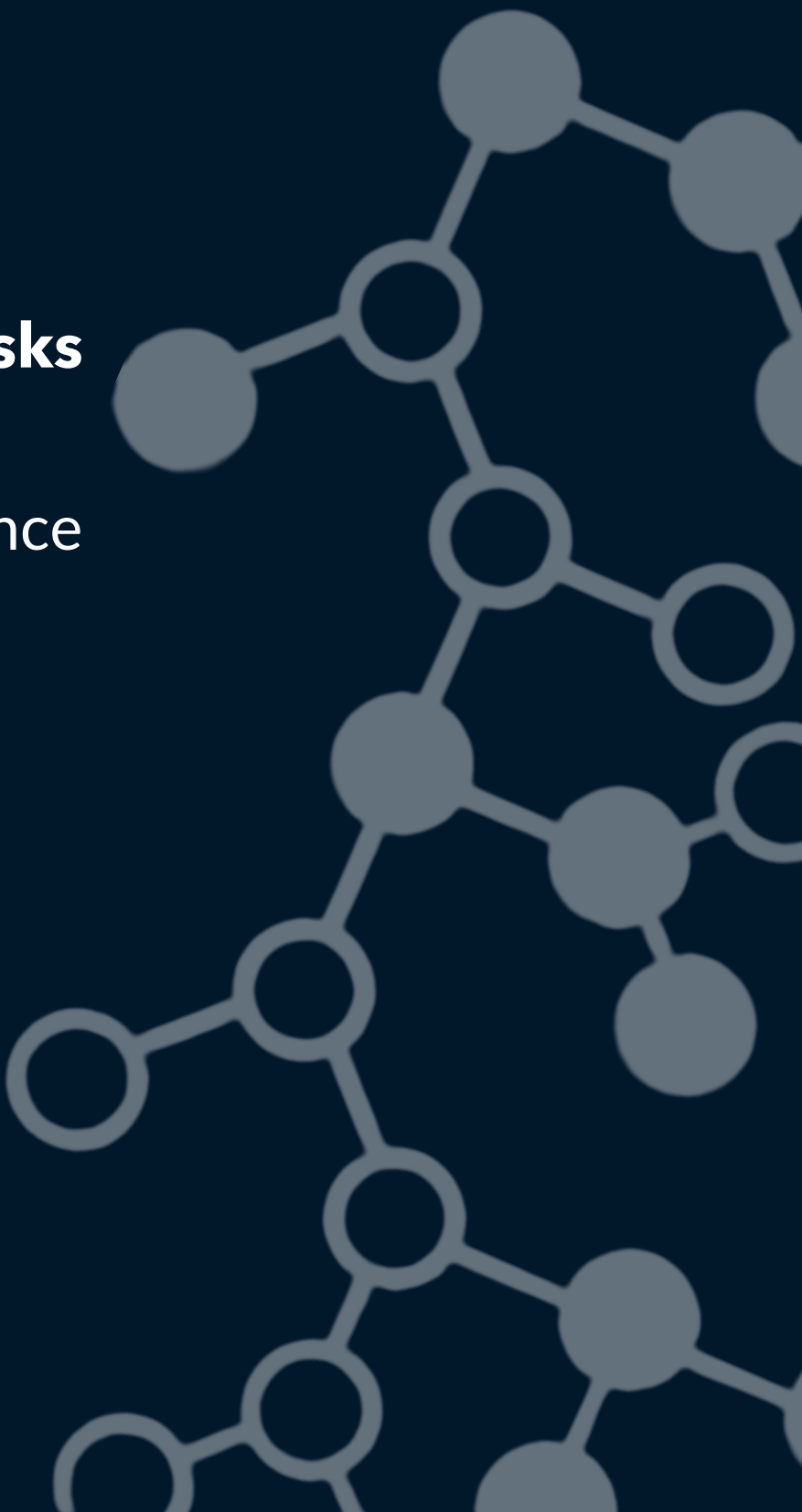
RISK LEDGER

# Supply Chain Risks Insight Report

## Security Governance

2021



riskledger.com

# Thoughts of a supply chain risk expert

**Haydn Brooks**
**CEO, Risk Ledger**

In our Supply Chain Risks Insight Report - Data Protection, I noted that third-party data protection risks loomed large from a small but significant proportion of suppliers whose poor implementation of risk controls is leaving their clients at risk of fines and other enforcement actions from regulators. Given the insights uncovered in this report, it is clear that many of the gaps identified in the data protection regimes of the problem cohort of suppliers could probably be explained by a poor security governance regime.

It is staggering to see that approximately 1 in 5 organisations don't have an information security policy, a backup policy or a formal remote working policy that includes security - over a year into a pandemic that has forced millions of people to work remotely!

I recognise that policies are not the be all and end all of information security. However, I take the view that while they might be necessary but not sufficient for a good information security regime, their wholesale absence is sufficient for a bad one and this is something that must be taken into account by professionals running a third-party risk management programme. Should your organisation be sharing data with or relying on the 18% of suppliers who don't have and implement a Backup Policy?

Policies define and underpin the implementation of risk controls within operational teams. When they don't exist, an organisation's security regime is disorganised at best and inconsequential at worst. For third-party risk managers, it is also important to consider how your suppliers communicate their information and cyber security policies to employees and their own supply chain. There isn't much chance of adhering to a policy they have never seen!

In cyber security, we constantly talk about layering security controls so that multiple layers combine to minimise the chances of a successful security breach. We can see from the insights and examples in this report that this also works in the other direction - if multiple basic security governance controls are missing, their absence combines to exponentially increase the possible attack vectors available to bad actors.

Third-party risk managers must consider this compound effect when reviewing a supplier if they are fortunate enough to have access to this level of granular risk control data on a supplier by supplier basis. If they don't, step one should be finding a third-party risk management solution that provides them with it.

One final note. What does a good information and cyber security regime actually look like? In 2019, Risk Ledger won the NCSC's Cyber Den innovation competition at the Cyber UK event and our reward was material support from the NCSC to develop our product. They supported us to refine this Supplier Assessment Framework which sets out what a good security regime should look like. Check it out. I welcome feedback so click on my photo above to connect on LinkedIn.

# Security Governance in the Supply Chain

Security governance is the setting of policies, processes, responsibilities and structures that provide the framework for an organisation to achieve its strategic security objectives. Good security governance coordinates the security activities of an organisation to ensure all relevant security risks are being managed and the flow of security information facilitates good decision making.

For professionals concerned with managing third-party risks, good security governance in the supply chain is foundational to cyber resilience. A comprehensive, joined-up security governance regime is a strong indicator of a third party that takes securing themselves, and protecting their clients, seriously.

When assessing the security governance of a third party or a prospective supplier, risk managers should consider whether they can:

- identify a link between the security activities the third party can evidence and their business priorities;
- identify all the individuals responsible for making security decisions in the organisation;
- see evidence of accountability and feedback loops; and
- see an approach to security governance that is on par with other important business governance domains.

This report looks at how security governance controls are applied by organisations across the supply chain ecosystem based on the Security Governance Section of Risk Ledger's full Supplier Assessment Framework (SAF)[1] - developed with support from the National Cyber Security Centre (NCSC).

## Highlights

- 1 in 10 organisations don't have an internal or external resource setting out the security risks they should be managing. They have simply not considered how to effectively govern security in their organisation.
- Despite being over a year into a pandemic-induced, mass working from home experiment, 19% of organisations still do not have a documented Remote Working Policy setting out rules and expected behaviours to mitigate the additional risks of working at home.
- Mobile devices are becoming increasingly integral to the work place but 21% of organisations don't have a policy governing their use.

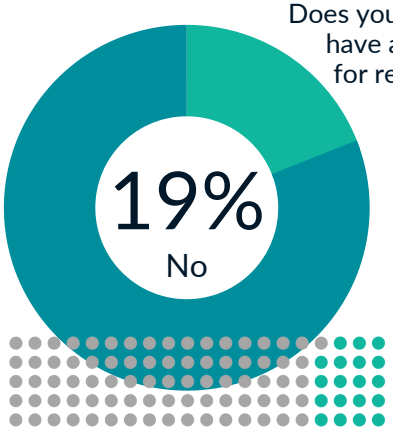


[1]This insight report takes a close up look at security governance risk controls in the supply chain ecosystem as reported directly by suppliers who use the Risk Ledger third-party risk management network to share supplier risk assessment data with their clients. Data analysed for the report has been collected from 700+ suppliers of all sizes representing a broad range of industries and is a strong reflection of the supply chain risks facing most enterprises.

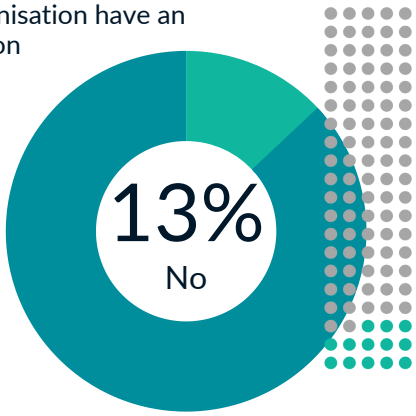
# Data Snapshot

These anonymised statistics are drawn directly from the aggregated data shared by suppliers on the Risk Ledger platform. Click on each one to find out more about that security governance risk control.

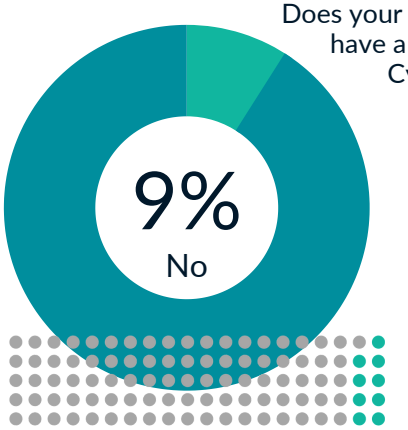
Does your organisation have a formal policy for remote working that includes security?



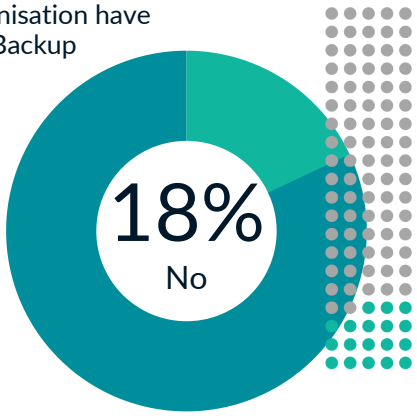

Does your organisation have an appointed person responsible for information security, such as a CISO?



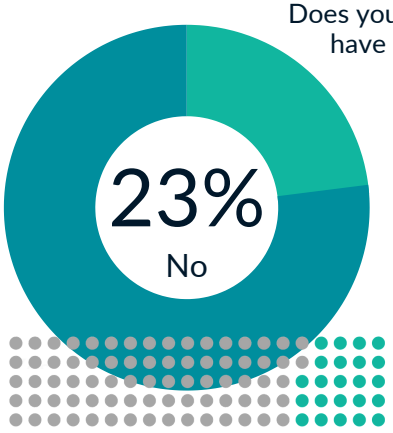

Does your organisation have a documented Cyber Security Policy or Information Security Policy?



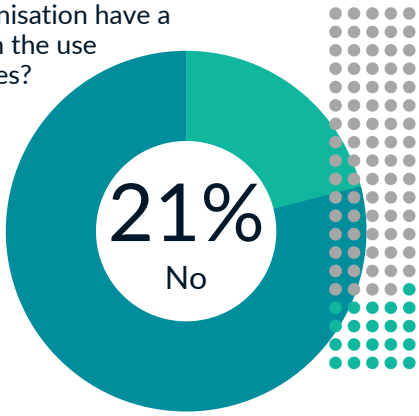

Does your organisation have a documented Backup Policy?




Does your organisation have a documented Information Classification Policy?




Does your organisation have a formal policy on the use of mobile devices?



# Insights

**10% of suppliers don't have an appointed person responsible for information security and don't conduct an annual, independent information security review.**

## They're flying solo... and blind

Both controls work hand in hand to allow an organisation to consistently identify, measure and mitigate security risks.

Without either, these organisations cannot effectively implement and maintain the appropriate risk controls relevant to their organisation and it is likely they wouldn't actually know if they were breached - and neither would their clients.

## Consider this simplified example

Payrollco is a medium-sized business that offers clients an outsourcing service for all payroll related administration. This includes the transfer of sensitive Personally Identifiable Information (PII) from clients to Payrollco. The company has just over 100 staff but has outsourced its IT support function after employing an IT consultancy to set up their IT infrastructure. They have an Office Manager who manages the relationship with these external IT resources when they are needed.

They were set up with an on-premises Microsoft Exchange Server several years ago. On 2 March 2021, Microsoft announced four critical zero-day vulnerabilities that impact multiple versions of Microsoft Exchange Servers including the one used by Payrollco. They also released patches and technical guidance for these vulnerabilities with the advice to implement the patches immediately to avoid exploitation by bad actors.

Payrollco doesn't have a member of staff or a contractor responsible for information security and they haven't conducted an independent security review of the organisation so the risk of using an email server that isn't properly maintained has never be identified or mitigated.

Currently, no member of staff at Payrollco is aware that the entire organisation, including client data, is vulnerable to an extensive cyber attack.

~~Do it securely~~
Do whatever is easiest

The lack of an Information/Cyber Security Policy fosters a 'do whatever is easiest' attitude within an organisation which does not adequately take security into account.

In many organisations, more systems and data are now in the cloud than on premise and it is poorly understood that many web and app-based services fall into this category too.

**9% of suppliers don't have a documented Information/ Cyber Security Policy and don't have a documented policy governing the use of cloud services.**

Without explicitly defining and enforcing which cloud-based services can be used and their terms of use, employees use them on a whim, leaving IT or security colleagues out of the loop and the appropriate risk controls are not implemented.

The absence of both policies makes it incredibly easy for sensitive data, including client data, to inadvertently end up on external cloud systems without any controls or awareness of the risks.

### Consider this simplified example

An Account Manager at Payrollco sends the 15 clients she manages a monthly report including all the payslips and other correspondence Payrollco has sent to the client's employees for the month. The bulk export feature on her system downloads each piece of correspondence as an individual PDF. To make life easier for her clients, she uses a free online tool to join all the individual PDFs she wants to send into a single PDF. The company does not have a policy governing the use of cloud services or an Information Security Policy.

Freepdfjoiner.com's business model is to make a simple but useful business tool available on their website and generate advertising income from the web traffic.

However, the tool was not designed with security in mind. When users upload their documents, a copy of each document is stored in an AWS S3 bucket in perpetuity and the S3 bucket has not been secured.

The Account Manager has been doing this for every client she has ever worked with at the company, every month, for 7 years.

## Easy Access... and lots of it

**8% of suppliers don't have a documented access control policy and do not technically enforce a password policy.**

The purpose of a password policy is to establish standards to ensure passwords are relatively strong, including, but not limited to, factors such as length, complexity requirements and change intervals.

Technically enforcing these controls ensures these criteria are adhered to as it is difficult to validate that rules are being followed and there will always be instances of weak passwords within an organisation if employees are given the freedom to chose indiscriminately.

If a password policy doesn't exist or isn't technically enforced and the organisation doesn't have an access control policy, the potential for security breaches increases exponentially as bad actors exploit stolen credentials across an organisation's IT estate for an attack or reconnaissance.

### Consider this simplified example

Payrollco's Finance Director has been with the company since it's founding and she has been using the same password since then too. She has said on numerous occasions: "It is simply not humanly possible for anyone to know or guess my trusty password - I use it for everything." The company does not have a Password Policy.

In the early days, the Finance Director was added as an admin user to every software and online service to manage payments and track spending but as the company grew, this continued out of habit. They do not have an Access Control Policy.

Unbeknown to Payrollco's Finance Director, her personal details have been leaked in several data breaches at companies that did not encrypted their users' passwords. She has used the same 'un-guessable' password across each one of those breached services and now her personal details including most common password and a link to her LinkedIn profile are on a target list for a group of cyber criminals skilled in Business Email Compromise (BEC) attacks.

**14% of suppliers don't have a documented backup policy and do not technically prevent the use of removable media.**

## When it's gone, it's gone!

Ransomware cyber attacks accounted for approximately 18% of the all reported cyber attacks in 2020 according to the Identity Theft Resource Centre. Palo Alto Network Unit 42's Ransomware Threat Report 2021 highlights that one of the main reasons organisations hit by a ransomware attack are forced to pay is the lack of recoverable backups.

This report is being published in Spring 2021 as organisations around the world prepare to return, at least in some limited way, to offices after the Covid-19 pandemic necessitated the largest and longest work-from-home experiment ever seen or imagined globally. For some employees who have been working on non-work issued devices during this period, the return to the office also means tackling the transfer of files from those non-work issued devices to computers on the corporate network. Apart from all the other risks that stem from the use of removable media in a business environment, the risk of introducing malware, stored unknowingly on personal, removable media, to corporate networks is huge and needs to be managed.

For the 14% of suppliers who don't have a documented backup policy and do not technically prevent the use of removable media, the potential for a catastrophic and costly ransomware attack or another security breach is vast and any clients relying on them to secure sensitive data or provide services will also suffer.

### Consider this simplified example

Payrollco's Finanace Director has been working from home on her personal laptop because it is faster than the laptop issued by work.

Her personal data has been on several cyber crime target lists and one criminal gang online has used the available information to create a spear phishing campaign against her with malware disguised as an excel spreadsheet. It didn't look urgent so she didn't open the excel attachment but downloaded it to look at after the end of the quarter in two weeks time when she will be less busy.

The Finance Director is preparing to return to the office part-time after Easter and plans to transfer her work files, including the malicious excel spreadsheet, from her personal laptop to her work computer using a USB flash drive she received at a conference just before the pandemic.

## 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.

Find out more about Risk Ledger

Contact us



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

Published March 2021

riskledger.com