MITIGO
CYBERSECURITY

CYBER SECURITY MATTERS

icas Partner 2024

ICAEW
MEMBER REWARDS
PARTNER

Contents

Why cyber security should be at the top of your risk register.

We have seen really good businesses brought to their knees by a cyber attack. It is a truly horrible, gut wrenching experience for the business leaders concerned: to watch the serious damage done to their brand, their reputation, client relationships, business operations and financial stability.

But it is a disaster which need not occur. Cyber breaches are not acts of God, nor do they result from bad luck. A serious cyber incident usually means that someone at board level has failed to understand the nature of cyber risk and has therefore not taken the right steps to protect the business. It is likely that legal and regulatory obligations have not been complied with either.

Obvious high risk sectors include professional services such as accountants, law firms and financial services. But the reality is that all sectors are under attack and all are at risk of operational disruption. This is more than just data protection, it is the ability of the business to withstand attacks and survive. All need to achieve full visibility of their cyber risks by undertaking proper cyber security risk assessments; have in place a comprehensive programme and control framework to manage those risks; with ongoing reviews of the effectiveness of defences; and independent assurance to give the board the confidence to sleep at night. And none of that is a job for your IT support - cyber risk management is a separate and independent specialist discipline.

So whether you are in private practice, private equity, industry or other commerce, I hope that what follows in this simple introductory guide will prompt you to ask yourself this question. Are we proving we are secure or are we just hoping we are secure?

Lindsay Hill
CEO
Mitigo Cybersecurity

Why Cyber Risk Management?

Managing cyber risk is a complex ever-evolving field, with numerous interconnected elements that must be considered to ensure comprehensive protection. Like pieces of a jigsaw puzzle, each component - from risk assessment to governance - must fit together seamlessly to create a robust defence. To combat the advanced threat landscape, businesses need a proactive, well-coordinated strategy that leaves no pieces missing in their defences.

It's a board level matter

The stakes are high. Cyber risk should have the same prominence as serious financial or legal risks, and responsibility and ownership of cyber resilience is a board level matter. Governance must include proper management information which is discussed by the senior leadership team at regular intervals.

Recognise the threat

You must understand the modern criminal ecosystem. Sophisticated and professionally organised gangs act with almost infinite geographical reach and frightening speed of execution. The returns are high and the chances of arrest are almost zero. Ransomware gangs develop and sell malicious software as a service to affiliates on the dark web, host data leak sites and manage ransom negotiations. Initial access brokers act as access lead generators. Attack techniques continue to evolve and so must your defences.

Cyber risk management is different to IT

Your IT people may be brilliant at their job. But assuming they are also cyber security experts with the up to date knowledge and experience to be responsible for advising on and implementing proper cyber risk management is the most basic error which can turn out to be fatal. That simply will not cut it, and it is the reason why so many businesses suffer a cyber breach.

It's not all about tech

The security and configuration of your technology is of course a big part of risk management. But there is much more involved in keeping safe. Your risk assessments come first. People and the activities they undertake are important. Provide training. Test it with simulated attacks. Governances should include the right policies and procedures for your business, with an ongoing programme to evaluate the measures in place. Security is not a one off MOT – it is a continuous process.

Operational resilience

The protection of confidential proprietary and client data is of crucial importance. But a lack of operational resilience can be more devastating. Few businesses recover from a successful ransomware attack within a few days, most remain crippled for weeks or months, wrecking their financial position. Few backups are correctly configured to survive an attack. Incident response and disaster recovery planning and rehearsal is needed so that the business can continue to provide services and function.

Comply with the law

Data protection legislation requirements include regular written risk assessments to enable clear visibility of risks and vulnerabilities relevant to the security of personal data; the determination and implementation of technical and organisational measures appropriate to control those risks (which must include people training, technical security and a governance regime); and the implementation of a process for regularly testing, assessing and evaluating the effectiveness of the measures you have in place. To understand just how widely the ICO interpret legal obligations, take a look at the cases of Tuckers (ICO fine £98,000) and Interserve (ICO fine £4.4m).

Regulatory compliance

All regulators of professional service businesses expect compliance with the law, as well as adherence to separate regulatory responsibilities including the duty to report breaches. Such obligations are not limited to personal data. In the case of a breach, expect the ICAEW or ICAS and the ICO to scrutenise amongst other things, the Code of Ethics.

Supply chain management

It's not just about you. You must consider your connected supply chain and how a breach could affect you or them. Who has access to your data or systems. Which organisations do you share them with. What are your critical supplier dependencies and what is your plan B if they go down. What checks and due diligence do you undertake to understand their security standards and back up arrangements, and do you have too many eggs in one basket.

The importance of independent assurance

Information that is business critical needs to be reliable. Good governance must include independent assurance carried out by genuine cyber security specialists with in-depth knowledge of the latest security risks and experience of the attacks taking place in your sector. They must be independent of your IT provider, because having your IT mark their own homework is a nonstarter from a risk management perspective. Your assurance should be in writing and intelligible to those who are not experts in cyber risk management, including those responsible at board level for managing the big risks in your business.

The role of certifications

A variety of certifications are available. Cyber Essentials Plus and ISO 27001 are best known, and can be useful as part of the risk management journey. They are sometimes necessary for contract tender purposes and can be helpful for marketing. But it would be quite wrong to assume they provide proper cyber security (they do not even satisfy data protection legislation). So reliance on either is misplaced.

The role of insurance - not a substitute for risk management

Insurance may be part of your risk management plan, but recognise its limitations - it is no more than the transfer of residual risk once you have taken the right steps to manage your cyber security in the first place. It will not prevent a breach, it will not satisfy your legal and regulatory compliance obligations and it can never repair all the damage to your reputation/business/finances.

Cyber Terms Explained

Welcome to the Cyber Security Explained section of our guide. No jargon, just clear explanations to help you understand some cyber basics. Whether you're new to cyber security or just need a quick refresher, this glossary will help you navigate the digital world.

Dark Web

The Dark Web is infamous for its illegal marketplaces, where drugs, weapons, and stolen data are frequently traded. It's a haven for cyber criminals. If your company's or client's confidential data is compromised in a ransomware attack, this is where the criminals will publish the data unless a substantial ransom is paid.

Email Account Takeover

Email Account Takeover (EAT) is the most common form of cyber attack and the consequences can be catastrophic. Criminals acquire your login details through phishing, dark web purchases, or password cracking algorithms. They then gain unauthorised access to your email account and once in control, they can:

- Monitor and intercept your messages.
- Initiate fraudulent transactions or send harmful emails.
- Steal sensitive information, like financial details or confidential client data, which can be used for blackmail.

Attackers frequently go unnoticed for months.

Multi Factor Authentication (MFA)

MFA is a security process that requires multiple forms of verification to access an account. Instead of relying solely on a password, MFA helps prevent unauthorised access and secures data by combining two or more factors, such as:

- Your password or PIN.
- A code sent to your phone or generated by an app.
- Biometrics like a fingerprint or facial recognition.

MFA makes it significantly harder (though not impossible) for hackers to gain access to your systems. MFA is often incorrectly configured and should be viewed as just one layer of a comprehensive defence strategy. Cyber criminals have found ways to bypass MFA, so it's crucial not to rely on it alone.

Phishing

Phishing is an extremely common type of cyber attack. It uses social engineering to trick individuals into revealing sensitive information. Attackers create fake emails or websites resembling legitimate ones, often creating a sense of urgency or fear to prompt quick actions without users verifying authenticity.

Clicking on spurious links can lead to:

- Confidential information being stolen – client data, passwords, etc.
- Malicious software (malware) infiltrating your systems.
- Unauthorised access to systems by collecting login credentials.

Phishing is a significant threat because it exploits human vulnerabilities rather than technical flaws, which makes it a favoured and effective method for cyber criminals.

Penetration Testing

Penetration testing (or pen testing) is a cyber security practice where experts simulate attacks on systems, networks or applications to find vulnerabilities that hackers could exploit. The goal is to identify and fix these security flaws before they cause harm.

Pen testing can play an important role as part of a comprehensive security strategy but should not be relied on in isolation. Only a full risk assessment can determine its role and effectiveness.

Ransomware

Ransomware is a type of malicious software (malware) that encrypts your files, devices and servers (and often backups), making them inaccessible until a ransom is paid. Whilst in your systems, criminals will also steal your data and threaten to release it onto the dark web. Ransom demands can run into millions.

Ransomware attacks often mean firms are unable to access their systems for weeks at a time. Full recovery can take months. The reputational and financial damage caused by these attacks can be devastating.

Busting Myths and Managing Risks

In today's digital landscape, understanding the true nature of cyber security threats is crucial for organisations to effectively recognise and respond to risks. However, myths and misconceptions can often cloud our understanding.

Let's debunk some common cyber security myths:

Myth 1: *"I am too small to be a target."*

Cyber criminals don't discriminate by company size. They exploit any vulnerabilities they find, regardless of how big or small the target is. Small businesses can be just as attractive for attackers, often because they may have less robust security measures in place.

Myth 2: *"My IT support has this covered."*

Cyber security and IT support are two separate disciplines. While IT handles functionality, cyber security encompasses risk management, policy development, and employee training, and much more. A comprehensive security strategy requires more than relying solely on IT.

Myth 3: *"Antivirus software makes me 100% safe."*

Antivirus software is just one layer of defence and does not by itself provide protection. It's essential to combine it with other security measures such as firewalls, regular updates, and monitoring. Make sure your antivirus software is centrally controlled and configured by a specialist for optimal effectiveness.

Myth 4: *"We are cloud-based, so we are secure."*

Cloud services are often targeted by cyber criminals. Although providers may implement strong security measures, it's your responsibility to secure your data, applications, and configurations through proper management and following security best practices. This includes conducting due diligence on the cloud provider's security arrangements.

Myth 5: *"We have cyber insurance."*

Cyber insurance can help mitigate financial losses from cyber incidents but doesn't prevent attacks or address all the issues arising from a breach. Effective cyber security practices are necessary to reduce the likelihood of an incident in the first place.

Myth 6: *"We have CE."*

Cyber Essentials (CE) improves basic cyber security but doesn't guarantee protection from successful cyber attacks. Sophisticated threats require a layered approach to security and expert guidance to address advanced and evolving risks that CE may not consider.

Myth 7: *"IT say we're secure."*

Without independent assurance, blind spots can go unnoticed, leaving the firm vulnerable to undetected threats. As we've already mentioned, IT and cyber risk management are different areas of expertise – and regardless, isn't it better to avoid having IT mark their own work? Get an independent expert to give a professional opinion on cyber security.

Myth 8: *"We've done pen testing."*

Penetration testing is great as part of an in-depth security strategy, but it is a point in time test, and will only reveal certain weaknesses and risks depending on the type and scope of testing. Thorough and regular vulnerability risk assessment provides a broader view of your security posture and helps uncover hidden threats that a pen test alone will miss.

Myth 9: *"Using a hosted service guarantees our security"*

Hosted services can manage infrastructure, systems, and applications for your organisation, but the responsibility for your data and its security still lies with your organisation. Ensuring managed services are properly protected needs to be considered and regularly reviewed to maintain appropriate overall security.

Myth 10: *"We have strong passwords, so we're safe."*

Strong passwords are important but they're not enough. Passwords can be cracked or stolen. Multi-factor authentication (MFA) adds an extra layer of protection, making it significantly harder for attackers to gain unauthorised access. When it comes to security, the more layers the better.

Awareness is the first line of defence against cyber threats. By understanding and addressing these myths, organisations can better protect themselves from the ever-evolving landscape of cyber risks.

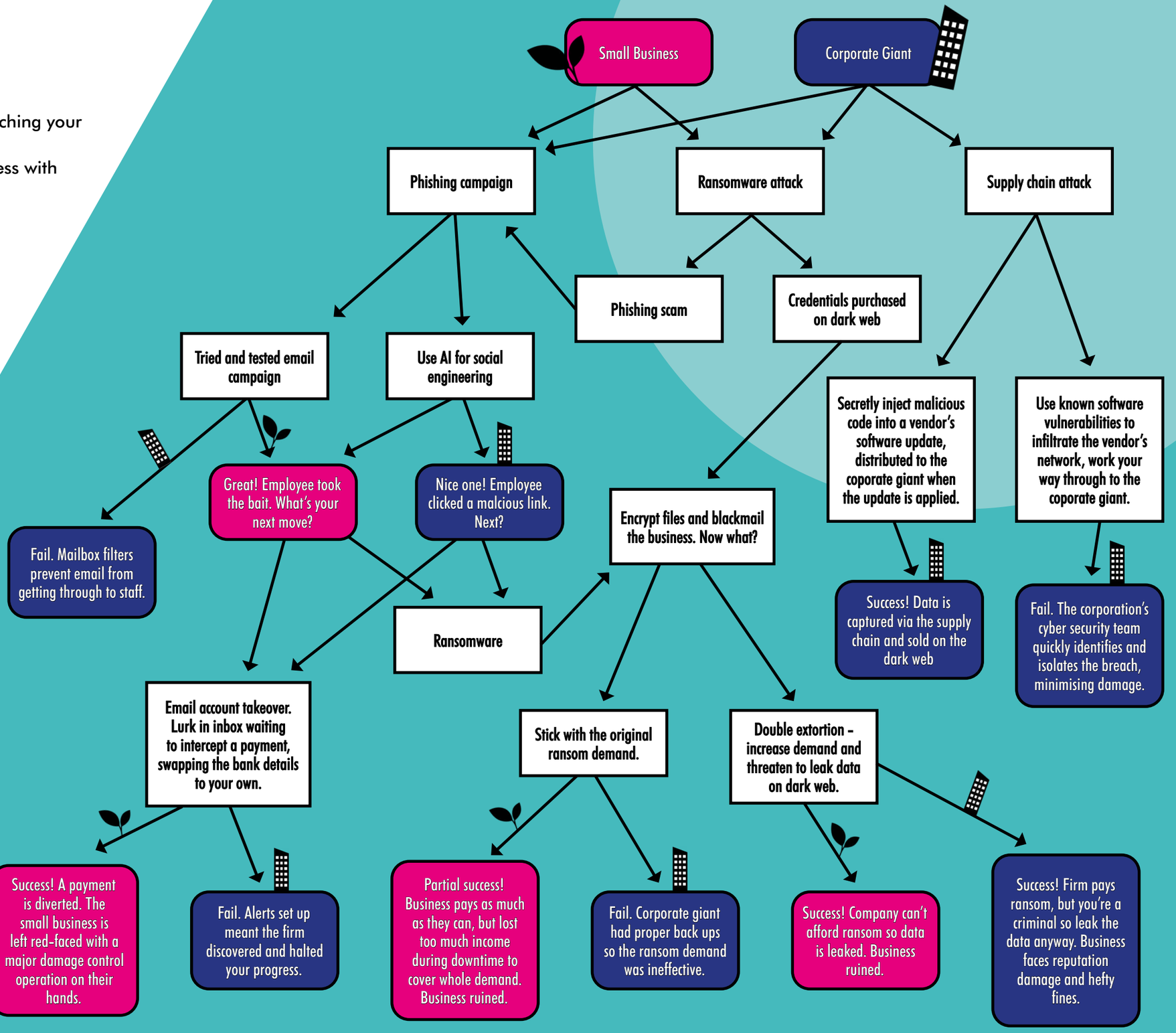
THE CYBER HEIST

You're a cyber criminal gang leader tasked with launching your next attack.
Cyber crime is an organised and sophisticated business with structured personnel.
At your disposal you have team leaders, malware developers, data miners and more.
The goal is to make the most amount of money, and not get caught.

To start, choose your target between:

Corporate Giant — Potentially harder to infiltrate, but the prize will be high.

Small Business — Easier to breach, but the payoff might be lower...



Disclaimer: Cyber crime is ever-changing and cyber security is complex. There are of course many more scenarios, access methods and outcomes.

Top 10 Tech Takeaways

Think of this as your starting cyber security checklist - ten very basic technical actions that every business, regardless of size, should prioritise. By addressing these key areas, you'll be taking significant steps towards securing your operations and safeguarding your future.
It's important to remember cyber risk management is not just all about tech though.

1 Web Browsing Controls

Fraudsters will often take unwitting staff to fraudulent websites. This risk can be minimised by correctly setting the controls in the browser, the AV and the operating systems.

2 Antivirus Software

Make sure it is centrally controlled, configured by a security specialist, kept up to date and on every device as a minimum.

3 Remote Authentication

When working remotely (VPN or RDP), username and password are not good enough protection for remote connection. Correctly configured MFA helps to stop a significant proportion of ransomware attacks.

4 Email Security Filters

Email platforms have filters that check incoming emails. Setting yours up correctly can help to protect employees from anything malicious.

5 Review Access Management

This relates to the documents, files, and folders that your system allows individuals to access. There is a generic setting of "Everyone" in many systems. Access to documents should be defined by role.

6 Test/Scan External Facing Assets

Tests and scans of firewalls, domain addresses, login pages and IP addresses will check for vulnerabilities and gaps in your security defences. You may not be scanning these, but the criminals are!

7 Security Patching

Software providers like Microsoft or Google issue regular software updates that patch (fix) known vulnerabilities. Criminals use bugs in software to compromise your defences and this is often used in ransomware attacks to get control.
75% of firms we assess have vital security patches missing.

8 Least Privilege

Ransom attackers take-over users' accounts and the more privileges that a user has, the more damage the attacker can do.

9 Alerting

The controls and administration of your IT systems have alerts that warn you something is not right. Configure these correctly and you have a chance of stopping a ransom attack in its tracks.

10 Back-ups

This is the process by which your business takes a copy of the systems, applications, and documents for use in an emergency.
Few back-ups survive a ransom attack, with everything ending up encrypted. Get yourself confident that yours would survive by getting independent assurance.

But it's so more than technology...

Cyber Risk Management is so much more than just focusing on technical requirements. It's crucial to consider the broader scope, including people and governance.

You can't effectively implement your controls until you've carried out a comprehensive risk assessment. This ensures that all potential vulnerabilities are identified and addressed.

Key areas to focus on include:

People

Your staff need to play their part in defending the organisation. And you must help them do so.

- Provide cyber awareness training.
- Test it is working with simulated attacks.
- Staff security handbook will set out the do's and don'ts.
- Create a security conscious culture where reporting issues is encouraged.

Governance

Put in place a management programme to identify and control your cyber risks and ensure operational resilience.

- Undertake formal risk assessments.
- Apply the right policies and procedures for your business.
- Include a process to assess the effectiveness of your controls.
- Plan incident response.
- Get independent assurance with board level oversight.

Regulatory Compliance

In the context of a cyber breach, expect scrutiny of your regulatory obligations, for example:

- Professional Competence and Due Care
- Client Confidentiality
- Compliance with relevant laws and regulation
- Industry Standards of good practice
- All guidance issued by ICAEW or ICAS, the ICO and NCSC.

CYBER ATTACK EMERGENCY?

Even if you just *suspect* you've been breached, seek specialist help immediately.

We can help.

24/7 Emergency Line:

020 8191 1048

Every second counts.

Do not email us as your email may have been compromised.

Gone Phishin'

Ready to test your phishing detection skills? In this "Spot the Phish" game, you'll practise identifying 10 common red flags of email scams. You're a new employee for Machin & Moore. See how many clues you can catch!

New Message

From: Machin&More1@gmail.com [EXTERNAL]

Subject URGENT: Immediate action required

Dear New Team Member,

I need you to urgently place an order for some important equipment that a key client requested. This is critical to maintaining our ralationship with them.

Please use the link below to complete within **48 hours**.

Click here

Make sure to include your full name, address, and phone number. once you've completed this, confirm with me directly.

Sincerely,
Robert Moore, CEO

Sent from iPhone

Reply Forward

1 _____

2 _____

3 _____

4 _____

5 _____

6 _____

7 _____

8 _____

9 _____

10 _____

ANSWERS

1. Email domain spelt wrong
2. From a Gmail account
3. [EXTERNAL] email
4. Sense of ugency
5. Doesn't personally address recipient
6. 'Relationship' is spelt wrong
7. Asking to click on a link
8. Requesting sensitive data /personal information
9. Poor grammar (Once isn't capitalised)
10. "Sent from iPhone"

MITIGO

CYBERSECURITY

If you've not suffered a serious breach, it may be hard to understand just how frightening and how devastating it is. But a cyber hit will stop you working, wreck your reputation, and may destroy your business.

Cyber protection is not the job of IT support, it requires specialist help (and insurance won't prevent a breach).

Services include:

- Technology vulnerability assessments
- Penetration testing
- Training and simulated phishing
- Cyber policies and governance
- Emergency cyber breach response
- All cyber certifications

Mitigo offers ICAEW members 10% discount and a free cyber security assessment to help you understand the areas of your business that are most vulnerable to attack.

If you think cyber security is expensive, try having a breach.

Trust Mitigo.

mitigogroup.com
0208 191 0936
icaew@mitigogroup.com

MITIGO
CYBERSECURITY

mitigogroup.com

0208 191 0936

icaew@mitigogroup.com

icas Partner 2024

ICAEW
MEMBER REWARDS
PARTNER