THE STATE OF CYBER SECURITY IN THE SUPPLY CHAIN

Data Insights Report 2023

RISK LEDGER

Message from the CEO

Welcome.

I am delighted to share with you Risk Ledger's new "The State of Cyber Security in the Supply Chain: Data Insights Report 2023".

This report zooms in on the question of how cyber secure the extended supply chain ecosystem currently is, based on data from the 2500+ suppliers with completed security profiles on the Risk Ledger third-party risk management platform, against more than 200 security controls. This data offers ample insights into those areas where the security posture of suppliers is already at a very high level, but also highlights those areas where significant improvements will still have to be made.

This report was not designed to shed light on the security posture of individual suppliers, but rather to provide a bird's-eye perspective of the broader challenges and opportunities that exist in the extended supply chain ecosystem. Given the enormous task of effectively managing risks in the supply chain, and given the escalating need for not just managing risks emanating from direct suppliers, but also from suppliers further down the chain, we strongly believe that only a new paradigm aimed at enhancing collaborative security efforts, something we have termed Defend-As-One®, offers a practical way forward for making us all more secure.

Risk Ledger's new report therefore has two main goals: To provide CISOs and other cyber security professionals with a basic benchmark against which to assess the overall security posture of their own suppliers, and, perhaps even more importantly, to focus our collective security minds on those areas where common weaknesses are most pronounced and thus deserve greatest attention. We believe that addressing these areas of common weaknesses would allow for the perhaps greatest and fastest leap in improving everyone's security in the wider ecosystem.

On that note, I do hope that the data and insights provided in this report are useful to you, and that they will help to generate further discussions on how best to address the growing challenge we all face from escalating cyber security threats in a rapidly digitalising global economy.

We would love to hear your views on this report, on whether it was useful to you, and how it can be improved in the future to achieve its goal of aiding efforts at collaboratively tackling the daunting task of managing cyber threats in our supply chains.

Haydn Brooks, CEO Risk Ledger

Table of Contents

Quick wins for busy CISOs

Throughout this report, we highlight controls which are consistently in place across a large proportion of the suppliers analysed, and those which are less consistently applied. This summary page in the form of "Quick wins for busy CISOs" aims to draw attention to those controls that stood out for their low implementation rate, but which have a high security impact. Hence, checking how well your own suppliers are doing against these controls might offer you a quick and easy way of improving the overall security in your supply chain with a relatively small time investment.

The controls we want to draw your attention to here are important, but have not yet been put in place by a significant proportion of suppliers. If you're looking for areas to focus on to quickly improve the level of security maturity among your suppliers, these twelve controls are a good place to start.

23% do not use Privileged Access Management controls to securely manage the use of privileged accounts.

14% do not regularly audit employee access rights for all IT services

20% do not use a password manager.

17% do not enforce multi-factor authentication on all remotely accessible services.

29% do not conduct threat modelling during the design phase of an application or system build.

11% do not conduct appropriate security testing as part of their development lifecycle.

40% do not conduct regular penetration tests (or red teams) of internal systems.

23% do not have formal agreements in place with their suppliers that have appropriate security clauses, including a right to audit and mandatory adherence to security policies.

51% do not have a 24/7 security or reception team at all of their physical premises.

43% do not require visitors to undergo an ID check on arrival at all premises.

19% do not have a formal policy for remote working that includes security.

25% do not conduct an annual independent information security review and act upon the findings.

Methodology

The data presented within this report is based on an anonymised aggregation of information provided by suppliers using the Risk Ledger platform to showcase their security controls to their clients and customers. When a supplier joins Risk Ledger, they complete a security profile consisting of 211 control questions spread across twelve risk and security domains:

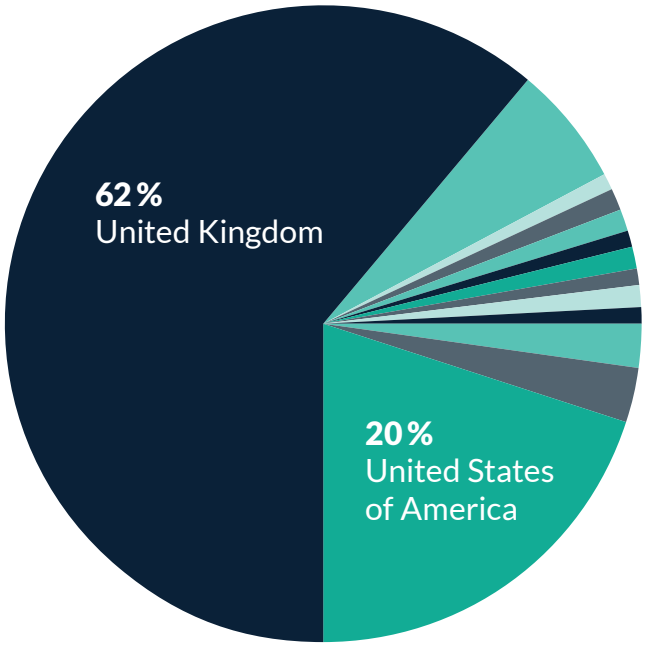
- IT Operations
- Software Development
- Network and Cloud Security
- Supply Chain Management
- HR Security
- Physical Security
- Data Protection
- Security Governance
- Security Certifications
- Business Resilience
- Financial Risk
- Environmental Social and Governance (ESG).

The full Risk Ledger framework, with the exact questions and guidance provided to suppliers, can be found at **https://riskledger.com/resources/framework.**

This report focuses only on the cyber security aspects. We will look to publish future reports that will also cover Business Resilience, Data Protection, Financial Risk and ESG.

There were 2525 suppliers included within this analysis, with geographical representation as follows (among the 6% 'Other', there are an additional 47 countries represented):

Geographical spread of suppliers analysed



6% Other

1% Switzerland
1% India
1% Netherlands
1% France
1% Israel
1% Sweden
1% Ireland
1% Germany

2% Canada

3% Australia

Methodology

Not every supplier has answered every control question. When a supplier completes their profile on Risk Ledger, the framework dynamically adjusts the questions being asked depending on foregoing answers provided, removing questions which are not relevant for them. So, for example, if the supplier does not develop any applications or systems that collect, process, or store data on behalf of clients, they will not have to answer the control questions within the Software Development domain. For each control presented in this report, the data only relates to suppliers for which the control question was relevant.

Not all controls are included in this report. We have highlighted key control areas we felt would be most interesting and beneficial to our readers.

Organisations using Risk Ledger for their supply chain risk management are able to analyse information across all controls and apply their own policies to give contextual risk for their organisation. They can see live assessment data in supplier-owned profiles, do continuous monitoring of the security posture of their suppliers, but from inside out, send and receive updates about controls instantaneously, and they can collaborate more easily on remediation and other tasks with their suppliers directly on our platform.

If you would like to access this data for your suppliers, please get in touch.

Introduction

Supply chain attacks have become the fastest rising cyber threat confronting organisations in recent years. Documented instances of attacks against organisations through their suppliers had already **risen by 300% in 2021,** while increasing by **over 600% in 2022,** and they will likely continue to increase in the years to come. Supply chain attacks are escalating not least as a result of a volatile global geopolitical situation and a rapid growth in attacks on our economies and critical national infrastructure by hostile state actors, and hacker groups they have invited or paid to participate in these attacks.

The growing importance of supply chain security has prompted the UK's National Cyber Security Centre, which is part of GCHQ, to issue a guidance, **"How to assess and gain confidence in your supply chain cyber security",** to help organisations better assess the potential risks posed by their suppliers as well as to manage and reduce them where possible. Meanwhile in the US, according to the **Federal News Network,** the Cybersecurity and Infrastructure Security Agency (CISA) is setting up a new cyber supply chain risk management (C-SCRM) office to help companies, government agencies and other organisations stay on top of recent guidance and policies and implement them. The increasingly hostile global threat environment also prompted the EU to enact the second iteration of its Network and Information Security Directive, i.e. **NIS 2,** in order to "strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU."

Risk Ledger was founded with the aim to do our part to protect global supply chains, and measurably reduce the number and impact of supply chain cyber attacks in the future by building the world's first network of connected organisations, working together to improve the security of suppliers and their clients collaboratively, through a new paradigm we have termed Defend-As-One®. Unlike past efforts at supply chain risk management, commonly little more than paper exercises which have provided, at best, moment-in-time snapshots of suppliers' security postures, the Risk Ledger platform provides suppliers and clients with a continuous monitoring capability into suppliers' security controls.

This grants Risk Ledger unprecedented insights into the overall state of supply chain cyber security among the now over 2500 suppliers on our platform. This not only allows us to provide meaningful data for benchmarking supply chain risks, but also to identify the most common weaknesses and areas for improvement that organisations can check their suppliers against and ask them to focus on. Focusing on these areas, we believe, would make a material difference in improving not just their own security and that of their suppliers, but of the entire supply chain ecosystem.

This is what our first report on The State of Cyber Security in the Supply Chain will offer. We have set out to provide a useful and industry-spanning overview of the state of supply chain security in general, but which in the future will be complemented by similar insights for specific industries with often very different and specific supply chain realities and challenges.

In addition to providing you with an overview of the state of supply chain cyber security, more specifically this report will give you:

- A benchmark of security controls across six specific domains to use against your own suppliers.
- A list of twelve common weaknesses in the security postures of suppliers, providing CISOs and other security professionals with a list of controls to focus on when re-evaluating their own suppliers' security posture to achieve quick but meaningful wins.
- A set of practical recommendations for how to gain real cyber security benefits through your supplier engagement, moving away from the common tick-box third party risk management approach.

1 IT Operations

There are many activities and controls that fall under this category - but for our purposes, IT operations refers to how an organisation manages and maintains the security controls related to its IT systems and processes. With that in mind, the importance of security in IT operations cannot be understated and the work involved in getting this right should not be underestimated, particularly in larger organisations. Not only must technical dependencies & the knock-on impacts of any changes be thoroughly considered, but it is often equally complex to align all stakeholders and effectively balance priorities. It is common within the world of IT operations to be working towards tight delivery timescales, with stretched or overworked resources trying to ensure functionality and performance are always up to scratch to meet business requirements. Sometimes, this comes at the cost of a growing backlog of security changes.

What's going well?

Inventories, patching, and backups

Based on our data, 95% of organisations keep an up-to-date inventory of all their IT assets with assigned owners, and 86% keep the same records with regard to their data repositories. Most IT or security managers (at least within larger organisations) will know that asset management can feel like a continuous uphill battle, with systems/devices being added or changed on a daily basis. However, it continues to be a necessary area of focus since the attack vector of shadow IT systems remains a serious problem. Albeit difficult to reach perfection when it comes to effective and complete IT asset management, the closer a supplier can get to that, the more they minimise their unmanaged attack surface.

of suppliers keep an up-to-date inventory of all IT assets with assigned owners

of suppliers keep an up-to-date inventory of all data repositories

Our data also shows that most organisations are patching their systems regularly (96%) - an absolute must - and are taking backups of production data in line with best-practice guidelines (95%). Given the prevalence of ransomware attacks, the fact that backups are being done regularly and securely is an encouraging sign.

We know that these activities are incredibly challenging for organisations. With acquisitions, employee turnover, and the constant cycle of new projects, it can feel impossible for IT to keep track of what's changing, keep an up-to-date inventory and keep up with maintenance. So it's good news that so many organisations are taking these efforts seriously. We salute you!

The importance of knowing what you have

The 2015 TalkTalk breach was still making headlines years later, and at the time of the breach incurred the largest fine ever handed out by the ICO.

The breach took place via three Tiscali web pages, which TalkTalk had become operators of after their 2009 acquisition of Tiscali. A patch had been made available three years prior that would have remediated the vulnerability exploited in the attack - but those inherited sites had not made it onto TalkTalk's patching list.

The fact that TalkTalk should have known about the pages, but did not, was a deciding factor in the ICO handing out a fine of £400,000. The lessons for other organisations are clear: If you don't know it's there, you can't protect it, so an up-to-date inventory of all your IT assets and data repositories is vital.

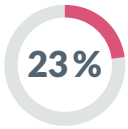
1 IT Operations

What needs attention?

Privileged access management, device wiping, and data loss prevention

Our research shows that more than one in five suppliers (23%) do not use privileged access management (PAM) controls in their organisations. You are likely well aware of the value that proper PAM controls add to your security efforts, given that vulnerabilities like those exploited in **the OS Zoom installer hack** continue to be discovered and reported. This, combined with the fact that a surprisingly high proportion of organisations (14%) do not regularly audit employee access rights, means that the risk of zombie or legacy accounts being exploited and used for privilege escalation remains high.
We also discovered that nearly a third of organisations (30%) are unable to remotely wipe laptop devices (the figure rises to 40% for mobile phones and tablets). This means that they have no way of removing (or rendering unusable) information on devices that are lost or stolen. A notable example is the incident impacting the **Hong Kong government,** which in 2017 lost two computers containing the personal data of every registered voter in the city.

On top of this, 36% of organisations do nothing to prevent unauthorised transfers of data outside of the organisation. Although data loss prevention (DLP) controls that would provide this capability do not offer absolute protection, they can be effective in preventing accidental data transfers, if configured correctly.



of suppliers do not use privileged access management controls to securely manage the use of privileged accounts for system administration

Some of these statistics may seem worrying and are indicative of the challenges involved in deploying and maintaining effective security controls as part of already highly complex day-to-day IT operations. It is important to note that an organisation's lack of any particular control does not necessarily mean they don't have robust overall security defences. By deploying techniques such as defence-in-depth and prioritising controls using likely attack paths, an organisation can make life very difficult for an attacker, even without controls such as remote device wiping or DLP. Good access management, however, is non-negotiable.

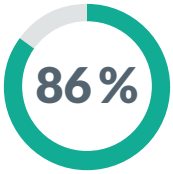
ACTION PLAN

1. Review third party access to your own systems. If necessary, use a 'disable by default' method for this, i.e. if you can't validate what an account is used for within a certain time-frame, disable it. Of course, this method should only be used if you deem the risk posed by unused or unmanaged accounts greater than the operational risk of disabling access. It requires careful consideration and communication across the organisation, but it will ensure the accounts you have remaining are necessary and can be managed effectively.
2. Ask your suppliers what methods they use to ensure they stay on top of asset management as and when things change across their organisation. This will give you an idea of how well thought-out these processes are and give you some confidence over how likely it is that they miss something important. You may also learn some tips and tricks to use yourself! It's important to remember that suppliers are organisations just like yours, with security teams battling the same challenges—collaboration on these tricky topics is therefore vital.
3. Consider third party touch-points across all of your operational processes and the assets involved to ensure supplier risks are accounted for and responsibilities are clear. For example, do you have an on-premise system accounted for in your asset inventory that is managed by a supplier? Who is responsible for patching that system?

1 IT Operations

What works?

keep an up-to-date inventory of all IT assets with assigned owners

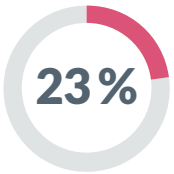


keep an up-to-date inventory of all data repositories with assigned owners

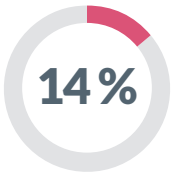
ensure that all IT systems are regularly patched

take regular backups of their digital production data in line with current best practise guidelines

What needs attention?

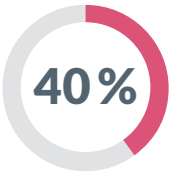


do not use Privileged Access Management controls to securely manage the use of privileged accounts

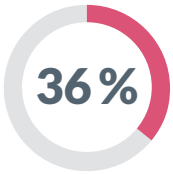


do not regularly audit employee access rights for all IT services

cannot remotely wipe company data on laptop devices



cannot remotely wipe company data on mobile phones and tablets



do not prevent unauthorised transfer of data via email, web browsers, or other data transfer mechanisms

A pain in the password?

Who doesn't love a password debate? Depending on who you ask, they are a useful-but-poorly-used security measure, or an outmoded security measure that should be replaced as soon as humanly possible. But, while alternatives to passwords remain relatively expensive to implement, and are not without their own limitations, the password remains a fixture of the security landscape.

Our data shows that 90% of organisations are technically enforcing a password policy, ensuring uniqueness and appropriate length or complexity (note - it is no longer recommended to enforce regular password changes - see guidance from the NCSC). We can also see that 80% of organisations use a password manager, recognising that users almost universally struggle with password fatigue, causing them to reuse passwords across systems and to create weak passwords. Those 20% of organisations that are not using password managers could be forcing users to resort to sequential, repeated or simple, easy-to-remember passwords, or to keep a record of them insecurely, e.g. in a file on their desktop or even a file shared with colleagues. It is important not to blame employees for insecure password practises if they are not provided with a practical alternative—for the most part, people are just trying to do their jobs.

of organisations use a password manager

A spotlight on multi-factor authentication

Multi-factor authentication (MFA) is one of the most impactful controls any organisation can put in place to improve security. Microsoft has asserted that using MFA can reduce the chances of an account being compromised by 99.9%. Whilst it's simple to implement, it increases friction for the user and is therefore often provided as an optional setting which needs to be intentionally configured. This sometimes leaves MFA disabled and the accounts vulnerable to unauthorised access through credential stuffing or brute-force attacks. Our research has discovered that 83% of suppliers enforce multi-factor authentication on all remotely accessible services; 17% do not. When it comes to remotely accessing internal company networks or cloud environments, 12% are still not using multi-factor authentication for these connections.

Ideally, your suppliers (and you) will enable MFA on any systems that are accessible from the public internet - and on all web-based third-party services that your employees use, such as Microsoft 365 or GitHub. Although MFA using a text message (SMS) is better than none at all, alternatives with higher integrity are recommended, such as an authenticator app, push notification or other software or hardware tokens. Alternatively, why not start exploring fully passwordless authentication options?

of suppliers use MFA to secure all remotely accessible services

of organisations use MFA to secure remote access to its network or cloud environment

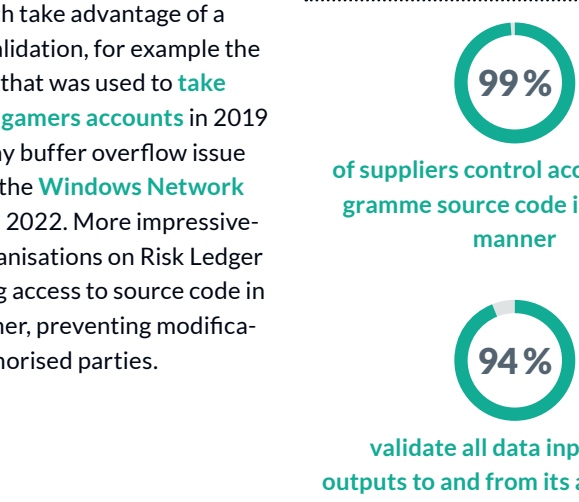
2 Software Development

Not all of your suppliers will develop software, but for those that do, ensuring they have robust development practices will go a long way to assuring you of the security of the applications they provide or use to process your data. Regular penetration testing of the software used is an important step in gaining security assurance, however, pentesting will not identify all vulnerabilities in your software and should not be relied upon as the primary method for securing the software. It is important to prevent those vulnerabilities from making it to production in the first place; providing sufficient guardrails for developers, shifting left with testing, and embedding security hygiene throughout the software development lifecycle (SDLC) offer the best chance of preventing significant vulnerabilities.

What's going well?

Data validation and securing access to source code

Our data shows that a vast majority of organisations (94%) validate all data inputs and outputs for the software they develop. There are many attack methods which take advantage of a lack of data validation, for example the SQL injection that was used to take over Fortnite gamers accounts in 2019 or the zero-day buffer overflow issue discovered in the Windows Network File System in 2022. More impressively, 99% of organisations on Risk Ledger are controlling access to source code in a secure manner, preventing modification by unauthorised parties.



of suppliers control access to programme source code in a secure manner

validate all data inputs and outputs to and from its applications

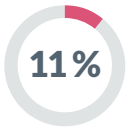
2 Software Development

What needs attention?

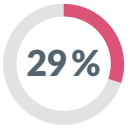
Threat modelling and security testing

Threat modelling involves taking a holistic view of the application in question in order to find weaknesses that could be exploited and other ways in which it could potentially be misused by a threat actor. This is something that 29% of organisations do not do during the design phase of an application or system build. For those organisations, the overall architecture of the systems they develop may not be designed in the most effective way to prevent likely attacks. This may make it harder for development teams to avoid vulnerabilities further down the lifecycle.

Once code begins to be produced, frequent testing aims to identify potential issues. With the movement towards DevSecOps encouraging earlier and more continuous security testing, vulnerabilities are being caught sooner; this also makes it easier (and cheaper!) to resolve them. However, according to our data, a significant minority of organisations (11%) still do not conduct security testing of all applications and systems during the build process.



of suppliers are not conducting appropriate security testing in the development lifecycle



do not conduct threat modelling during the design phase of an application or system build

ACTION PLAN

1. For those suppliers where secure development practices are particularly important for you (e.g. they provide a bespoke, critical system), ask them to describe how their software development practices have changed over time. This will give you a good indication of whether they are taking security within the development process seriously and putting the time and effort into continual improvement, particularly as guidance such as the OWASP Top 10 evolves.

2. If you are using software provided by a third party, pay particular attention to

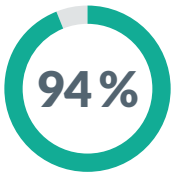
   a. bespoke integrations, ensuring any middleware is covered by security controls clearly managed by either you or the supplier;

   b. application interfaces (APIs) that may be offered for you and other organisations to integrate data exchange between the supplier's services and your existing systems; these are often overlooked in application security testing and can be vulnerable to misuse.

3. Consider conducting your own threat modelling of your most critical applications. Even if the supplier has done this initially, it may be that your particular environment or configuration changes the likely attack vectors, making additional mitigating controls necessary.

2 Software Development

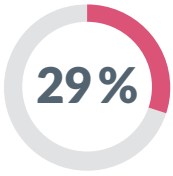
What works?



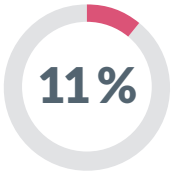
validate all data inputs and outputs to and from its applications

control access to program source code in a secure manner

What needs attention?



do not conduct threat modelling during the design phase of an application or system build



do not conduct appropriate security testing as part of their development lifecycle

3 Network and Cloud Security

Whether your suppliers are managing their own server racks, or whether they are more concerned with containers and services running in the cloud, they will need to secure their environment. This is not just about keeping attackers out of your internal environments, but about ensuring you can minimise the damage and respond quickly when compromised. Good network and cloud security should give you defence-in-depth--so that you are increasing the cost to an attacker during each phase of the attack, not just at the initial stages.

What's going well?

Perimeter controls, segmentation & monitoring

Our data was generally very positive when it comes to network and cloud security measures. Almost every supplier on Risk Ledger has:

- Firewalls protecting all ingress and egress points for traffic in their network and cloud environments (98%);
- Implemented those firewalls using a "deny all" policy and only building 'allow' rules based on their organisation's specific requirements (94%);
- Appropriate segmentation within its network or cloud environments to restrict the level of access to sensitive information, hosts, and services (91%);
- Defined processes in place to ensure that all security alerts from logging and monitoring solutions are reviewed and actioned as necessary (92%).

These controls combined provide reasonable assurance that the suppliers in question have good preventative measures in place to stop an attacker from entering their environment undetected. They also ensure that, if the attacker does successfully penetrate perimeter controls, they cannot easily traverse through the network from a DMZ to a high security segment housing their most critical applications. Network or cloud security controls in any functioning business cannot give guaranteed protection - after all, there need to be accessible communication channels to allow for the legitimate connections necessary to operate the business.

This is why detection and response controls are equally important, so that when, inevitably, something unexpected happens within your environment, you have the people, processes and technology in place to quickly identify whether it is an indication of malicious activity, and if so, to then respond effectively. However, simply having good detection technology is not enough. It is common for security teams to be overwhelmed by large volumes of security alerts, making it difficult to differentiate between early indicators of an attack and noise, so it's important to put time and effort into making sure your detective tools are working for you, not against you.

protect all ingress and egress points for traffic through their network or cloud environment using firewalls

3 Network and Cloud Security

What needs attention?

Penetration testing

Whilst 80% of organisations are conducting regular penetrating tests of their public facing infrastructure, only 60% are doing the same for their internal systems - an exercise that assumes a compromise of perimeter controls. There are very good reasons why testing externally facing systems is given a higher priority than testing internal infrastructure. However, given that it is widely accepted that becoming the victim of a cyber attack is a case of 'when', not 'if', it is important to also gain assurance over how well you are able to defend against an attacker that is already inside your environment. With regard to the 40% of suppliers who are not yet conducting such tests, it's a potential sign that they're not applying the concept of defence-in-depth. Defence-in-depth - and the related concept of assumed compromise - are much more effective at disrupting ongoing attacks and at mitigating the amount of damage an attacker can do once inside an environment.

of suppliers do not conduct regular penetration tests of internal systems

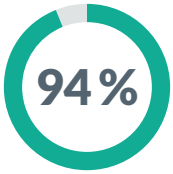
ACTION PLAN

1. When reviewing pentest reports from your suppliers, pay particular attention to the scope of testing. This will reveal the level of assurance the report provides you with.
2. Bear in mind that security testing, particularly more in-depth assumed compromise or red-teaming exercises can be very expensive, and it may be more appropriate (depending on the size and nature of the supplier) to focus their limited resources on specific control improvements. A lack of penetration testing doesn't necessarily mean the supplier poses a high risk to you - you may just have to work a little harder to gain the assurance you need.
3. Consider the interfaces between your networks / cloud environments and those of your suppliers. How trusted are those connections? Are you and the supplier using similar zoning principles for the onward connections? Could the supplier provide a weak point of access into your environment through that trusted connection?

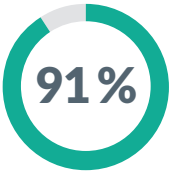
3 Network and Cloud Security

What works?

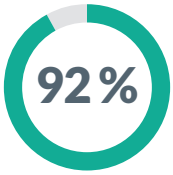
protect all ingress and egress points for traffic through their network or cloud environment using firewalls



have implemented firewalls using a deny all policy, with rules built around their organisation's requirements

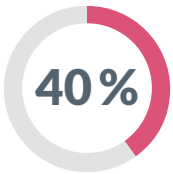


have implemented segmentation or segregation in their networks and/or cloud environments



have defined processes in place to ensure that all security alerts from logging and monitoring solutions are reviewed and actioned as necessary

What needs attention?



do not conduct regular penetration tests (or red teams) of their internal systems

4 Supply Chain Management

At Risk Ledger we are all about helping you manage your supply chain security, and we mean your whole supply chain. We are not just talking about third-party risk management, but about viewing your suppliers as an extension of your own organisation, and thus also considering their third parties and the wider ecosystem as a whole. Widely used systems and services that are known to be deeply integrated into business operations across many sectors have been historic targets of supply chain attacks (examples are products by Microsoft, Fortigate, Magento and many others). However, there are indications of a strategic shift to other contributors to critical services in the supply chain (examples include Twilio, Okta, Kaseya and others) and tactical targeting of smaller companies with less mature security operations to gain access to larger organisations. So, although it might feel complex to have to think about your supplier's suppliers, it's not an area of cyber security to be ignored.

What's going well?

Formal agreements controlling personal data

The majority of organisations on Risk Ledger (86%) ensure that all the third parties they work with which have access to personal data have a formal agreement in place that covers all the requirements of relevant data protection regulations. Those agreements will typically include:

- Responsibilities of each party relating to the services to be delivered, instructions for data processing and requirements for security;
- Definitions making it clear who is the data processor and who the data controller;
- Clauses covering the use of sub-contractors or international data transfer, as well as any other specific legal clauses required by local data protection legislation.

This then provides a legally binding standard that both your suppliers, and the extended supply chain, must follow when dealing with your personal data. It's important to remember that under most data protection legislation, the data controller remains accountable for the data, regardless of who is doing the day-to-day processing of the data. So, whilst formal agreements are vital to give you the right of recourse if your data were stolen or misused as a result of a breach further down the supply chain, they are no replacement for thorough due diligence and ongoing governance.

of suppliers have formal agreements in place to control third party use of personal data

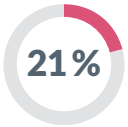
4 Supply Chain Management

What needs attention?

More formal agreements, and greater attention on supplier security

23% of suppliers do not have formal agreements in place with their third parties containing appropriate security clauses, including a right to audit and mandatory adherence to security policies. This means that, while they may have agreements pertaining to how data will be handled or the service provided, there are no contractual commitments around security—which would make the organisation more vulnerable in a breach.

Similarly, a third of suppliers (32%) do not have their own supplier security policy, meaning they have not set out any expectations as to the minimum level of security controls their suppliers should have in place. That leaves room for ambiguity—a supplier might deem their protection sufficient, when in fact it is woefully inadequate for the service they are providing you or with a view to your own risk profile; and therefore puts you at significant risk. This is particularly likely to be the case for the 21% of suppliers that do not conduct security due diligence on their own suppliers.



of suppliers do not conduct security due diligence against their suppliers before entering into a contract

At the same time, over a third of suppliers (36%) on Risk Ledger do not conduct business impact assessments on their own suppliers in order to understand the true impact to their business in case one of these suppliers was to suffer a disruption or security breach. Without a business impact assessment, assigning meaningful criticality ratings and risk prioritisation is difficult.

Business Impact Assessments - why bother?

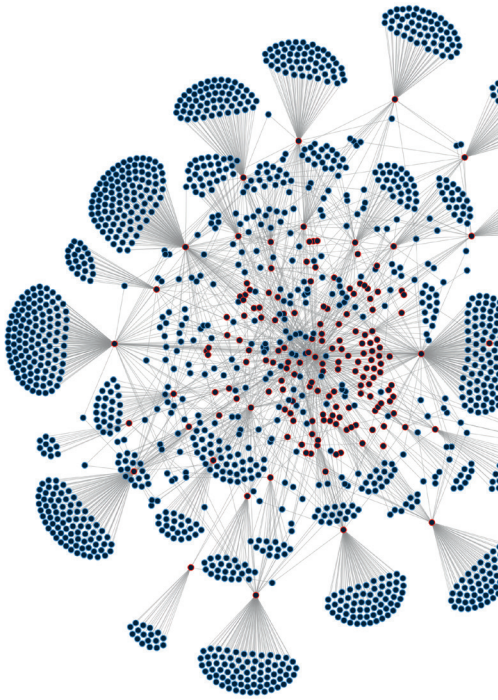
Some of your suppliers would have a larger impact on your organisation than others if they were to suffer a security incident. Some will not have access to any of your systems, some may never touch your data. A business impact assessment (BIA) helps you understand what would happen if a particular product or service was no longer available, or if the integrity or confidentiality of your data had been compromised as a result of an incident involving a supplier. Gaining an accurate understanding of business criticality allows you to:

- Specify the level of control expected from each supplier, ensuring you have adequate protection but are not reducing your pool of supplier options. This is especially important if you're using specialist, innovative or niche services/solutions which are likely to only be provided by a few suppliers—often smaller, newer organisations who may not have the resources to maintain enterprise-level security maturity.
- Focus your efforts on the suppliers who matter the most; you only have limited time and resources and it's likely you will not be able to review or support every single supplier you use. This will provide you with an effective method of prioritisation.
- Plan your response and recovery if an incident was to occur with a specific supplier. Understanding the impact of an incident in advance enables you to plan and rehearse specific scenarios, containing the incident, mitigating the damage done and enabling the continuation of business operations.

4 Supply Chain Management

We also found that 33% of organisations do not conduct regular assurance activities with their suppliers. That means that they are not regularly assessing whether their own suppliers are still providing an adequate level of security. It also means that these organisations, while knowing that their suppliers were secure when they were onboarded (inviting complacency), can no longer confirm whether they are secure now (which, of course, they may not be). It's important to find a way to maintain up-to-date information about the security of your supply chain, preferably without repetitive annual reviews.

So, does all this mean that your suppliers are likely to suffer attacks through their own supply chains? Not necessarily. None of these findings mean that the extended supply chain is vulnerable—just that a significant proportion of suppliers are not holding their own supply chain to account and thus ensuring that their supply chain is secure. Everything might be shipshape—but it might not be, and a relatively large number of suppliers don't know which is the case.



ACTION PLAN

1. Make sure you have included assessing supply chain management within your own supplier security programme. When focusing on third parties, it is easy to forget that there is a whole network of other organisations supporting that third party in providing the service to you. That one third party is your gateway to understanding the wider supply chain and the risk and opportunities involved, so you want to make sure your supplier is taking the security of its own supply chain seriously.
2. For your most critical suppliers, it may be appropriate to ask them to reveal the names and relationships of their most critical suppliers, so that you can assess the dependencies further down the supply chain and any concentration risks that may exist. The right technology pays dividends here. Using a tool which automatically maps connections will provide insights that simply wouldn't be possible manually.
3. When approaching your suppliers about their own supply chain security, try the carrot before the stick. Acknowledge that supplier security can often be further down the priority list than other security issues and perhaps offer some practical guidance on how they can start small.

Practical advice for tackling supply chain security

Don't let the enormity of the task overwhelm you. Break it down into two distinct projects:

Project 1: New suppliers in the future:
What is the process going to be for onboarding a new supplier? What do you need to put in place now so that, over time, your situation gets better not worse?

> Using the onboarding of each supplier as an opportunity to build a meaningful connection with the security teams within that supplier organisation will put you in a situation where you have more ready access to immediate risk mitigation support when you need it, as well as in a situation where an incident occurs.

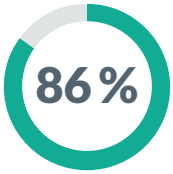
Project 2: Backlog of existing suppliers:
what suppliers do you currently use and what risk do they pose?

> This can be chipped away at over time - you may have hundreds (sometimes thousands) of existing suppliers, so it's important not to let the perceived scale of this challenge prevent you from doing project one and starting to make improvements for the future.

The solution to those two problems might be quite different, but solving the first one well means you will be gradually improving your situation over time, regardless of what happens with the second project.

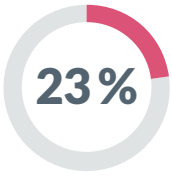
4 Supply Chain Management

What works?

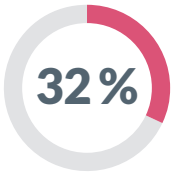


have formal agreements in place with suppliers to control third party use of personal data

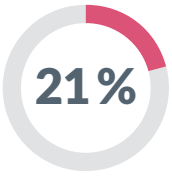
What needs attention?



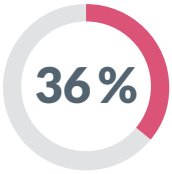
do not have formal agreements in place with suppliers that have appropriate security clauses, including a right to audit and mandatory adherence to security policies



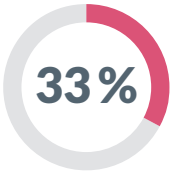
do not have a supplier security policy that outlines the security requirements that their suppliers are expected to meet



do not conduct security due diligence against suppliers before entering into a contract



do not conduct a business impact assessment for each of their suppliers and give them a corresponding criticality rating



do not conduct regular assurance activities against their suppliers to ensure they are meeting their information security requirements

5 People & Physical Security

Cyber security isn't just about securing the digital space; it must also consider how to secure the means and methods cyber criminals will exploit to gain access to this digital space - the people operating within it and the physical spaces used by those people or to house your hardware. Physical breaches have admittedly become fairly rare - but that doesn't mean they do not happen. **An article for Dark Reading from November 2022** showed how an attacker with an NFC-enabled phone and an NFC tag could hack their way past an access control system used by the White House and the Houses of Parliament to gain physical access to those locations. This article demonstrated but one of many ways in which threat actors could breach the physical security of your premises, which remains a real concern especially for organisations operating critical national infrastructure. So while personnel security is high on the agenda of most organisations, physical security often only comes into sharp focus when running operational technology such as Industrial Control Systems (ICS), or running other high security premises, such as government buildings.

What's going well?

People are being vetted and educated about cyber security

Our data indicates that the vast majority (89%) of suppliers are performing background checks on both employees and contractors. Though a background check only offers a snapshot of a person, at least if not conducted periodically to provide a better profile of a person over time, at the very least it is a good way to check for any initial red flags (criminal record, discrepancies in address or employment history, credit ratings etc.) before a new employee or contractor walks through the door.

Nearly every organisation (90%) also provides a training programme for its employees in data protection and information security. There is a human element involved in 82% of data breaches, according to research by Verizon, with incidents ranging from losing laptops, attaching the wrong files to an email, to falling victim to phishing attacks. Effective training goes a long way to helping reduce these incidents. It is important that employees are empowered and supported to act in a secure and responsible way with appropriate fail-safe defaults and just-in-time nudges complementing an educational training programme.

receive an information security and data protection training programme

5 People & Physical Security

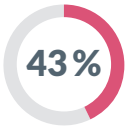
What needs attention?

Physical security

Many suppliers appear not to pay the same attention to their physical security than to other elements of their security posture. There are some measures that might be considered overkill for some organisations, such as staffing their premises with security or reception teams 24/7, which over half (51%) the suppliers analysed do not do.

There are other measures though that could be considered as basic best practices, which a significant minority of suppliers are also not embracing. These include not using an access control system (18%) or CCTV to monitor entry and exit points (22%), and not requiring visitors to undergo an ID check on arrival (43%).

If your supplier is not taking these measures, this means that it will be easier for someone to gain unauthorised access to their building. The suppliers included in these statistics are those who rely on office space, warehouses, data centres or any other type of physical premises. The risks involved in having insufficient safeguards for physical security in place, of course, very much depends on the type of premises in question and what they are used for. Ultimately, the risk this lack of physical security control poses to you (as the client or customer) is something you will need to evaluate. When doing so, also consider other security measures your supplier might have in place that would prevent, or at least make it harder, for an unauthorised person on their premises to access systems and data. However, if the supplier in question supports critical infrastructure or runs facilities that house operational technology or highly-sensitive information, then the risk goes up significantly.



of suppliers do not require visitors to undergo an ID check on arrival

ACTION PLAN

1. Look for the 'why not?' in supplier explanations to whether they have certain physical security controls in place, or not. From there, you can make a judgement as to the level of risk emanating from a possible physical security breach, and what role such a breach could play in a successful attack on that supplier.
2. Set different thresholds for physical security control expectations for different types of suppliers - this could be based on the type of supplier themselves (e.g. manufacturing physical products vs. providing a service), based on the part of your business they support (e.g. internal operations vs. site/resource management), or based on the data or systems they have access to.
3. Ask to see details of your suppliers' cyber security employee awareness and training programmes. It is very easy to quickly spot the difference between once-a-year compliance-driven training and thoughtful, embedded training / support programmes that empower employees to act securely and responsibly in their day-to-day work.

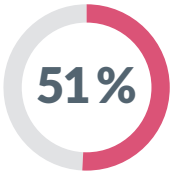
5 People & Physical Security

What works?

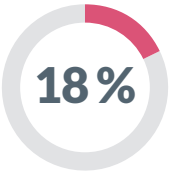
perform background checks on staff and contractors

receive an information security and data protection training programme

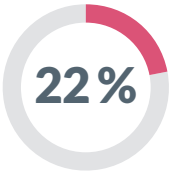
What needs attention?



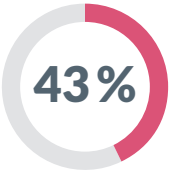
do not have a 24/7 security or reception team at all of their physical premises



do not use an access control system on their premises' entry and exit points that includes logging of access



do not use CCTV to monitor entry and exit points of all premises



do not require visitors to undergo an ID check on arrival at all premises

6 Security Governance

Sound security governance directs the efforts of security teams in maintaining consistent and effective security controls. A lack of proper governance doesn't necessarily mean that an organisation's security is weak per se. But it does mean that strengths in that organisation's posture are more likely to be found in specific teams or departments rather than across the whole organisation, leaving them with weak spots.

What's going well?

Policies are in place and infosec is embedded in project delivery

Most (92%) of the suppliers on Risk Ledger have a documented cyber security or information security policy that has been reviewed in the last year.

This is an indication that cyber security is being taken seriously - although, there is of course a world of difference between having a policy and having an effective policy in place.

It is also encouraging to see that the vast majority (90%) of organisations include information security in the planning and delivery of projects. Most organisations ensure that when a project is initiated, risks, including new risks the project might expose the organisation to, are assessed, and that steps are taken to mitigate them. Given that project work often makes up the bulk of an organisation's activity, the fact that cyber security is being taken seriously even at individual project level suggests a heightened security awareness among teams and organisations at large.

of suppliers include information security in the planning and delivery of projects

have a documented Cybersecurity Policy or Information Security Policy

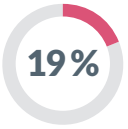
6 Security Governance

What needs attention?

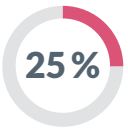
Remote working and independent reviews of security

On the downside, 19% of organisations do not have a formal policy for remote working that includes security considerations. This does not mean that no steps are taken to ensure remote working happens securely, but it does mean that many organisations don't take a cohesive and documented approach to the issue. Recent news from **Hornet Security revealed that 74% of remote staff have access to critical data,** yet nearly a fifth of IT professionals believe that workers are not secure when working remotely. This means that a formal policy on remote working that includes information security should become the norm.

Another area ripe for improvement is how organisations review and improve their security maturity. 25% of organisations on the Risk Ledger platform do not conduct annual independent information security reviews and then act upon those findings. There are two things at play here: First, obtaining an independent review of the effectiveness of your security controls and second, acting upon the findings. Too often, reports on the state of an organisation's security can sit on the shelf brimming with recommendations for improvement that are never enacted. It's important to note that not every recommendation received in a security review is necessarily the right thing to do, but the findings should be considered and acted upon based on a risk-based prioritisation approach, being cognisant of available resources.



of organisations do not have a formal policy for remote working that includes security considerations



of organisations do not conduct annual independent information security reviews

ACTION PLAN

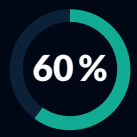
1. Ask your suppliers about remote working and how they're keeping employees and critical data secure. What technical measures are they taking? How are they supporting employees in identifying and mitigating the plethora of risks specific to remote working?

2. Ask to see the most recent report that was prepared on your supplier's security posture (this could be from an external party or an internal audit function). When doing this, it is important to reassure the supplier that you know these reports are designed to highlight areas of weakness and that you are more interested in the progress that has been made in addressing them since the review, rather than the weaknesses themselves. Using this as a basis for conversation will give you a more honest picture of how your supplier manages and improves security, whether they have the capability to operate security controls effectively and ultimately, whether you can trust them with your data or critical operations.

3. Why not also take this opportunity to check your own effectiveness in these areas - are you confident in your remote working practises? Do you make the most of the perspectives and insights provided by independent reviews? Or perhaps, would it be valuable to rethink the purpose behind independent reviews conducted, and consider how they could help you bolster your defences as well as provide assurance and compliance benefits?

The challenge with security certifications

A common method for gaining confidence in a supplier's cyber security posture is to check their certifications. While this can be a useful initial indicator, we caution against placing too much reliance on (or to be too concerned about a lack of) certifications. There are many different security certifications an organisation can choose to obtain, each with their own focus and limitations. Whichever certification you are looking at for your supplier, make sure you fully understand the context, scope, and limitations so that you can make an informed judgement on exactly what the certification is telling you. One of the most common information security certifications recognised somewhat globally is ISO27001.



of suppliers are ISO27001 certified

Obtaining independent advice, assurance, or an outsider's perspective on your security is important, but that does not need to be in the form of a formal certification. If your supplier is not certified, perhaps look more closely at whether they obtain regular independent reviews of their cyber security in other ways. If they do not hold any certifications, and they have not sought independent reviews of their security posture, then there may be more cause for concern.

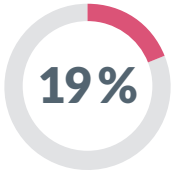
6 Security Governance

What works?

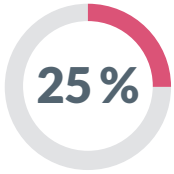
have a documented Cybersecurity Policy or Information Security Policy

include information security during the planning and delivery of projects

What needs attention?



do not have a formal policy for remote working that includes security



do not conduct an annual independent information security review and act upon the findings

So, what now?

The management by clients of risks emanating from individual suppliers, as important and indispensable as it is, falls short of addressing the increased complexity in the wider supply chain ecosystem, especially the further down one goes in the supply chain. Our aim is therefore to make the entire supply chain ecosystem safer for the benefit of all.

In this report, we have hence focussed on trying to reveal some key common security weaknesses across the supply chain as well as to provide guidance for how to better communicate and collaborate with suppliers for mutual benefit, and for the benefit of the ecosystem as a whole.

We all depend on one another to improve the overall security of the ecosystem and we hope that our findings, summarised in the „Quick wins for CISOs“ section of this report, inspire you to compare your own suppliers against these common weaknesses and, if their controls in some of these areas need improvement, to then focus on remediating those first, and if possible collaboratively. We know CISOs time is scarce and valuable, and their jobs are difficult and multi-faceted enough as it is. What we hoped to thus provide you with are areas where quick, yet also high impact, wins are possible. Help us to make the supply chain ecosystem for everyone a bit safer by embracing our vision of ‘Defend-as-One’.

We are keen to further improve the way in which we make data on risks in the supply chain accessible and useful for the benefit of security professionals. If you enjoyed this report as our first attempt at doing so in a methodical way, please do let us know. Equally, if you have any other comments, feedback or suggestions for how to improve our approach and presentation of the data (and which data we present) for similar future exercises like this one, we would be extremely appreciative. Get in touch and let’s make this an iterative exercise for the benefit of everyone working towards making our supply chain ecosystem more secure.

Make the process easier with Risk Ledger

Also, if you would like to get a much more tailored insight into your own supply chain, get in touch with us, too. We would love to hear from you, and demonstrate our platform and its benefits to you in person.

Be confidently on top of your supply chain security

HOW DOES IT WORK?

- Get the right risk assessment data with our Dynamic Controls Framework. It unlocks network effects to scale your supply chain security.
- See live assessment data in supplier-owned profiles (like LinkedIn for cybersecurity).
- Send and receive updates about controls in real time. Our network model means suppliers and clients are always connected.
- Collaborate on remediation and other tasks directly in the platform.
- Visualise concentration risk beyond third parties.
- Do continuous monitoring, but from inside out.

WHY RISK LEDGER?

- Get your risk assessment tasks done in hours, not days.
- Shorten your procurement cycle to weeks, not months.
- Communicate easily with the people you need to.
- Scale your coverage of suppliers from 5% to 95%.
- Spot more vulnerabilities at 10% of the cost of your current programme.

Join us in creating the future of defend-as-one. No organisation is an island. Already, many customers use Risk Ledger as both a client and a supplier.

As a SAAS platform, Risk Ledger can be deployed in minutes. We'd love to show you more.

Contact us today to book a demo.
riskledger.com | info@riskledger.com

You're in good company

Comply with regulations
"Risk Ledger are continually developing their product to help us comply with changing regulations. Being able to identify concentration risk and critical dependencies through Risk Ledger's live mapping functionality means that when new regulation is introduced, we will be well prepared."
-CISO, SCHRODERS PERSONAL WEALTH

Visualise concentration risk in your supply chain
"Using the visualisation tool in Risk Ledger, we discovered that one of our prime suppliers was closely linked with three other suppliers. If one went down, the whole lot went down. After looking at the graphical analysis, we could then reach out to the other firms to investigate and remediate the risk."
-CISO, NHS TEST & TRACE

Respond to supply chain incidents in real time
"Responding to incidents like Log4j would have been a really long tedious process without using Risk Ledger. We felt the benefits of agreeing the questions and sending it off. About 75% of supplier replied straight away. This helped us to very quickly understand how SGN and our supply chain would be impacted by this vulnerability."
-CISO, SCOTTISH GAS NETWORKS

Get an accurate snapshot of your supply chain risk that you can monitor in real time
"We are pleased to partner with the Risk Ledger network and to work proactively with our suppliers to drive down risk. Working with Risk Ledger allows us to get a better snapshot of the overall risk within our supply chain."
-GLOBAL IT DIRECTOR, APAX PARTNERS

Drive up your supplier engagement
"Since our organisation is so large, we don't often respond to specific questionnaire requests, but because Risk Ledger was so comprehensive, it really helped us through the process and makes it easy for us to respond."
-BP OIL UK

Free up resource with supply chain assurance programme
"Using Risk Ledger we were able to increase coverage of our supply chain assurance programme by 500% with the same amount of resource. Even more impressive, we were able to achieve this in a quarter of the time, compared to the tool we were using previously."
-CISO, FIRST SENTIER INVESTORS

6POINT6 Crowe Digital Intelligence BAE SYSTEMS CITY OF LONDON POLICE Civil Aviation Authority Gamma
UK Health Security Agency Pennon SGN SUCCESSION WEALTH telenor yieldbroker

RISK LEDGER