RISK LEDGER

The State Of Security: Finance

Analysis into the security posture of finance industry suppliers

Introduction

Increasingly, financial organisations are insisting that their suppliers adhere to strict security guidelines in a bid to ensure that their own business isn't damaged by a cyberattack that involves a supplier. Since financial organisations often have mature security measures in place, attackers are likely to target suppliers as a way to circumvent those controls. This makes supply chain attacks a particularly high risk for financial organisations when compared to other industries.

Supply chain attacks can take a number of forms:

- If a supplier has direct access to your internal systems - whether by design or due to oversight on your part - then once an attacker has access to your supplier's systems, they can easily move laterally to your systems.

- Your supplier may have your data stored on their systems, which attackers can steal once they've broken into the supplier's network without ever having to breach your defences.

- An attacker might leverage your trust in your suppliers by impersonating them in a phishing attack, or even attempting to access your buildings.

According to data from Black Kite, this year alone there have been 53 breaches where the attackers got in through the systems of a third party supplier - and, according to the European Union Agency for Cybersecurity, the volume of supply chain attacks is growing rapidly.

This report shares insights into which measures suppliers to the financial services industry are taking to keep themselves secure. You could use this information to benchmark your own suppliers to understand how they are doing compared to other suppliers you might use - and, of course, it may also give you food for thought in your own security posture.

Methodology

Risk Ledger is a supply chain security platform enabling organisations to share risk information and collaborate on improving security and risk controls. Over 3000 organisations are currently using Risk Ledger to run their supply chain assurance programmes, or to showcase their security controls to their clients and customers.

When a supplier creates a free profile on Risk Ledger they answer a series of questions on the controls they have in place. Every supplier profile is structured around the same standardised control framework, which allows us to pull out trends across different industries and geographies.

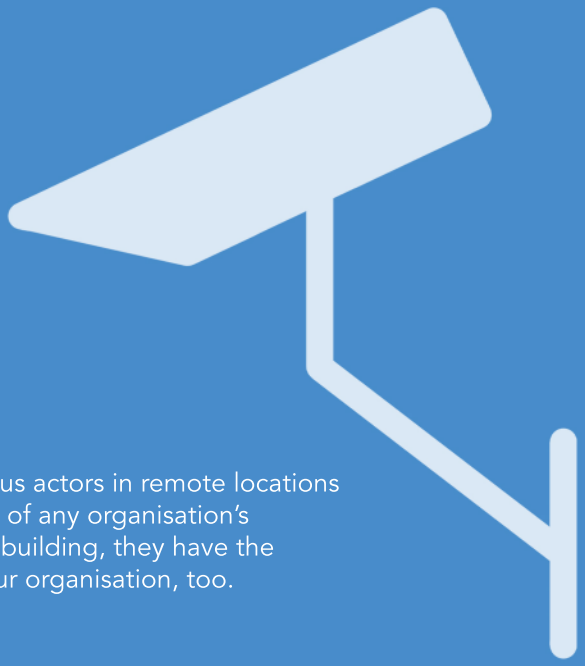
To write this report, we analysed data from all organisations on Risk Ledger who supply the financial services industry - 218 organisations in total. The supplier organisations represented in this report are largely based in the UK and Europe, but include organisations across the world, including the United States, Australia and India. The data was pulled from the platform in November 2022

Page 6 of this report contains data on the use of unsupported systems across different industries. This includes data from all 3000 suppliers on Risk Ledger, which gives a comparison of the financial services industry against other industries.

We've broken this report into five major sections: physical security, cybersecurity, cyber resilience, third-party risk management, and data protection. This report contains anonymised aggregated data and highlights a cross-section of control areas. Organisations using Risk Ledger for their supply chain risk management are able to analyse information across all controls, apply their own policies to give contextual risk for their organisation, and communicate directly with suppliers about control improvements or risk concerns.

If you would like to access this data for your suppliers, please get in touch with a member of the team.

Physical Security



It's easy to think of information security as purely about stopping malicious actors in remote locations from getting into your systems. Of course, physical security is a vital part of any organisation's information security posture. If an attacker can get inside your supplier's building, they have the potential to cause a lot of damage quickly - which in turn could harm your organisation, too.

36% of organisations do not require visitors to undergo an ID check on arrival at all premises

Q: Does require visitors to undergo an ID Check on arrival at all premises?
(This question is only asked of businesses who own/manage physical premises)

The reception desk is the first line of defence against physical attacks, including attempts to access an organisation's network, devices, or people. An ID check is a simple layer of security that can go a long way towards keeping malicious actors out of the building.

If your suppliers are in that third of organisations that don't use ID checks, then you know they are at greater risk of an attacker managing to steal data or gain access to your supplier's systems from within their building.

Be very careful about what data you send them, or what systems you give them access to - especially if their offices are based in a densely populated area where anyone an get in.

29% of organisations are unable to remotely wipe company data on laptops

Laptops are great, but they can be stolen or lost much more easily than desktop machines. If a supplier's laptop goes missing, then it's not just their data that's at risk - it could well be yours, too.

Device wiping is one of the surest ways to keep data from falling into the wrong hands (ideally accompanied by other controls such as hard drive encryption). Yet nearly a third of organisations can't do it.

That means that if they lose a laptop containing client data on it, they can't stop anyone who can get into the laptop from accessing the data.

Q: Can yourorganisation remotely wipe company data on laptop devices?

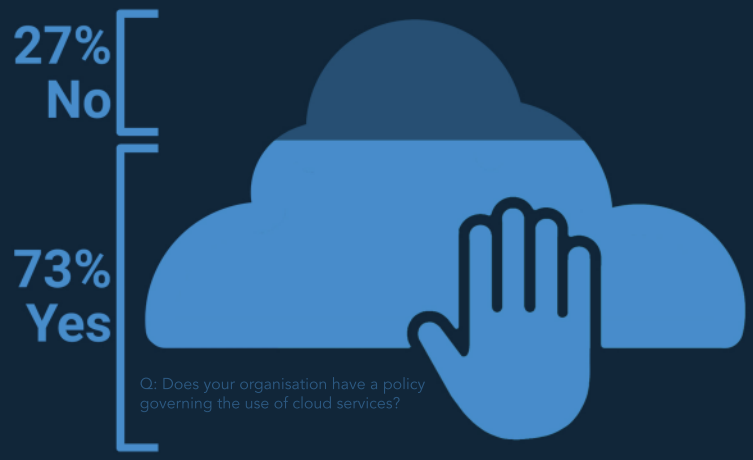
Cybersecurity

OK, now we're talking about remote threats from malicious actors ranging from nation states, to criminal gangs, to lone wolves. With supply chain attacks such as Okta and GitHub making headlines this year, there is no time for complacency when it comes to your suppliers' cyber defences.

27% of organisations do not have a policy governing the use of cloud services

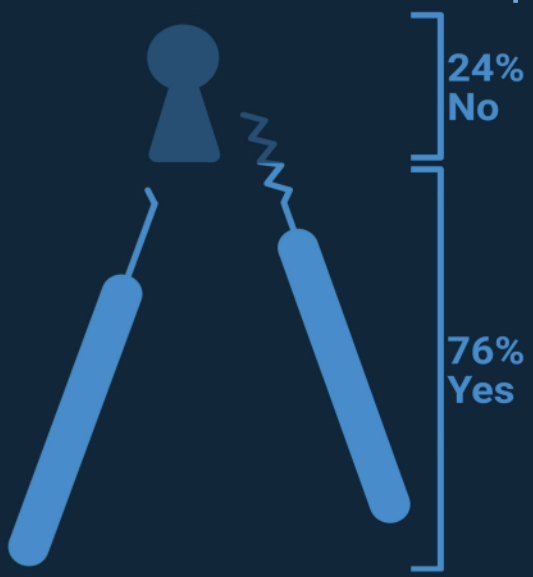
Thales reports that 45% of organisations experienced a cloud-based data breach in 2022. Organisations can take steps to use the cloud safely - but those steps will only work if everyone knows them and follows them. That's the role of a cloud services policy.

The policy will document any laws employees need to comply with, how to securely choose, procure, and start using cloud services, and what to do in the event of a breach or similar incident. If your suppliers don't have a document like this, they could be opening themselves up to a breach similar to Accenture's or Kaseya's last year - which could put you at risk as well.



Q: Does your organisation have a policy governing the use of cloud services?

24% of organisations do not conduct regular penetration testing (or red teaming) of internal systems



Q: Does your organisation conduct regular penetration tests of any applications or systems that it develops?

Most companies conduct pen testing and/or red teaming at least annually - but they often only test their perimeter defences. Nearly a quarter of suppliers on Risk Ledger don't conduct similar tests on their internal systems - meaning that if an attacker got past the perimeter, they may have free rein in that supplier's systems.

We're in the age of defence in depth; nobody can assume that their perimeter is secure. Suggest to your suppliers that they implement defences designed to address every stage of the Cyber Kill Chain®, for example limiting movement between systems walling off important data, so that even if an attacker gets into their systems, they can still be found and stopped before they do harm. And, of course, those defences need testing just as much as your perimeter defences do.

Cybersecurity

Four-fifths of organisations use forced TLS

Q: Have your organisation configured its email services to use enforced TLS?

Transport Layer Security (TLS) is an encryption method that protects online communications. Organisations can set their email servers to only send emails via TLS, or to use SMTP if the sending server cannot make a TLS connection with the receiving server. Forced TLS is obviously more secure - but can lead to email deliverability issues.

81% of suppliers are using forced TLS, indicating that they are prioritising security in their email communications.

That's encouraging news, and means that you need to ensure you set up your own email servers correctly in order to send and receive email from that supplier. If your supplier doesn't use forced TLS, it's not necessarily a bad thing - but it means you should consider alternative secure communication channels such as Mimecast for sharing sensitive information.

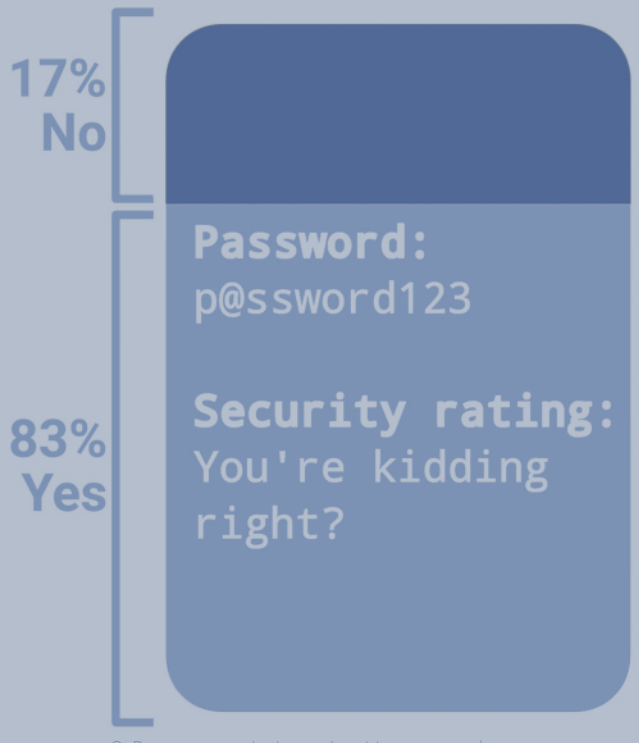
17% of organisations don't use a password manager to ensure complex, single-use passwords

Passwords are the bane of everyone's lives. Bad passwords are incredibly easy to crack, and once they are cracked, an attacker has complete access to whatever system they have broken into - and the data it contains.

Combined with other vulnerabilities such as poor cloud governance, weak passwords can bring an organisation - and its customers - to their knees.

Many organisations use password managers to make it easy for users to create and store highly secure passwords - and ensure that they don't reuse passwords across multiple accounts.

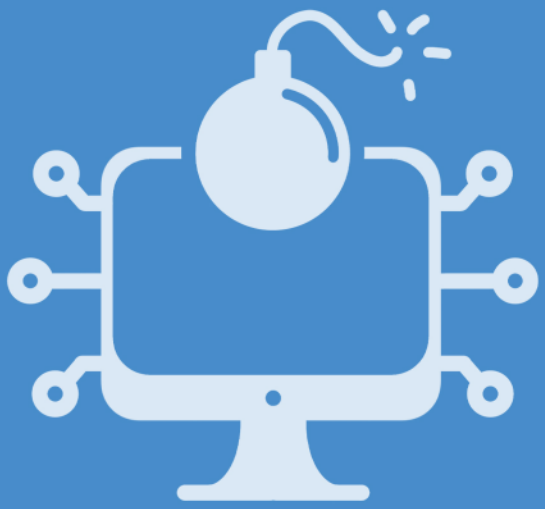
Unfortunately, 17% of suppliers on Risk Ledger still rely on users to create and remember their passwords, which inevitably leads to weak passwords or passwords used across multiple systems. That means an attacker will have a much easier time getting into your supplier's systems - either to steal data or perform other malicious activities without detection.



Q: Does your organisation use/provision a password manager to ensure passwords are of the required complexity and only used once?

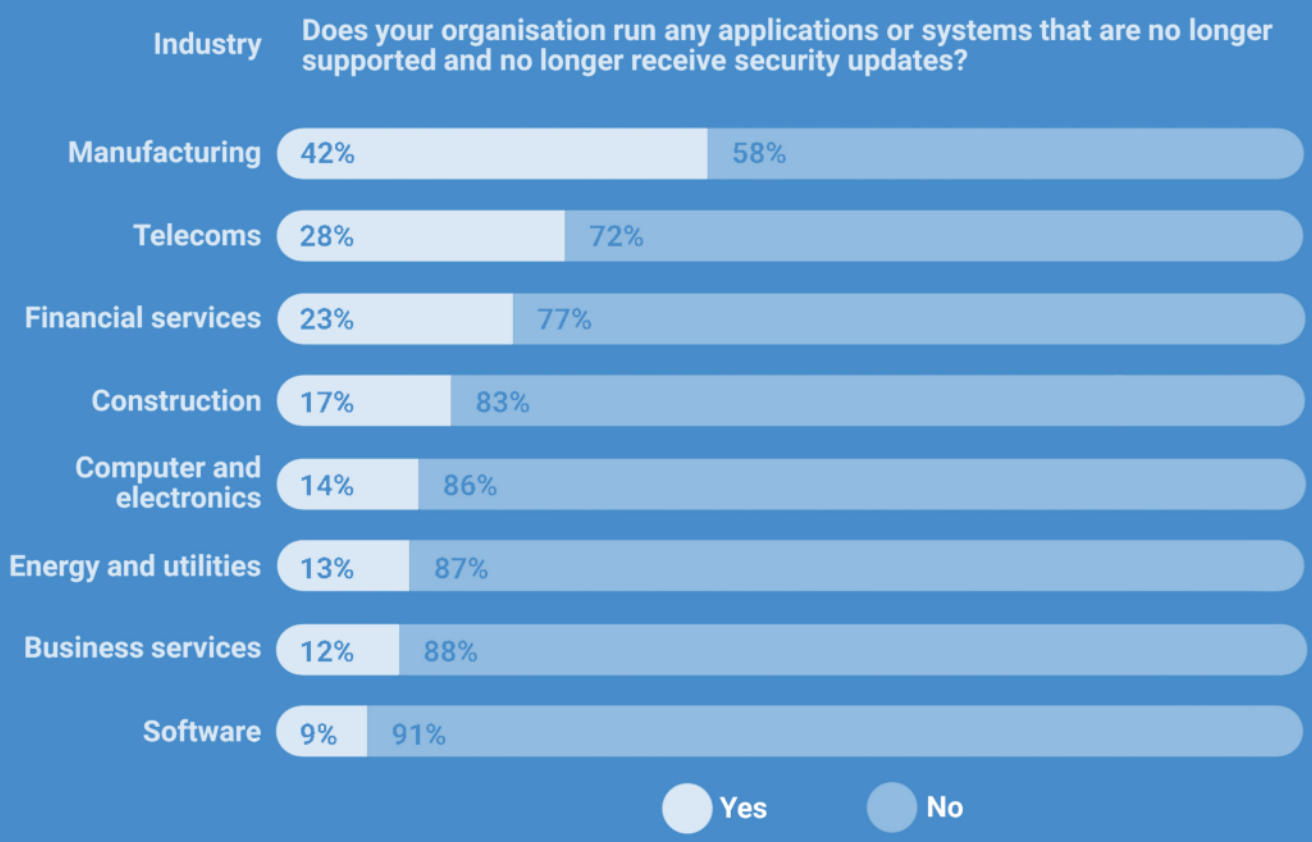
A spotlight on security updates

A key part of any company's cybersecurity posture is ensuring that its applications and systems are up-to-date. All software providers release security patches and updates for their programmes, to protect users as new threats emerge - but not forever.



Eventually, software falls out of support and is no longer updated - meaning that the longer an unsupported application is used, the greater risk it presents to your cybersecurity.

Part of the security profile suppliers set up on Risk Ledger asks: "Does your organisation run any applications or systems that are no longer supported and no longer receive security updates?" We've compared all industries to show where suppliers are the most likely to be using software that no longer receives security updates - revealing that unsupported systems are most likely to be used by manufacturing, telecoms, and financial services industries.



In all of these industries, it's possible that the reason they are using out-of-date software is that the software in question is too integral to their business to update - the risk to their business of the update is greater than the risk of a breach. Or, if not a business-critical system, there might be a process-critical system where updating the software would risk breaking the process, and the process in question isn't deemed enough of a risk to spend the time ensuring the update is done - perhaps it's an isolated system, not connected to any others.

Bearing in mind what we've said before about working in a state of assumed compromise, it's a risk to assume that any system, no matter how sandboxed it is, isn't a target for an attacker. If your supplier is using unsupported software, we'd advise asking them exactly which systems are not supported, whether your data would ever pass through those systems, and what steps they take to protect that system from compromise. Then you can make your own judgement call as to whether the risk is acceptable

Third Party Risk Management

No organisation is an island. Your suppliers have suppliers of their own - and just as you want to know your suppliers are secure, your suppliers should be taking steps to make sure *their* suppliers are secure, too.

25% of organisations do not have a supplier security policy in place

If you're reading this, you know what a supplier security policy is. It helps a supplier understand what security requirements are expected of them when they work for you helping everyone stay more secure.

Yet a quarter of suppliers in our network don't use them for their own suppliers. Perhaps they believe their suppliers are too small to be a target - but speaking of targets, the infamous Target hack of 2013 was perpetrated through their air conditioning supplier - proof that any supplier, big or small, can be used to gain access to your systems.

Q: Does your organisation have a supplier security policy that outlines the security requirements that your suppliers are expected to meet?

Most organisations do conduct business impact assessments for their suppliers

Q: Does your organisation concudct a business impact assessment for each supplier and give them a corresponding crticality rating?

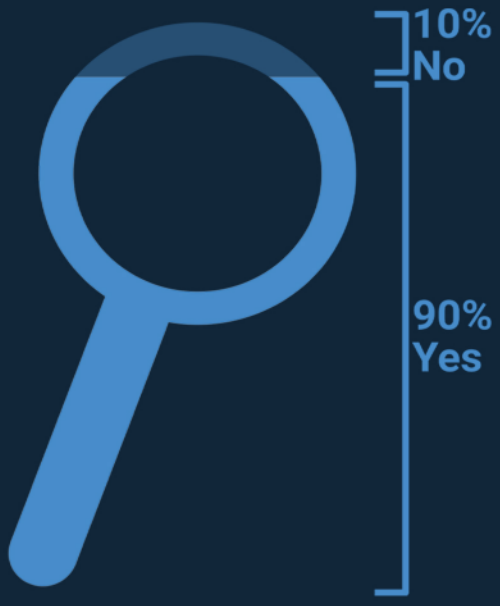
A business impact assessment, as the name suggests, documents the impact to your supplier if something happened to one of their suppliers. That might include a cyberattack or a data breach, or if they simply ceased trading.

A business impact assessment allows your supplier to think through the consequences of those events, and plan a response so that, should the worst happen, they are ready to respond.

It's great to see that the majority of suppliers do conduct this activity, meaning that they will be able to respond to an adverse event such as a cyberattack in their supply chain much faster than those without a business impact assessment.

Cyber Resilience

90% of organisations do have a cyber incident response and forensic capabilities



Q: Does your organisation have a documented incident response plan and forensic capability?

The core goals of cyber incident response are to contain a threat that's been identified, mitigate the damage caused, and take steps to prevent such an attack from happening again. Forensic capabilities help incident response teams to spot where a breach has occurred, how it happened, and what damage has been caused - and, when used collaboratively across organisations, they can protect many organisations against specific attacks by sharing and blocking specific indicators of compromise.

The vast majority of suppliers using Risk Ledger do have these capabilities, either internally, through a third party, or as part of an insurance policy. It means that these organisations are able to reduce the impacts of a breach - including financial and reputational damage, fines, and penalties - by responding to it faster, easily demonstrating compliance with any relevant policies or legislation, and contributing to the global fight against cybercrime.

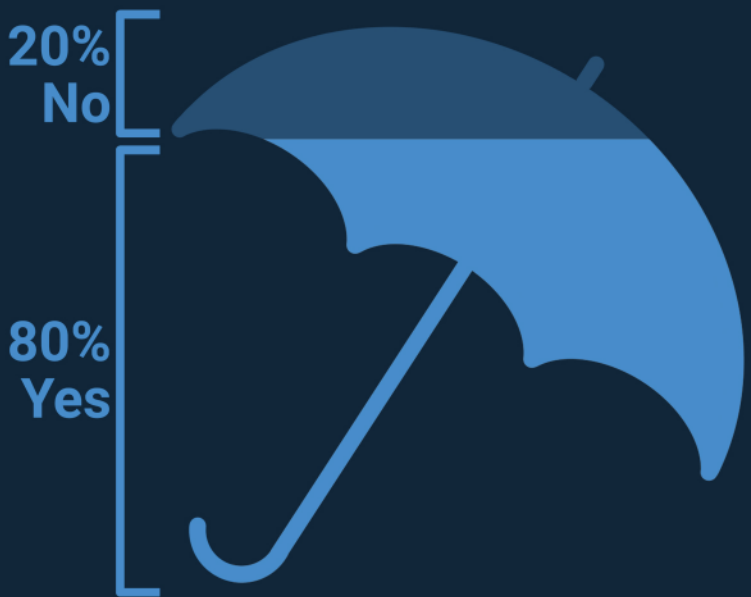
20% of organisations do not have cyber insurance

Cyber insurance cover can include a variety of things, but generally will include the costs of investigating, containing, and repairing the damage from cybercrime.

Cover can either be first party - only covering assets and data belonging to your supplier - or include third party which would include your data, if the supplier held any that was affected by a cyberattack.

One in five suppliers do not have this insurance. For financial organisations like yours, that's a potential sign that they may not have a mature response to cyberattacks - and means that you may be exposed to greater costs if they are the victim of an attack where your data or systems are compromised.

It's worth considering whether you make third-party cyber insurance a requirement for working with you, to ensure you are covered.



Q: Does your organisation have cyber insurance?

Data Protection

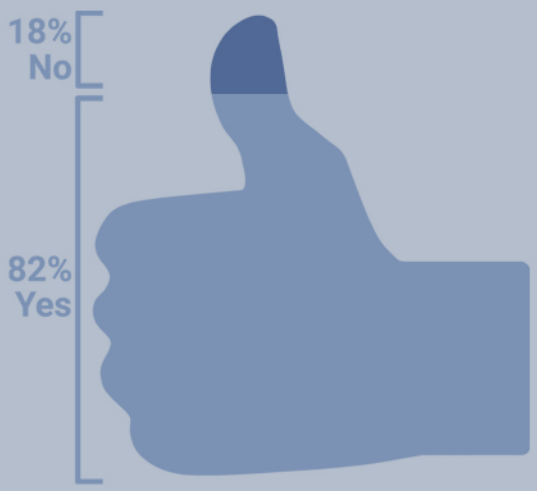
This section contains information that relates to how suppliers handle personal data. As you might expect, many of these questions are closely tied to compliance with various regulations such as the GDPR, the UK-GDPR, the US and Australian Privacy Acts, and so on.

The vast majority of organisations have an up to date data protection policy

A data protection policy details how an organisation handles data, how it protects that data from being stolen, corrupted, or used without an individual's consent, and how anyone who wants to access that data can do so.

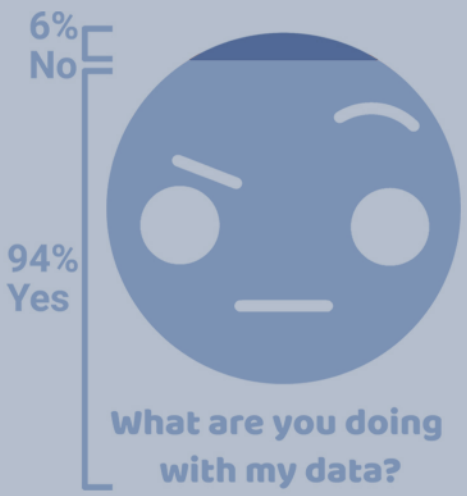
It's good to see that only a very small minority of companies don't have an up-to-date policy. It means that you can be confident your supplier's approach to handling data including your organisation's is watertight.

If one of your suppliers is in that 3%, it means that you can't be sure what they will do with your data. Will they delete any data you give them after a certain period of time? Will they protect it properly while they have it? You won't know - and may not be able to find the right person to ask.



Q: Does your organisation have an up to date data protection poicy?

Most organisations maintain a record of data collection & processing



Q: Does your organisation maintain a record of all personal data collectoin & processing actvities

It's vital that organisations can show exactly what they have been doing with people's personal data – when they gathered it, what they stored, what processing activities it's been part of, and so forth. The information is vital in the event of a breach, to help understand where it occurred and what data may be at risk, or if someone requests access to their personal data or for their data to be deleted.

Essentially, the 6% that answered no to this question have told us they process personal data, but haven't documented the process they follow – and they really should, even if it's not a full-blown audit trail. Without that record, it's impossible for you to understand what data of yours (or your customers') a supplier might be holding and processing, making it hard for you to fulfil your own organisation's commitment to data privacy.

Conclusion

We're passionate that security isn't just about ticking boxes and complying with legislation; it's a vital part of conducting business in the modern world, and something that every organisation should aspire to do well. And, as this report has shown you, most of the suppliers in our network who serve financial organisations share that passion.

However, there are enough exceptions to that rule that you can't always assume your suppliers are doing the right thing. Any area of weakness in your supply chain is a potential route for an attacker to steal your data, access your systems, or derail your business.

There will no doubt be reasons why a supplier isn't implementing various security measures. Some may not believe they are enough of a target to warrant the expense of securing themselves; some may not have realised there were steps they could take to reduce the risks they are exposed to. Some may be victims of tight budgets. You may agree with them. But the truth is that you need to assume that any supplier, large or small, is an attractive target for an attacker looking to get your data. So for every supplier you work with, you need to know whether they are keeping themselves - and therefore you - secure.

Looking to understand the security of your supply chain in real time?

www.riskledger.com
info@riskledger.com