RISK LEDGER

Supply Chain Risks Insight Report

IT Operations

2021

riskledger.com

Thoughts of a supply chain risk expert

Emily Hodges
Cyber Security Consultant
Risk ledger

(Click to connect with Emily on LinkedIn)

Effective management of IT operations is not easy. Ever competing priorities and conflicting demands from different business stakeholders mean that security controls are often not given the priority they should. There has been huge improvement over the last few years as cyber security risk is brought to the forefront of minds by high profile breaches and increased regulation. However, there are still challenges to overcome as this report demonstrates.

A good example of how we still haven't fully solved the conflict between IT, security & the business can be seen in the statistics for change management. 23% of organisations on the Risk Ledger platform do not have formal change management that considers security; this only makes things harder because it means that security issues will need to be fixed at a later date, creating more work and more changes to deploy in future, sometimes as an emergency change which disrupts operations and carries further risk. Our 2021 Insight Report looking at Security Governance risks in the supply chain highlighted that 13% of organisations do not have an appointed person responsible for information security which naturally makes it more difficult for security to be properly considered across an organisation.

We all talk about getting the basics right, and the risk reduction this gives cannot be overstated. This is not always easy. An asset inventory, for example, whilst crucial, can be very difficult to put together and maintain. The key here is to not be paralysed by the search for perfection. Effective security management is all about being risk focused, and the 80-20 rule here will serve you well.

Legacy systems are another ongoing challenge which our data shows organisations must do better at managing. One in five organisations are running systems which are no longer supported by the manufacturer. Replacing outdated systems is something that requires input from a variety of stakeholders and is often pushed back in favour of business requirements. If this decision is made with proper consideration of security risks, it may well be the right decision for the organisation but it is important to be aware of the legacy risks within your supply chain and ensure you are comfortable of what that means for your own business.

Not all security controls are difficult to implement. There are some simple things all organisations can do which make a big difference. For example, data shows that 23% of organisations do not offer their employees a password manager and 22% do not enforce multi-factor authentication on all systems. The combination of these two risk control gaps makes for easy pickings for attackers. The security around passwords is a contentious topic in the information security world, and in future we may see an increased uptake in novel ways to manage identity which don't rely on passwords, but for now at least, passwords are here to stay and organisations need to take more responsibility for educating & providing appropriate tools for their users to keep their passwords safe.

You'll see other examples as you read through the report. The key to effective, secure IT operations is cross-team collaboration; respecting each other's priorities to keep the organisation running whilst being cognisant of the security risks involved.

IT Operations Risks in the Supply Chain

IT operations are a set of processes and services designed to monitor and control IT services across an organisation. This includes risk controls that should be implemented to maintain the health of an organisation's IT systems.

For third-party risk managers, if they have access to data about the set of IT operations risk controls implemented by an organisation in the supply chain, they get direct insight into the specific measures being taken to minimise the possibility of various types of disruptions and make decisions accordingly. Access to accurate, up-to-date data is essential in that process.

This report makes use of data collected in the IT Operations section of Risk Ledger's standardised Supplier Assessment Framework (SAF)[1] developed with support from the National Cyber Security Centre (NCSC). Over 1000 organisations have now completed and continuously maintain a supplier assessment on the Risk Ledger platform so existing and new clients are able to access the data contained in this report on a granular, supplier by supplier basis with the addition of contextual notes and evidence supporting the implementation of each risk control.

Throughout the report, we have tried to contextualise the statistics we found to make them more informative. The last section looks at combinations of risk controls that complement each other, how they are, or are not, being implemented across the supply chain ecosystem and what this means for cyber resilience in the supply chain.

Highlights

- 1 in 4 organisations don't enforce passwords on their employees' mobile devices, or have the ability to remotely wipe compromised devices, despite allowing employees to access company sensitive data on those devices.
- 1 in 5 organisations run applications or systems that are no longer supported with security updates by the manufacturer.
- Over a quarter of organisations have not implemented TLS email security, leaving the content of their email communications, and any sensitive information shared in them, unencrypted and easily accessed by those other than the intended recipients.

Contents

[1]This insight report takes a close up look at IT operations security 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 950+ suppliers of all sizes representing a broad range of industries and is a strong reflection of the supply chain risks facing organisations across most industries.

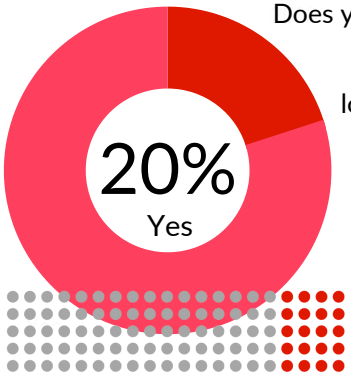
Data Insights

The statistics in our Insight Reports are drawn directly from the aggregated and anonymised data shared by the 1000+ suppliers on the Risk Ledger platform. Click on each statistic to find out more about the risk control and how to implement it.

Suppliers with a completed Risk Ledger supplier assessment include:

Capita, UiPath, Raytheon Technologies, HubSpot, LexisNexis, VISA, Klarna, citrix, AON, Adobe, headspace, DHL, SurveyMonkey, Lloyds Bank, bp, LinkedIn, ATKINS, invision, salesforce, DELL, CBRE, DARKTRACE, Auth0, Bupa, NOKIA, okta, Raytheon Technologies, SITECORE, PLURALSIGHT, KPMG, vodafone, zendesk, Looker, mastercard Payment Gateway Services, EY, HUAWEI, DocuSign, checkout.com, ERICSSON, clearpay, American Express

Patch Management

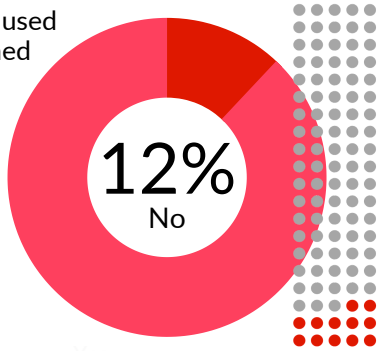


Does your organisation run any applications or systems that are no longer supported and no longer receive security updates?

This is too high. Vulnerabilities found in applications and systems that are no longer supported can be exploited by relatively low skilled attackers. Third-party risk managers should seek further information from suppliers about their exposure to these applications and systems and other measures being taken to minimise the risks.

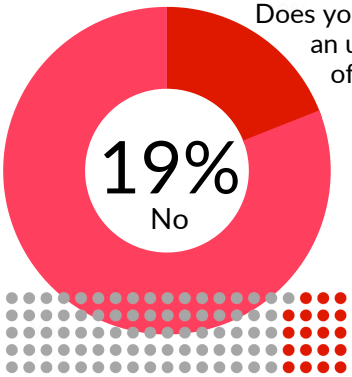
A significant proportion of attacks happen because of unpatched systems. The NCSC says that 'patching remains the single most important thing you can do to secure your technology'. Third-party risk managers should assess whether their third parties who say no to this control are able to at least say they regularly patch the most critical vulnerabilities in a timely manner.

Does your organisation ensure that all IT systems used are regularly patched with security patches in line with vendor recommendations, including user end point devices, network devices, and servers?



Asset Management

Click on each statistic to find out more about the risk control and how to implement it.

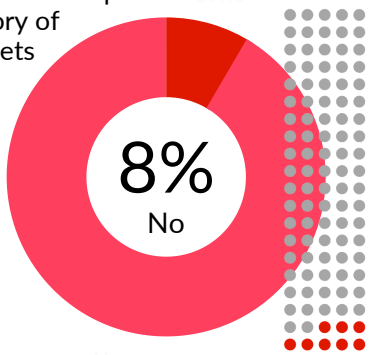


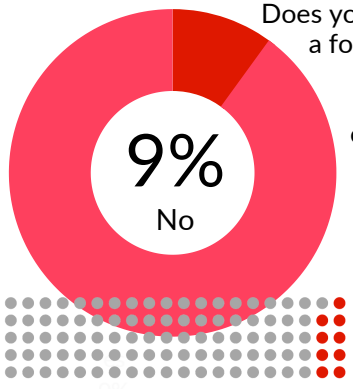
Does your organisation keep an up-to-date inventory of all data repositories (such as databases) with assigned owners?

It is self evident that you can't secure data if you aren't sure where it is. Shadow IT is a big part of the challenge here so third-party risk managers should be trying to understand whether their suppliers have a good partial inventory or whether this control is totally absent.

Maintaining this inventory is a prerequisite to implementing security controls across the IT estate. Again, third-party risk managers should be trying to understand whether a 'no' response means there is a good partial inventory or that this control is totally absent.

Does your organisation keep an up-to-date inventory of all IT hardware assets with assigned owners?



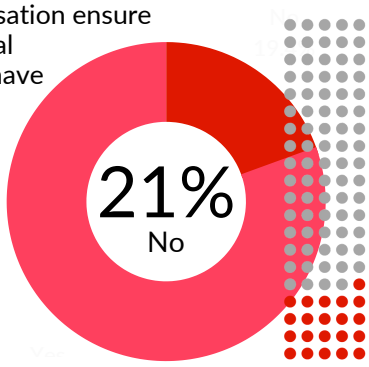


Does your organisation have a formal leaver's process to ensure that employees, contractors and third party users return all IT assets when they leave the organisation?

In the absence of a formal process, third-party risk managers should seek evidence that suppliers track custody of IT assets throughout their lifecycle.

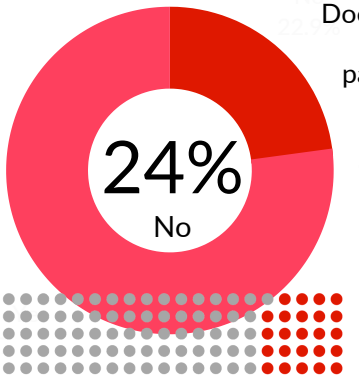
Third-party risk managers need to challenge the 1 in 5 organisations who do not currently implement this control to understand how they can be confident there is no unauthorised access to sensitive data during and after decommissioning.

Does your organisation ensure that all used digital media (that may have stored data) is disposed of securely and are certificates of destruction obtained?



Authentication

Click on each statistic to find out more about the risk control and how to implement it.

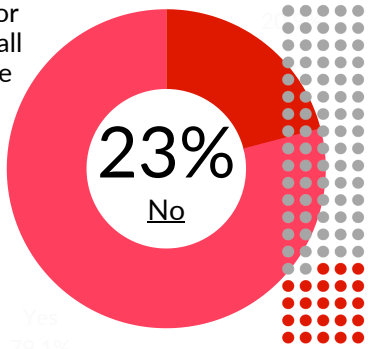


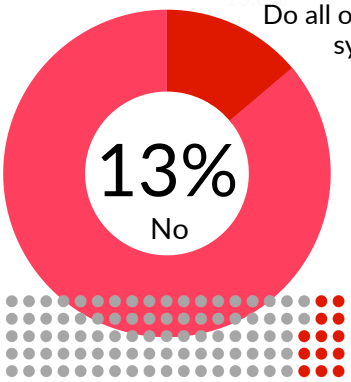
Does your organisation use/provision a password manager to ensure passwords are of the required complexity and only used once?

For IT teams, password managers are currently the only real way to effectively manage passwords and they are relatively easy to implement. While there are some interesting new alternatives emerging that don't use passwords, they are not yet widespread.

There is little excuse not to enforce multi-factor authentication when it is available. Third-party risk managers should be pushing for this additional layer of security to be enforced on at least the most sensitive applications and services.

Does your organisation enforce multi-factor authentication on all remotely accessible services (both within your internal IT systems and on third party services)?



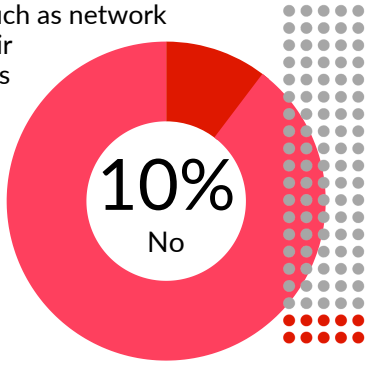


Do all of your organisations' systems automatically lock after a short period of inactivity (requiring re-authentication)?

The average number of minutes that a user has to be inactive before the system automatically locks is 56 minutes as reported by suppliers who do have this control in place.

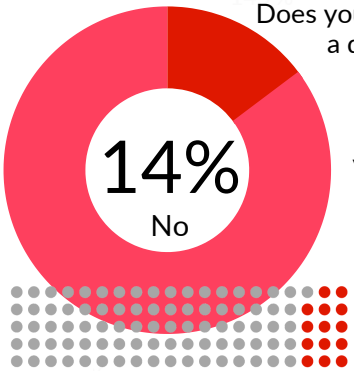
This control should be implemented as part of even the most basic security regime. Not taking this precaution as matter of policy could be an indicator of poor cyber security awareness and a supplier that requires further scrutiny and support.

Do all systems (such as network devices) have their default credentials changed on installation or provision?



Identity and Access Management

Click on each statistic to find out more about the risk control and how to implement it.

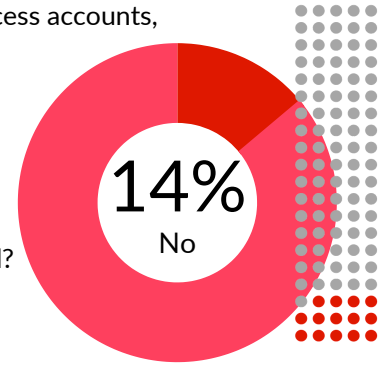


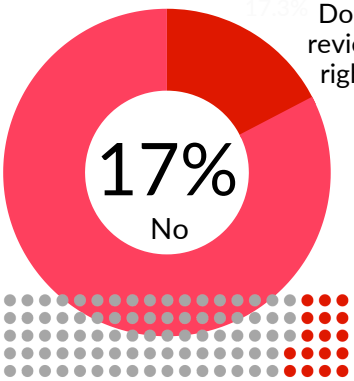
Does your organisation have a documented process for the provisioning and removal of user accounts for all of your IT services that includes a secure logon with unique user IDs?

Without a clearly documented process, organisations are reliant on individuals to ensure accounts are created & deleted securely. Third party risk managers should ask suppliers to demonstrate how they know this is done properly every time.

Usually, an attacker will first gain a foothold using a standard user account, and then look to escalate their privilege by targeting other, more highly privileged accounts. This control is important to ensure you don't inadvertently provide privileged access to an attacker.

Are privileged access accounts, and accounts of a sensitive nature, subject to a higher level of authorisation than user accounts before being provisioned?



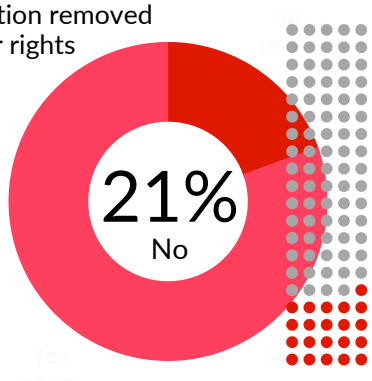


Does your organisation review employee access rights for all IT services (whether internal or third party based) at regular intervals?

Data shared on the Risk Ledger platform shows that suppliers who review employee access rights do so 7 times per year on average for both regular and privileged employee accounts.

This control is important to minimising the impact of a compromised device to the wider network and clients further down the supply chain. It is worrying that as much as 20% of suppliers do not implement this risk control as this puts more reliance on other controls if they are in place.

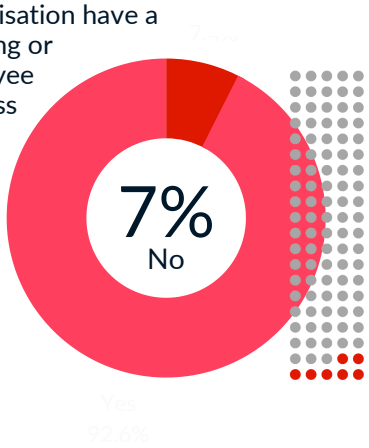
Has your organisation removed local administrator rights on all end point devices for all employees that do not require it?



Click on each statistic to find out more about the risk control and how to implement it.

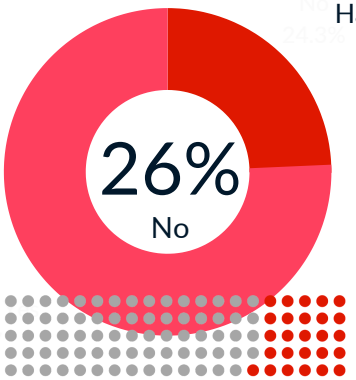
It is good that over 90% of organisations in the supply chain ecosystem have this control in place but given the significant turnover of employees caused by the pandemic during 2020/21, third-party risk managers should be checking how these processes are being maintained in a largely remote working environment.

Does your organisation have a process for editing or removing employee access to business confidential information (whether digital or physical) when they are changing role or leaving the company?



Email Security

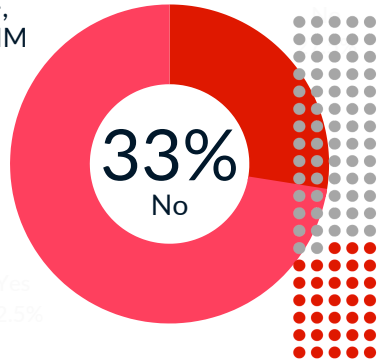
Has your organisation configured its email services to use enforced TLS?



Most employees at the 26% of organisations who do not enforce TLS on its email services will not know or understand that this means the sensitive data they send by email could be easily intercepted, viewed and modified.

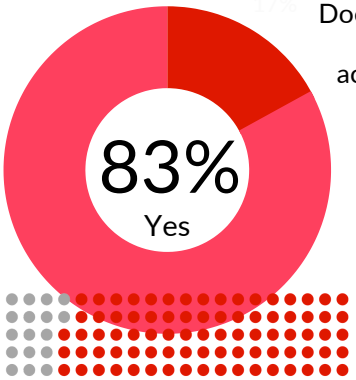
Although there are anti-spam tools that organisations can put in place, there is no good reason not to implement these three complementary protocols. Failure to do so by over 30% of organisations in the age of increasing ransomware attacks feels like an invitation to cyber criminals and a recipe for critical suppliers to be knocked offline easily. Only one phishing email needs to get through!

Has your organisation implemented SPF, DMARC, and DKIM for all of its email services?



Mobile Device Management

Click on each statistic to find out more about the risk control and how to implement it.

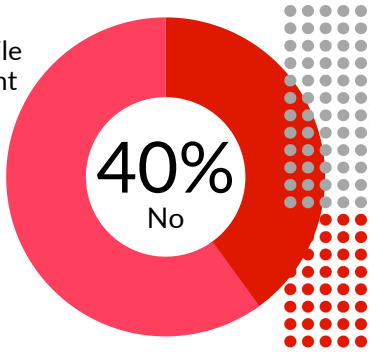


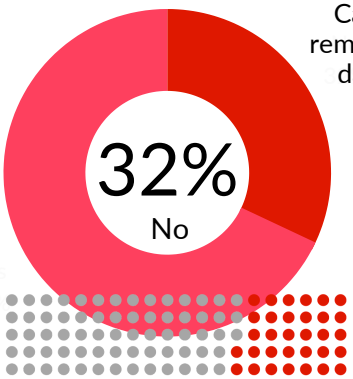
Does your organisation allow employees to access company data (including email) through their mobile phones?

This proportion will have increased during the pandemic so third-party risk managers should ensure their suppliers have implemented a set of security controls to manage the risks appropriately.

You don't have to be very creative to imagine the potential consequences for clients if a supplier employee's unsecured mobile device falls into the wrong hands with access to emails and cloud storage like OneDrive or GDrive.

Does your organisation control the use of mobile phones using mobile device management (MDM) software which enforces a password policy for all devices?



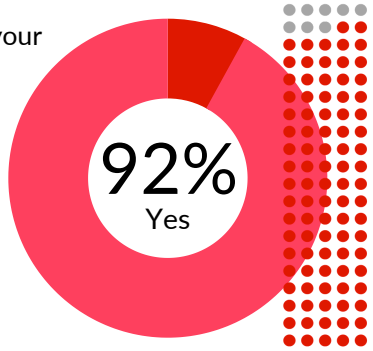


Can your organisation remotely wipe company data on compromised mobile devices?

Even if this control is in place, it is worth noting that it only works when employees understand the importance of notifying the right people when a device is missing or compromised.

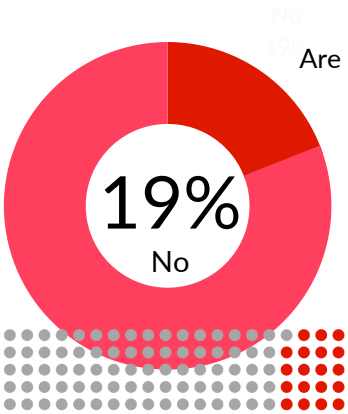
Third-party risk managers should be looking for suppliers to have in place a set of risk controls that acknowledge laptop devices present a different set of security risks to desktop computers.

Do employees in your organisation use laptop devices?



Encryption

Click on each statistic to find out more about the risk control and how to implement it.

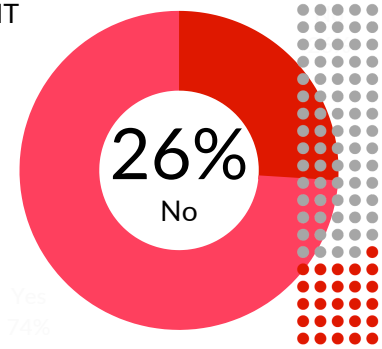


Are all of the laptop hard drives encrypted?

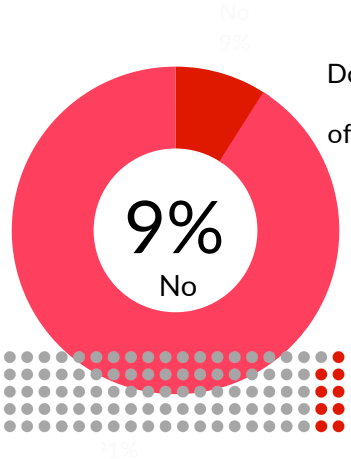
This is another control that has increased in importance due to the move to remote working during the pandemic in 2020/21 and it will remain highly relevant as organisations adopt much more flexible and mobile work patterns going forward.

This is a surprisingly high proportion and puts more reliance on other risk controls. If third-party risk managers are informed that their suppliers do not encrypt client data, it is important to review these other controls. This is particularly important if PII is involved and they are in scope for GDPR.

Does your organisation encrypt client data on its IT systems?



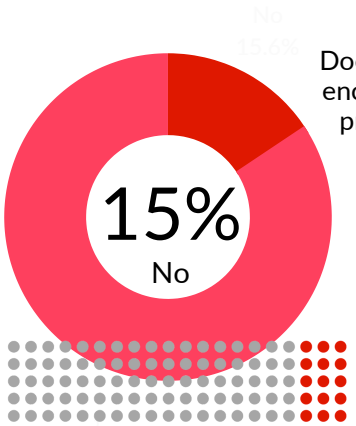
Operational Security



Does your organisation take regular backups of its digital production data?

Given the prevalence of ransomware attacks, even 9% is a high proportion of suppliers who don't backup digital production data. Third-party risk managers must consider the impact to their organisation if a supplier cannot deliver its services for an extended period of time.

Click on each statistic to find out more about the risk control and how to implement it.

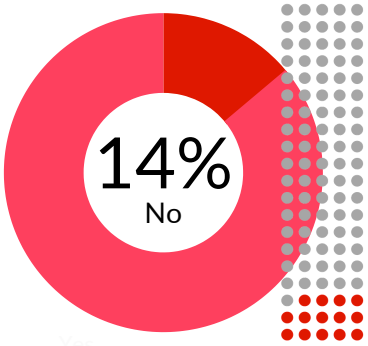


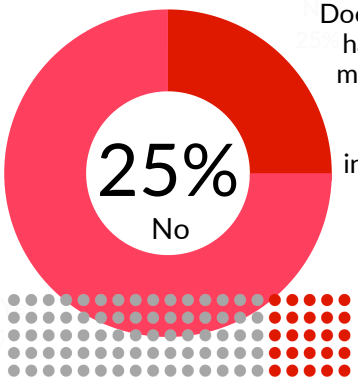
Does your organisation encrypt the backups to prevent unauthorised access to the backup data?

The dangers of not encrypting backup data are obvious but it is also important to consider the type of encryption used. If a supplier is critical or important to your organisation, you should interrogate the type of encryption used to ensure it is secure enough. A completed Risk Ledger supplier assessment will give you this information.

Without regularly testing backups and the ability to recover from an incident using them, they are nearly useless. Third-party risk managers must assess whether critical and important suppliers are running adequate tests. This is even mandated in some regulations for critical industries.

Does your organisation regularly test backups to ensure their effectiveness?



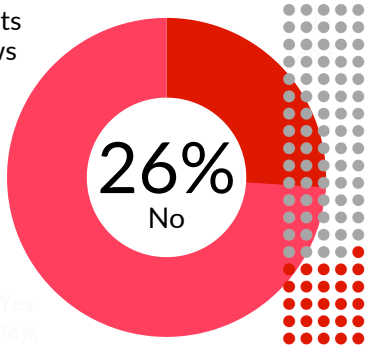


Does your organisation have a formal change management process that gives consideration to information security?

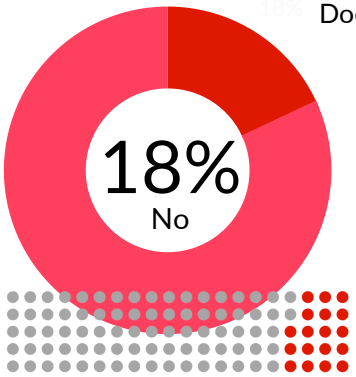
Change is inevitable at every organisation and the change process introduces risks of misconfigurations, new vulnerabilities and unexpected downtime. It is essential that information security is considered from the planning stage to mitigate these risks.

AutoRun and AutoPlay features on Microsoft Windows systems are well known attack vectors. While removable media may have fallen out of favour in mature security environments, that may not be the case in your supply chain.

Has your organisation disabled auto-run on all of its Microsoft Windows based IT systems?



Click on each statistic to find out more about the risk control and how to implement it.

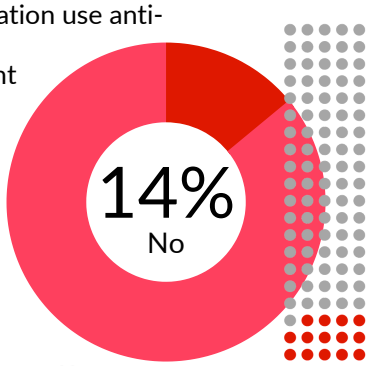


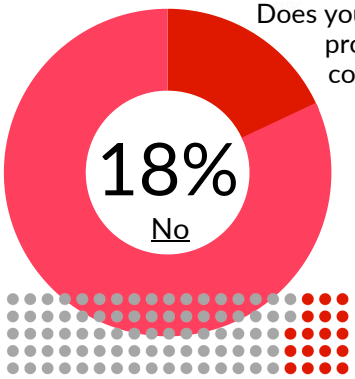
Does your organisation operate a secure configuration process to reduce any unnecessary vulnerabilities in your IT systems, including systems hosted in a cloud environment?

Translating an organisation's security principles into appropriate configuration of IT systems is not straight forward, particularly in cloud environments. Third-party risk managers should be looking for evidence of a robust lockdown/hardening guide for all relevant infrastructure.

This control should be part of even the most basic security regimes. 14% is high and even if data or access to networks and systems isn't shared with suppliers lacking this control, they are vulnerable to being used as a staging post to deliver malicious payloads to any client they do business with.

Does your organisation use anti-malware controls, such as an Endpoint Detection and Response (EDR) solution, to protect all of its endpoints and internal IT infrastructure?



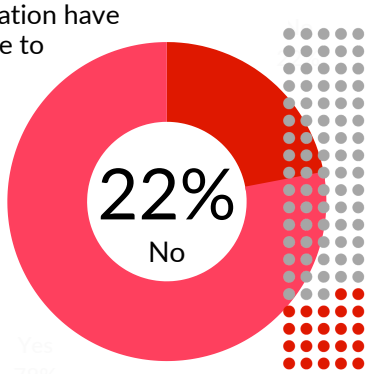


Does your organisation have procedures in place to control the installation of software on IT production systems (such as servers)?

The absence of this control and the next means that system administrators are the sole arbiters of what gets installed on IT production systems and for security, this relies on them never making a mistake or their accounts never being compromised.

Without this control, organisations are trusting their users not only to behave securely themselves, but also trusting that they will not fall foul of a phishing email or other social engineering attack which gives access to their device. Third-party risk managers should be looking for evidence of software restriction controls & robust exception processes.

Does your organisation have procedures in place to control the installation of software on user endpoint systems?



Insights

18% of organisations in the supply chain ecosystem either do not take regular backups of their digital production data or they don't regularly test backups to ensure their effectiveness. That is nearly 1 in 5 organisations who either don't have the option to revert to backup data or don't know whether their backups are useful. Backups are a critical control in any organisation's business continuity and cyber resilience planning and if that organisnation is one of your important suppliers, their resilience impacts your business too.

24% of organisations in the supply chain ecosystem allow their employees to access company data on mobile devices but cannot remotely wipe data on a compromised mobile device and do not use Mobile Device Management (MDM) software that enforces a password policy on the device.

In the age of mass remote working and an increased number of mobile devices being used to access company applications, services and data, this absence of mobile device security management gives too many options to malicious actors seeking to launch third-party cyber attacks or disrupt your supply chain.

11% of organisations in the supply chain ecosystem neither require a higher level of authorisation to provision privileged user accounts nor regularly review access rights to IT services for employees. This means that within these organisations, there are likely active privileged accounts that are surplus to requirements and perfect targets for attackers.

7% of organisations in the supply chain ecosystem do not maintain an up-to-date inventory of data repositories with assigned owners and do not have a process for editing or removing employee access to business confidential information when they are changing role or leaving the company.

This creates the real possibility that employees who no longer work for your third party continue to have access to confidential information relating to the business you do with them. This is a problem if it happens accidentally but insider threats determined to maliciously gain unauthorised access to confidential information are also a risk and they benefit from these risk controls gaps.

Upgrade your third-party risk management programme

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

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

Find out more about Risk Ledger

Contact us for a demo

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

Published June 2021

riskledger.com