NOT working
5. Future state

About GSK

We are a global biopharma company with a purpose to unite science, technology and talent to get ahead of disease together.

We aim to positively impact the health of 2.5 billion people by the end of the decade, as a successful, growing company where people can thrive.

GSK.COM

GSK

Third Party Security Risk

Data Breach Costs

$9.5 trillion USD

Cybercrime is predicted to cost the world $9.5 trillion USD in 2024

To put this figure into perspective, consider that the entire budget for the United States federal government in fiscal year 2023 was approximately $6.27 trillion USD.

This means the financial impact of cybercrime in one year is projected to be about **1.5 times** the U.S. federal government's annual budget.

Pharmaceutical sector

USD 5.2M

average cost of a data breach reached an all-time high in 2023 of USD 5.2 million

27%

Increase in reported cyber incidents over the previous year

Per-record cost

In 2023, the average cost per record involved in a data breach was USD 180

48%

of breaches involved the theft of intellectual property

Ponemon Institute's "Cybersecurity in Pharmaceuticals Report
Deloitte's "Cyber & Strategic Risk in Pharmaceuticals
Marsh & McLennan's "Cyber Risk in the Pharmaceutical Industry

Third Party Security Risk

Supply Chain Risk – A Growing Necessity

The concept of Third Party Security Risk Management (TPSRM) is relatively new but increasingly critical in today's interconnected business landscape.

75% of organizations have some form of TPSRM program in place

29% of organizations considered their TPSRM programs to be mature

53% of companies identified third-party vendors as a significant source of cyber risk.

ISACA 2023 State of Cybersecurity Report

50% Over 50% of data breaches involve third-party vendors

40% The cost of a third-party cyber breach is typically 40% higher than the cost to remediate an internal cybersecurity breach.

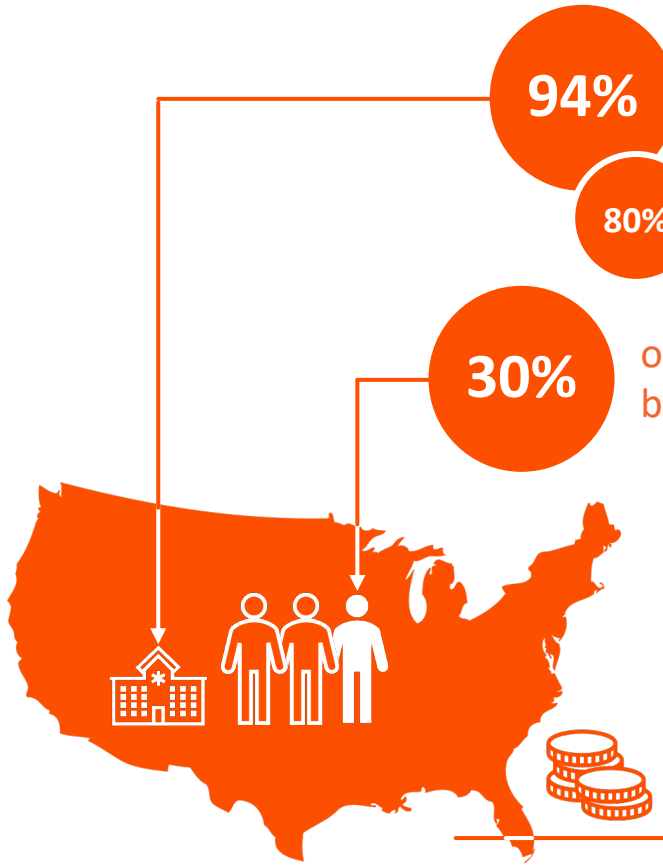
73% Nearly three-quarters of businesses experienced a significant disruption due to a third party in the last three years

Ponemon Institute's Cost of a Data Breach Report
Verizon Data Breach Investigations Report (DBIR)
Deloitte's 2023 Global Third-Party Risk Management Survey

GSK

Third Party Security Risk

Recent notable breach



US Population: 342 million

CHANGE HEALTHCARE

- 5,500 Hospitals & Health Systems
- $1 tryllion Healthcare Claims
- 14 Billion Healthcare Transactions
- 117,000 Dentists
- 2,100 Payer Connections
- 600 Laboratories
- 800,000 Physicians

Estimated Materiality Assessment

Primary Cost

$1.44 B	$1.94 **Billion**	$2.44 B
(Minimum)	(Most Likely)	(Maximum)

Before factoring cyber insurance claims

HowMaterialIsThatHack.org

GSK

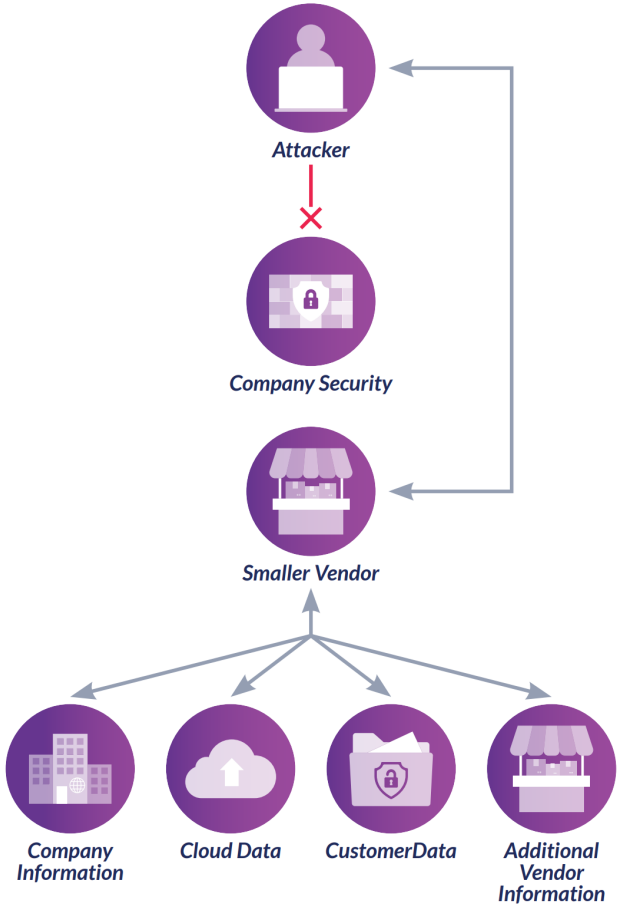
Third Party Security Risk

Supply Chain Attacks on the Rise

How a Supply Chain Attack Works

Rather than attack a single large organization – a large multi-national corporation with a well-resourced cybersecurity program, criminals will attack a smaller vendor with less security protections that supports the same large multi-national company along with many other businesses.

A supply chain attack can come in the form of breaching a single organization and stealing information from multiple companies or using flaws in a single product or service used by multiple companies to access the personal information stored in their databases.



ITRC 2023 Annual Data Breach Report

Third Party Risk Management

What, When and How

TPRM

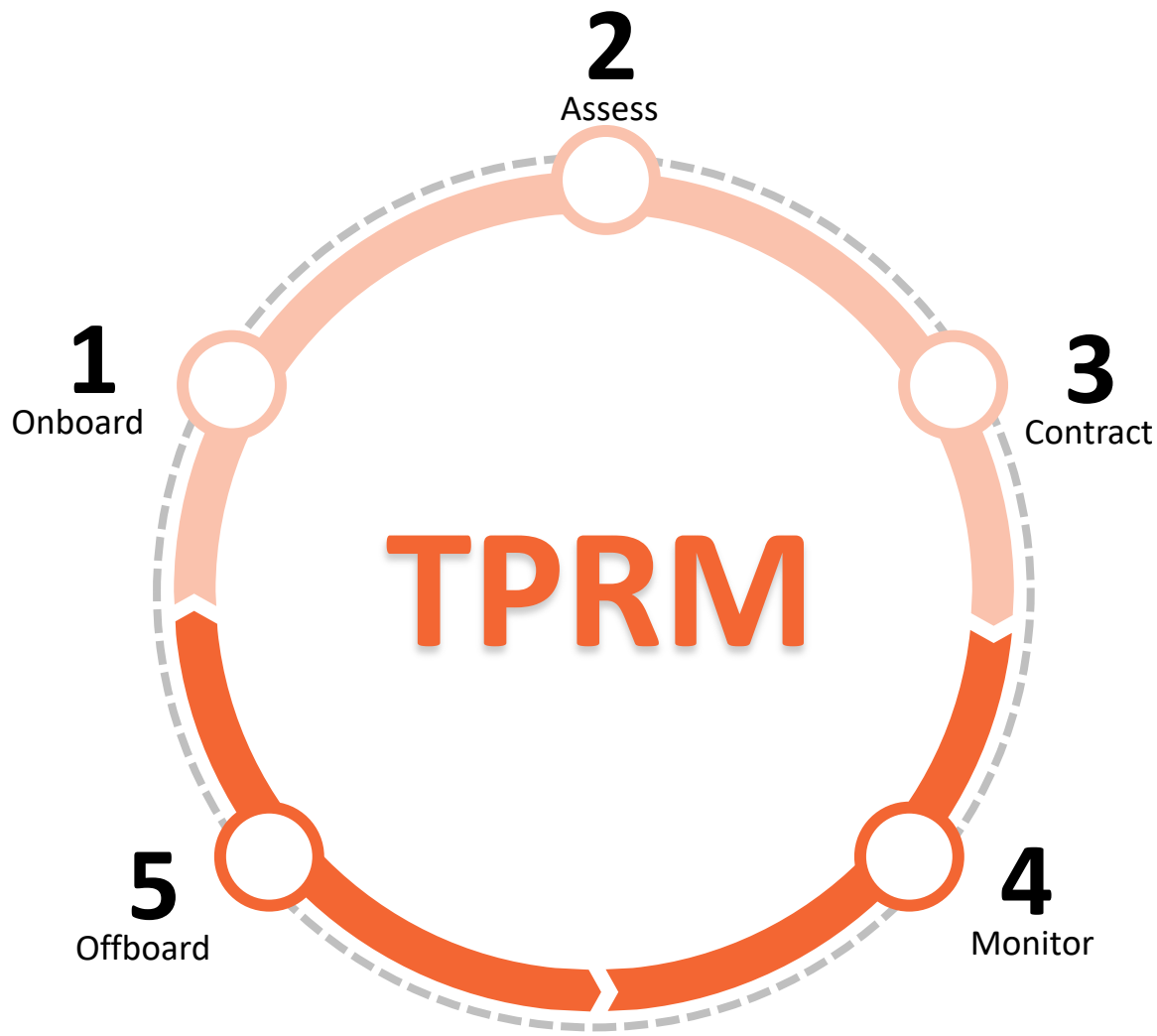
Third Party Risk Management is the process of identifying and mitigating risks introduced by third party vendors.

Risk areas

- Sanctions
- Privacy
- Labour Rights
- Human Safety Information
- Environment Health and Safety
- Information and Cyber Risk
- Inappropriate Promotion

and more...

Third Party Security Risk is one of risks evaluated by TPRM



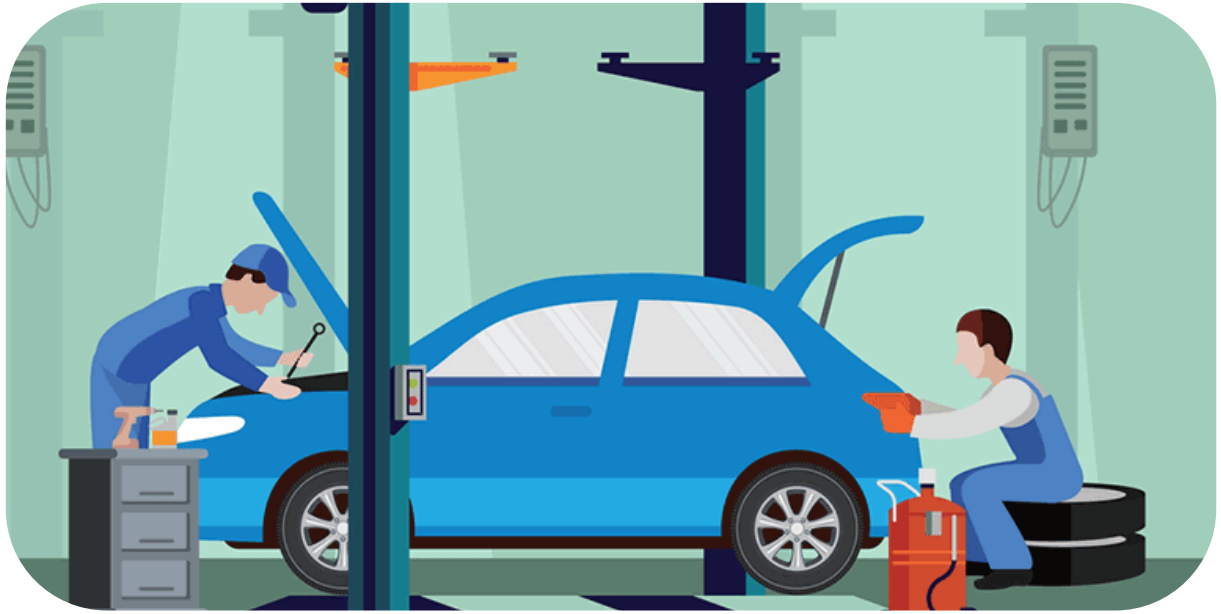
Pre-contract activity | Post-contract activity | Technology

Third Party Security Risk

What and Why?

What is Third Party Security Risk?

Third Party Security Risk refers to the potential threats and vulnerabilities that arise when organizations rely on external vendors, suppliers, or service providers. These risks can affect the organization's data, systems, and overall security posture.



How we evaluate Third Party Security Risk?

Third party risk can be evaluated by conducting **third party security assessment**.

Think of third party security assessment like a regular car safety check. Before a car can be safely used on the road, it must go through a series of inspections to ensure it's in good condition.

A third party security 'check' includes:

- Reviewing security policies and practices to ensure the third party has robust security controls in place.
- Reviewing compliance documentation (e.g., ISO 27001, SOC 2 report) to verify adherence to industry standards.
- Analyzing external signals (e.g., through automatic scoring tools) to confirm if a third party has a mature security posture.

Third Party Security Risk

What is working? What is NOT working?

NOT Working

- Questionnaire based
- Time consuming (avg 2-4 weeks)
- Point in time
- Not 100% reliable
- Tools that scan the external presence
- Too many false positives
- No actionable insights based on risks
- Don’t want to become vendor’s security department
- No strong partnership with vendors

Working

- Vendor classification (critical, high, medium, low)
- Vendor relationships

Third Party Security Risk

The NextGen TPRM must be… Data driven... Risk based... Continuous...

CISO	BISO	Business Risk Owner	Incident Response	Threat Intelligence	Third Party Risk Assessor
• What is external risk? • What I worry about? • What I worry about?	• What are most risky TPs? • What I worry about? • What I worry about?	• What are most risky TPs? • What I worry about? • What I worry about?	• Need TP details to manage TP incident? • What I worry about?	• What are most risky TPs? • What I worry about? • What I worry about?	• What are my priorities? • How am I performing? • What I worry about?

First party ⟷ Third party

Third parties within our environment

- Third party developers and administrators
- Third party users of applications
- Third party infrastructure
- Connectivity details

External view on Third Party

- External security posture
- Third party incidents
- Third party data leaks
- Internal & external threat intelligence

Inside-out view from within Third Party

- Questionnaires
- Data flow assessments
- Direct feeds from third parties (telemetry)
- External attestations & other evidences

GSK

gsk.com