littlefish
managed IT services

IMPROVE YOUR CYBER MATURITY

Twelve key controls you need to know

INTRODUCTION

littlefish
managed IT services

As cyber-attacks continue to increase in sophistication, taking advantage of at-risk data in growing and vast networks, and as new attack avenues also continue to be created using technology such as the Internet of Things (IOT), insurers grow increasingly cautious about who and what they are willing to protect.

Perhaps this is to be expected, after all, the UK Government's Cyber Security Breaches Survey 2023 revealed that 32% of businesses and 24% of charities suffered breaches or attacks in the last twelve months (although this is much higher for medium businesses (59%), large businesses (69%), and high-income charities (56%)).

There's also the – somewhat chilling – news to consider that cyber security as a business priority appears to be in decline. Password policies, use of network firewalls, and access management/use of admin rights have all decreased between 2022 and 2023, so it's perhaps no surprise at all that only four in ten businesses (37%) report being insured against cyber security risks – although this rises to 55% if only looking at large businesses.

Still, it does seem that cyber maturity for UK businesses is experiencing a contraction of sorts overall; possibly due to additional concerns surrounding the current economic climate, which has recently recorded its largest slump since March 2009, outside of the COVID-19 pandemic's impact, at least.

Even in this climate, cyber criminals remain ever opportunistic, however, and as cyber-attacks become more prolific, related insurance claims have followed. This means there's data to examine, through which a correlation between certain controls and corresponding cyber incidents has been identified.

It's common nowadays for underwriters to ask organisations to document their cyber security practices if they are to qualify for coverage and secure a reasonable premium, and – while most of the controls insurers are looking to see have been established security practice for several years – some companies are still struggling to adopt them or take them seriously, as more than 'just' box-ticking exercises.

In this guide, Littlefish hopes to share information to help your organisation get ahead of the curve. I hope to increase your cyber resilience and, in turn, ensure you are better 'cyber insurance prepared'.

Read on to discover the twelve key steps your organisation can implement now to achieve cyber maturity and insurability. I hope it helps.

Best wishes,

Sean Tickle
Cyber Services Director

littlefish
managed IT services

CONTENTS

01 Multifactor authentication (MFA)

02 Endpoint detection and response (EDR)

03 Secure backups

04 Email filtering and web security

05 PAM and PIM

06 Patch and vulnerability management

07 Incident response planning

08 Awareness training and phishing simulations

09 Remote desktop protocol (RDP) mitigation

10 Logging and monitoring

11 Replacement of end-of-life (EOL) systems

12 Digital supply chain risk management

Select page

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 1: Multifactor authentication (MFA)

Without MFA as a security baseline, it's practically impossible to get cyber insurance. MFA requires the user to provide two or more pieces of evidence in order to pass security controls, e.g., a password or PIN along with an authentication key or other security token. By providing an additional layer of defense, MFA reduces the risk of account compromise should one form of authentication become compromised.

This is of particular importance given that weak, short, or re-used passwords are a major vulnerability hackers seek to exploit and still one of top risk issues for organisations (and people in general!) today. As such, MFA is an essential part of a strong identity access management (IAM) strategy and one that insurers will not overlook.

Meeting MFA requirements

It may not be straightforward for organisations to meet MFA requirements and become completely cyber mature in this area. Littlefish's cyber team is always on-hand to guide you through this process – especially if your digital infrastructure is complex – but, as a basis, consider:

- **Identifying all systems and applications** that are accessible remotely and ensuring this infrastructure is accessible through a VPN, with MFA enforced as standard.
- **Identifying what critical and sensitive data** your organisation processes or stores, as well as the systems and applications it's stored on.
- **Identifying high-privileged users,** e.g., admin, and implementing risk-based authentication.
- **Identifying all corporate devices used by anyone** to access company systems and implementing restrictions for personal devices or certain geographic locations (e.g., additional security protocol for access outside of your country).
- **Implementing security defenses** to avoid infecting the entire network if one device should become compromised.
- **Rolling out regular user education** on the importance of MFA.

At absolute minimum, it's important to enforce complex, long passwords companywide (at least fourteen characters, including upper and lowercase letters, numbers, and symbols) and to also enforce **MFA** on all:

Critical assets

Privileged accounts

Remote applications

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 2: Endpoint detection and response (EDR)

All organisations use endpoint devices, e.g., desktop computers, laptops, mobile phones, the organisation's servers, and so on.

As user devices that connect directly to company networks and store confidential information, endpoint devices are immensely appealing targets for cyber criminals and require monitoring to detect and counter cyber-attacks before they spread to wider organisational assets.

EDR assumes and promotes a security strategy in which teams accept security breaches as inevitabilities, whilst still understanding how they can detect, respond, and remediate threats effectively. Using EDR, company endpoints are monitored around the clock, detecting and countering suspicious activity before it spreads to wider internal networks.

EDR solutions use machine learning (ML) and continuous monitoring to identify security threats. They also collect data to determine when that threat began, the scope of the compromise, and the root cause – as well as having the ability to remotely respond and contain threats across the endpoint device estate.

Putting EDR in place

It's worth mentioning that, in a robust cyber security strategy, advanced attack response capabilities would spread across as many attack vectors as possible; not just end points, but also other surfaces including email, user accounts, applications, and cloud infrastructure.

If your organisation is looking to implement an EDR strategy, remember to search for the maximum level of protection, and to speak to your service provider about:

- **Providing real-time visibility** to view suspicious activities across all endpoints and stop breaches entering your environment.
- **Provide more granular detail in the processes** running upon these endpoints and if their activity is considered malicious.
- **Collating data and other threat intelligence** from endpoints to inform your security strategy and identify indicators of attack (IOAs) before breaches occur.
- **Implementing a cloud-based endpoint detection and response solution** to ensure integration with current systems.
- **The ability to take enhanced response actions remotely**, such as restricting what can be run on the device, establishing a remote connection for further investigation, and isolating the device from communication with anything but the EDR solution itself.
- **Providing the ability to embed centrally managed proactive policies** to block potentially harmful activity and reduce the attack surface of your endpoint assets.
- **Setting-up automated actions**, based on your risk appetite, should a possible breach occur.
- **Ensuring your solution** minimises the likelihood of false positives.

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 3:
Secure backups

Secure, available, and accurate backups are essential to ensure business resilience and reduce the risk of needing to pay ransom should a cyber-attack be successful. As organisations increasingly move to cloud-based solutions, ensuring that compromised credentials do not lead to losing cloud-based back-up data is imperative.

Since, unfortunately, many ransomware attacks now target backup data precisely to prevent recovery and, in this way, gain leverage, your organisation's backups need to be secured. This means isolating them from the core IT network and/or implementing multifactor controlled access and encryption.

Backups should generally not be able to be deleted or modified once accessed and must undergo regular testing to ensure availability and prove your team's (or service provider's) capability for managing a full (and often complex) restoration process. Testing also ensures that any errors in the process are identified and can be rectified prior to the pressure of an attack.

Having a thorough and viable backup process in place means your organisation will be able to recover from an attack relatively quickly and with less financial loss. It can also avoid the need to engage with cyber criminals, which is never an advisable option without specialised support, and therefore reduces the business loss insurers would be required to cover.

Ensuring your backup plan is viable

It's always a good idea for organisations to review their critical systems and assets and ensure that internal IT teams (or their service provider) have a failsafe backup plan in place and that it is regularly tested and modified accordingly.

As part of disaster recovery, business continuity, and incident response procedures, backup plans are a vital part of organisational resilience and, when considering yours, it's important to remember to:

- **Identify critical data** - identify and classify the data that needs to be backed up.
- **Ensure backups are scheduled regularly** to confirm data is always up-to-date and readily available in case of a disaster.
- **Ensure your backup and recovery plan includes offsite storage of backups.** This guarantees that your data can be recovered from the offsite storage location even if a disaster affects your primary site.
- **Put a disaster recovery plan in place** which outlines the steps your business will take in case of a disaster. This includes activating the backup plan, notifying stakeholders, and testing the recovery process.
- **Roll-out employee training on the backup and recovery plan to key stakeholders.** This will ensure that your staff members are aware of their responsibilities in the event of a disaster and are capable of acting accordingly.

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 4: Email filtering and web security

Since malicious phishing campaigns containing links and files are one of the primary methods cyber criminals use to compromise user accounts and insert malware into an organisations' system, email content filtering and protection solutions are a must. These tools are used to enforce proactive policies that scan email elements such as URL links and attached files, identify malicious content, and block malicious emails/ content based off criteria outlined within your risk appetite.

Web and email filtering can stop users from ever receiving flagged content by automatically filtering it out. In this way, filtering negates, or at least drastically reduces, the chance of users needing to identify malicious content themselves (while also making them hyper-aware of the content and the threat it poses by flagging it very obviously). Using email security software, additional functionality can be achieved, such as the deletion of a suspicious email across the organisation's entire email estate and the sender to be blocked. This means, in the event of a widespread attack, your response can be swift and effective.

Web filtering is used to prohibit users from accessing malicious or unauthorised content through their web browser and can be deployed at the endpoint or network level. It's also useful as an additional layer of security to email protection since it can block malicious email links from ever being opened.

Reasons for web filtering may include blocking malicious or dangerous content, as well as restricting access to unsavory or non-compliant sites, e.g., certain forums, gambling sites, video streaming sites, and so on.

Implementing email security and content filtering

Email security and content filtering is essential for cyber security maturity, particularly because email phishing is one of the top initial attack vectors leading to severe cyber incidents, especially user account compromises.

In order to put these controls in place, remember to:

- **Talk to your teams or service provider** about implementing technology to scan and filter incoming emails for malicious attachments and links.
- **Ensure that macro-enabled and executable files** are prevented from running by default.
- **Speak to your IT team or service provider** about creating a sandbox environment prior to user delivery.
- **Evaluate what proactive email security policies**, based on your risk appetite, you wish to embed within your email infrastructure.
- **Discuss which websites you wish to block** and use technology to regulate access to malicious websites.

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 5: Privileged access management (PAM) and Privileged identity management (PIM)

Just as it sounds, privileged access management is a security technology that controls privileged access of machines, systems, or applications. Together, identity and access management (IAM) and privileged access management (PAM) solutions establish strong access controls and run on the principle of 'least privilege' (meaning all users receive the minimum level of access required to perform their job functions).

Enhancing your PAM solution with privileged identity management (PIM) ensures that permissions will be assigned just in time, and for a time-bound duration, ensuring privileges are not active any longer than necessary. PAM solutions also monitor sessions that are used by administrator accounts and generate alerts and reports for unusual usage, thus affording more control over privileged identities and activities and the ability to identify and investigate anomalies.

A PAM solution must always have the capability to support company access policies (for example, MFA), and security administrators will be able to modify or delete accounts and their level of access as necessary. By limiting the number of users who have access to administrative functions, cyber security is bolstered while additional layers of protection mitigate data breaches by threat actors.

Introducing a PAM solution

While every PAM solution will be different, there are best practices to keep in mind when planning for yours.

See below, these should be discussed with your team or service provider:

- **Multifactor authentication**, so privileged access users can provide additional identity verification through another verified device.
- **Human error risks can be reduced** by leveraging automation within the security environment, e.g., by automatically revoking access whenever a threat is suspected.
- **Unnecessary endpoint users** should be identified and removed regularly.
- **Ensure privileged access activity is monitored** regularly to establish what is 'normal' activity and help spot anomalies.
- **Always apply least-privilege policies** to all users and elevate as needed.
- **Avoid perpetual privileged access** and consider temporarily granting privileged access just in time. This ensures access is only granted for the time required.

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 6: Patch and vulnerability management

A consistent approach to vulnerability management, including patching and updating software and operating systems, helps limit exposure to ransomware and other malicious endeavors.

Vulnerability management involves continuous, proactive, and oftentimes automated processes that work to keep company systems and networks safe. It's a hugely important part of any cyber security strategy and helps organisations to identify, assess, and address potential security weaknesses, reducing overall risk exposure.

Remember, vulnerability management is a continuous process rather than a scheduled process that can be performed ad-hoc. Today, with the growing Internet of Things, running occasional security scans and dealing with cyber threats reactively rather than proactively is not sufficient (and insurers certainly don't see it as such).

Whilst establishing a relationship between proper IT vulnerability management and risk tolerance is complex and can also be time consuming (making it therefore difficult to always get board level buy-in), a proper patch and vulnerability management function is incredibly worthwhile when it comes to cyber resilience.

Expect vulnerability management to reduce or eliminate the potential for exploitation, provide up-to-date reporting on your security posture, and offer operational efficiencies by understanding security risks and minimising downtime.

An effective vulnerability management program

While complex, most vulnerability management plans will have commonalities which **include the below:**

- **Asset discovery and inventory,** i.e., the tracking and maintaining of all devices, software, servers, and more, across the company's digital environment.
- **Vulnerability scanners –** these work by running tests against systems and networks and looking for common weaknesses, flaws, or known vulnerabilities.
- **Patch management software,** which helps organisations keep all systems and software up to date and secure.
- **Installation of security configuration management (SCM) software** to ensure that devices are configured in a secure manner and that changes to device security settings are tracked and approved.
- **Use of a security incident and event management (SIEM)** system to offer visibility into everything that occurs across the digital estate.
- **Penetration testing to help IT professionals** find and exploit vulnerabilities in computer systems.

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 7: Incident response planning

Incident response plans are integral when it comes to increasing your organisation's cyber resilience.

Whether created in-house or alongside an external cyber service provider, a formal incident response plan which details a complete 'plan of action' in the event of a cyber-attack is much sought after by cyber insurers and is even more effective when built upon a recognised standard (such as the SANS PICERL process).

Incident response plans offer assurances that your organisation understands its own unique risk profile and also has a trained team in place that can respond to cyber incidents effectively, speedily, and professionally.

Incident response plans usually comprise of an IT disaster recovery plan (DRP), which describes how you will recover data during and after a crisis or disaster, as well as a business continuity plan (BCP), which sets out how you intend to maintain essential business practices and value-making processes.

It's important for all relevant stakeholders to be trained in the process of incident recovery and to understand the steps of the plan thoroughly. This significantly reduces the impact of successful cyber events, saving time, costs, and possibly your reputation.

Additionally, it's a good idea to perform annual tabletop exercises around your incident response plan. These exercises consider simulated scenarios that could negatively impact your organisation and usually involve both internal and external stakeholders. It's a chance to analyse the crisis management capabilities of your team and test the efficacy of your incident response plan.

Creating an incident response plan

Incident response plans should include several core capabilities and be tested regularly for errors or necessary modifications.

Your plan should include the following components:

- **A thorough and well-defined process and procedure** for cyber incident handling, reporting, and recovery.
- **Each response team members' roles, tasks, and responsibilities** during a security incident, including decision making processes/people.
- **What part of the plan will be dealt with externally,** e.g., criminal investigations or backup recovery, and any contact information needed to set this in motion.
- **Regular reviews and updates incorporating recent developments**, such as new threats, different infrastructure, changing employees, etc.

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 8: Cyber security awareness training and phishing simulations

User education helps to inform and empower employees, imparting the knowledge they need to recognise and protect themselves in the event of an attempted cyber-attack. It's important for insurers to see organisations undertaking regular cyber security training with their users, after all, it exemplifies that your organisation is doing all it can to equip users with the necessary information to mitigate everyday risks.

Awareness training also helps keep security practices fresh in the minds of users, reducing the risk of human error due to complacency or simply being too busy to think – both are major factors in almost all cyber security incidents, as most phishing attempts simply hope to catch users unawares.

Effective security awareness training helps employees understand the role they play in helping to combat security breaches, the security risks associated with their day-to-day activities, and what cyber-attacks they may encounter via email or other work-related actions and/or devices.

Phishing testing will form a major part of organisational security awareness training since it tests the effectiveness of the training itself and determines any behaviors that require further improvement. Phishing simulations use real-life, defanged attacks to analyse user behaviour and roll out additional training to anyone who falls for the 'scam'.

Ensuring your user education is effective

Whilst offering users cyber security training courses is a good start, there are things organisations can do in addition to this to boost user awareness levels:

- **Focus on behaviour -** awareness training is about changing behaviours, not passing tests. To achieve this, content should be user-led and based upon identified areas of weakness and gaps in knowledge.
- **Time it right -** awareness training programs should never be deployed in haste. Consider a phased rollout, perhaps utilising microlearning modules to allow you to meet some immediate requirements whilst still factoring in your employees' workflows.
- **Offer continuous education -** for long-term success, your staff awareness program should be an ongoing process; one that begins at induction and continues frequently (certainly more than annually) and offers education about a variety of cyber security topics, not just the hum drum.
- **Consider specific needs -** when it comes to staff awareness, the 'one-size-fits-all'. approach isn't appropriate for most organisations. Consider the diverse needs and culture of your business – as well as any specific cyber risks your industry faces – and tailor the awareness training accordingly.
- **Simulate attacks -** deploy simulated phishing attacks designed to test the susceptibility of users to falling victim to a phishing scam. Further training can then be quickly deployed to any employees that need it – i.e., those that clicked on the fake phishing link – therefore building your organisation's resilience against this very common attack vector.

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 9: Remote desktop protocol (RDP) mitigation

Remote desktop protocol (RDP) is a secure network communications protocol developed by Microsoft. It enables users to access company resources remotely using an internet connection.

In essence, RDP is a way to access and control a computer over a network and gives users remote access to their physical work desktop computers, which, for best practice, would be when they are VPN'ed into the network securely.

Benefits of utilising RDP include safely storing and encrypting data using cloud servers (thereby reducing the risk of data loss), however, exposing RDP to the wider internet is not recommended and the use of VPN would always be encouraged. RDP clients are available for most versions of Windows as well as other operating systems such as macOS, Linux, Unix, Google Android and Apple iOS. An open-source version is also available.

To mitigate cyber risks when using RDP, hardening techniques are used to minimise the attack surface available to cyber criminals, e.g., by disabling unused or insecure services, limiting connection access, mitigating vulnerabilities, and improving weak configurations that could be used by malicious actors.

Hardening remote desktop protocol

For cyber resilience, it's important to follow RDP best practices, e.g., not using open RDP connections over the internet or giving anyone direct access to an RDP server.

Other hardening techniques may include the following:

- **User and access management -** only granting access to users who have a valid business requirement and only the permissions required for them to carry out that purpose.
- **Password policies -** enforcement of a password policy of sufficient length and complexity, along with other best practice advice, such as leveraging a passphrase instead of a password on its own, and the use of a password manager.
- **Secure services and protocols -** ensure only secure and in-support protocols are used and disable protocols no longer in use, out of support, or vulnerable.
- **Firewall configurations -** it is important that both perimeter and internal network firewalls are configured to only allow in authorised traffic and block/alert on sustained malicious connection attempts.
- **Network configurations -** the segregation of networks and enforcement of mitigation features against hackers.
- **Log management and audit policies -** logging retention policies should be set on critical sources to an adequate level for review, ideally the use of a SIEM.
- **Endpoint Protection -** standard anti-virus solutions should be installed, up to date and active on all endpoints operating with your environment. Ideally, the use of an EDR solution would be embedded in addition to standard anti-virus.
- **Application control -** to establish proactive and secure application usage it is encouraged to first review what applications are required for business purposes and then sanction/prohibit their use within your organisations environment.
- **Security updates -** as a minimum, security updates for all systems and applications in use should have the latest security update installed and implemented within ten days of their release.
- **Encryption -** encryption of sensitive data in transit and at rest is an important security control to embed in order to mitigate unauthorised access to this data.

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 10: Logging and monitoring

As a result of digital transformation initiatives such as cloud adoption, IoT convergence, remote working, and third-party infrastructure integration, IT environments are becoming increasingly complex and sophisticated. It's partly due to this, and partly due to the ever-evolving threat landscape, that organisations need to enable strong logging and monitoring capabilities for all systems, software, and endpoint devices.

Logging is what we call the process of collecting and accessing logs, i.e., the parsing and collection of events that occurr within systems and applications inside your IT estate. These logs are timestamped and recorded and can be used to gain insights into the application's performance over time.

Monitoring, on the other hand, examines these logs for signs of unauthorised activity. Should anomalies be uncovered during monitoring, the data will be analysed further by security professionals and then necessary action taken, such as launching counter measures or initiating the incident response plan.

Remember, security event logging and monitoring only work as part of an effective data collection and analysis process. Therefore, establishing logging and monitoring capabilities requires specialist knowledge, tools, and processes, and normally falls under the remit of a security operations center (SOC) or an external managed security service provider (MSSP).

Implementing logging and monitoring

As mentioned, logging and monitoring capabilities are specialist capabilities that will usually **include the following:**

- **Identifying all systems and platforms** that are to be monitored.
- **Implementing** a security incident and event management system (SIEM).
- **Analysing the logs and identifying common patterns and any behaviors** the organisation would like to flag and react to (this information will also be used alongside threat intelligence information which would primarily be delivered by ensuring that the alert rulesets within the SIEM are up to date and mapped to your organisations threat landscape).
- **Defining clear processes** to review the behaviour and actions of users inside critical systems and the surrounding infrastructure.
- **Training/hiring or working with a managed service provider** to ensure a team of specialists monitors security events 24/7 and has an incident response plan in place.
- **Defining and monitoring key performance indicators** for continuous improvement.

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 11:
Replacement of end-of-life (EOL) systems

Perhaps unsurprisingly, cyber criminals target applications and systems that have reached end of support (EOS) or end of life (EOL), meaning they are no longer supported, patched, or updated by the vendor.

It goes without saying that once technology is unsupported, it's exposed to vulnerabilities. In fact, known vulnerabilities are openly discussed on hacker forums, and cyber criminals are able to scan for still-in-use EOL systems to target them specifically. What they're looking for here, of course, is an easy way to enter the network.

To put this into perspective, consider the WannaCry ransomware attacks of 2017. Wannacry utilised Windows XP's EOL by exploiting a vulnerability in the XP operating system, which was no longer supported by Microsoft. The attackers used a file called EternalBlue, which allowed the malware to spread from system to system without user interaction. In later Windows operating systems, this vulnerability could not be exploited, but since support for Windows XP ended in 2014, it remained wide open to attack.

Companies with outdated systems and no plan for upgrades are viewed as big risks by most insurance underwriters and there's really only one way to mitigate this risk: stop using them.

EOL and EOS applications should be replaced or upgraded to a newer solution with ongoing support, patches, and updates. Should this not be possible, additional security measures must be put in place, e.g., managing access to the system, isolating EOL systems from other applications, removing them from the internet, and so on.

Managing EOL systems

It can be difficult to discuss EOL systems with business stakeholders – and security teams often hear the same old cry: that the legacy system or technology in question is "critical" to the organisation (especially after having operated without issue for many years).

However, it's usually the case that EOL components become less and less reliable over time and therefore more prone to failures. It would be amiss to tolerate these symptoms until something goes really wrong.

Organisations can mitigate the risk associated with EOL technologies by taking a proactive approach with their service provider or vendor, staying abreast of new technology changes, and planning for them before the risk is overwhelming. **Organisations can, for example:**

- Research new technologies or new versions of existing technology
- Develop a timeline for transition
- Train staff on new features
- Create budget plans for the transition
- Buy technology with longer lifecycles
- Invest in backup systems in case of problems/delays during transitions

12 CONTROLS TO IMPROVE YOUR CYBER RESILIENCE

littlefish
managed IT services

Control 12: Digital supply chain risk management

The digital supply chain includes all information technology and operational service (OT) providers utilised by an organisation, as well as the organisations' in-house teams themselves. Obviously, digital suppliers can present entry points to hundreds of companies and, thus, by exploiting just one single vulnerability, cyber criminals have access to multiple networks and devices.

Unlike a traditional supply chain which usually encompasses a mix of paper and technology, digital supply chains capitalise on smart components and connectivity. They utilise advanced digital technologies so that businesses can make better decisions about the supplies they need, the demand for their products, and all the relationships in between.

The connectivity of the digital supply chain, however, means that risk can propagate throughout the supply chain network quickly. Thus, by exploiting just one single vulnerability somewhere in the chain, cyber criminals possibly have access to multiple networks and devices.

To ensure cyber insurance preparedness, organisations should evaluate their suppliers' security practices and ensure to incorporate specific security requirements into their contracts.

Protect your organisation against supply chain exposure

It's important for organisations to consider how they will manage digital supply chain risk and to discuss supply chain security with their internal teams or an external service provider.

When doing so, consider the following:

- **Adopting a risk management strategy** for the digital supply chain, including risk assessments for vendors and suppliers.
- **Implementing a robust cyber security framework** which includes zero-trust expectations and sharing information with third parties only on a 'need to know' basis.
- **Enforcing PAM and IAM strategies** for all external interactions (see control 5).
- **Developing and testing an incident response plan** for digital supply chain scenarios.
- **Discussing service agreements and escalation protocols** with each supplier.
- **Engaging with your internal procurement department** to put in place mandated cyber security practices to be followed for all contracts and renewals.

littlefish

managed IT services

PROTECT YOUR BUSINESS, PROTECT YOUR VALUE

To find out more about how Littlefish
can help protect your business:

Get in touch

info@littlefish.co.uk

0344 848 4440

Microsoft Solutions Partner

CYBER ESSENTIALS

CREST

SOC