RISK LEDGER

Supply Chain Risks Insight Report

Data protection

February 2021

riskledger.com

Data Protection in the supply chain

Data protection in the supply chain is a particular challenge for information security and compliance professionals because breaches often lead to real world, negative impacts for consumers and significant costs for breached organisations.

The introduction of specific supply chain risk management obligations in landmark data protection and privacy legislation such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) means that it is crucial for organisations to:

- explicitly set out exactly what their third parties do with shared data; and
- assess the security controls in place to protect that data.

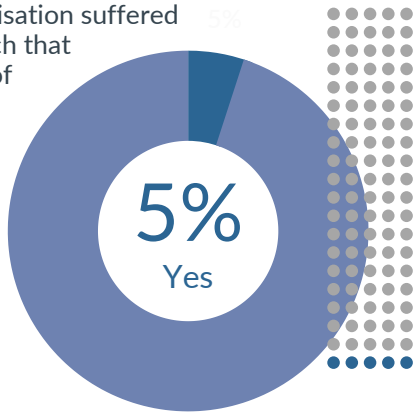
This report looks at how data protection risk controls are applied by suppliers based on the data protection section of Risk Ledger's full Supplier Assessment Framework (SAF)[1] - developed with support from the National Cyber Security Centre (NCSC).

Highlights

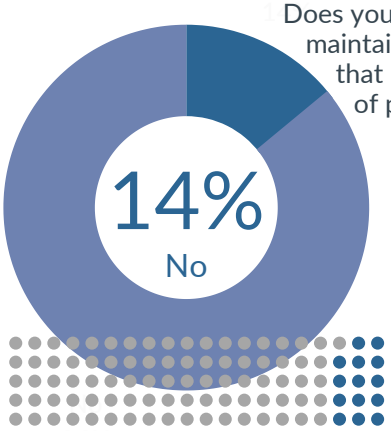
- A small but consistent percentage of suppliers have a dangerously cavalier attitude towards data protection.
- Cyber Essentials certification for suppliers isn't enough to effectively mitigate third-party risks.
- There are GDPR breaches (and fines) waiting to be uncovered in your supply chain caused by third parties failing to implement sufficient data protection controls.

Data Snapshot

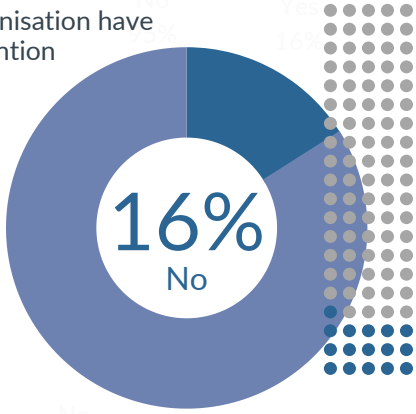
Has your organisation suffered a security breach that led to the loss of any Personal Data in the last 6 months?



Does your organisation maintain a breach log that records losses of personal data?

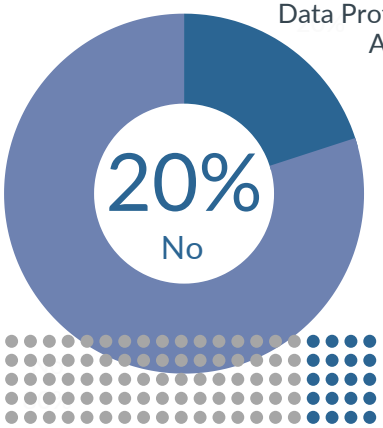


Does your organisation have a Records Retention Policy?

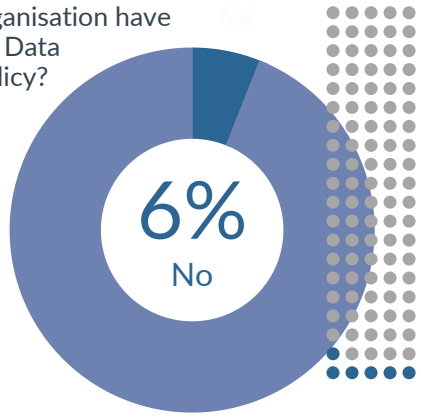


[1]This insight report takes a close up look at data protection risk controls in the supply chain ecosystem as reported directly by suppliers who use the Risk Ledger third-party risk management network to share supplier risk assessment data with their clients. Data analysed for the report has been collected from 600+ suppliers of all sizes representing a broad range of industries and is a strong reflection of the supply chain risks facing most enterprises.

Does your organisation conduct Data Protection Impact Assessments as part of its risk assessment processes?



Does your organisation have an up-to-date Data Protection Policy?



8% of suppliers with a Cyber Essentials certificate have suffered a security breach that led to the loss of personal data in the past 6 months.

4% of suppliers don't have a Data Protection Officer or a data protection policy.

7% of suppliers who don't conduct Data Protection Impact Assessments have suffered a security breach that led to the loss of personal data in the last 6 months.

11% of suppliers don't have a defined and documented lawful basis for each instance of collecting/processing personal data they conduct.

1 in 10 suppliers have no process in place for notifying their information Supervisory Authority or other relevant parties if they suffer a data breach and 75% of those suppliers don't even maintain a breach log that records losses of personal data.

10% of suppliers who transfer personal data outside of the UK and EEA don't conduct Data Protection Impact Assessments.

Recent third-party data protection fines

€80,000 GDPR fine for Italian hospital

£250,000 GDPR fine for UK medicine distributor

Haydn Brooks
CEO, Risk Ledger

Thoughts of a supply chain risk specialist

If I put myself in the position of a senior informational security or compliance manager at a large organisation, the most worrying aspect of this report is the 5-10% of the supply chain ecosystem who have failed to implement a minimum standard data protection regime. This cohort expose their clients and consumers to serious, but avoidable, data breaches, fines and/or clean up costs.

I am also concerned that many third-party risk managers don't actually know these easily mitigatable risks are lurking in their supply chain because they don't have access to granular data and evidence assessing their suppliers' data protection regimes.

I am seeing an over-reliance on Cyber Essentials and other certifications despite the data showing they aren't reducing the probability or number of breaches. It's why Risk Ledger exists!

My advice to those responsible for managing data protection in the supply chain is to quickly find a tool to get visibility of actionable supply chain risk data, such as the Risk Ledger platform, and act fast on the glaring gaps.

Upgrade your third-party risk management programme

Risk Ledger gives organisations of all sizes the tools to identify, measure and mitigate third, fourth, and fifth-party supply chain risks. We use a combination of smart workflows, technical automations, and real-time data to give you the visibility you need to protect your supply chain.

See why clients like BAE Systems AI, ASOS and Scottish Widows Schroder's Personal Wealth are all using the Risk Ledger platform.

Watch a 3 minute demo video

Contact us

Risk Ledger Ltd,
7-10 Adam St,
London,
WC2N 6AA,
United Kingdom

Published February 2021

riskledger.com