"It's Not a Matter of If, But When..."

The Small to Mid-Size Business' Guide to Cyber Security

cmi The business IT experts

Introduction

The State of Cyber Security

Regularly ranked as the number one concern across all UK businesses, cyber security is no stranger to company owners and leaders. You're undoubtedly familiar with the threat of malware, the devastating effects of ransomware, and the importance of tight web and email security.

Yet knowledge is only half the battle.
The Cyber Threat is evolving - and it will continue to do so.

While UK businesses are more aware than ever of how crucial cyber security is, the modern workplace moves at a blistering pace. Just how up to speed is the average UK business with their technologies, strategies and vulnerabilities?

Nearly four in ten businesses (39%) and **over a quarter of charities (26%)** suffered a security breach in between 2020 and 2021.	**65% of medium businesses, 64% of large businesses** and **51% of high-income charities** were affected in that same period.
Less than half of all UK businesses have taken out cyber insurance, undertaken risk assessments or tested staff security awareness since 2020.	**Less than one third of business (31%) and charities (27%)** have a cybersecurity business continuity plan in 2021.
Since the pandemic and the rise of home working, **less than a quarter (23%) of all businesses and charities** have implemented secure home working policies.	**1/3 of businesses (35%)** report being negatively impacted, requiring new post-breach measures, staff time diverted or wide business disruption following a breach or attack.

***Source: UK Cyber Security Breaches Survey 2021**

The statistics, while less than ideal, aren't entirely surprising. A global pandemic, and the subsequent worldwide adoption of Cloud services, has shifted our technical landscape dramatically - and left businesses little time to review their security standards.

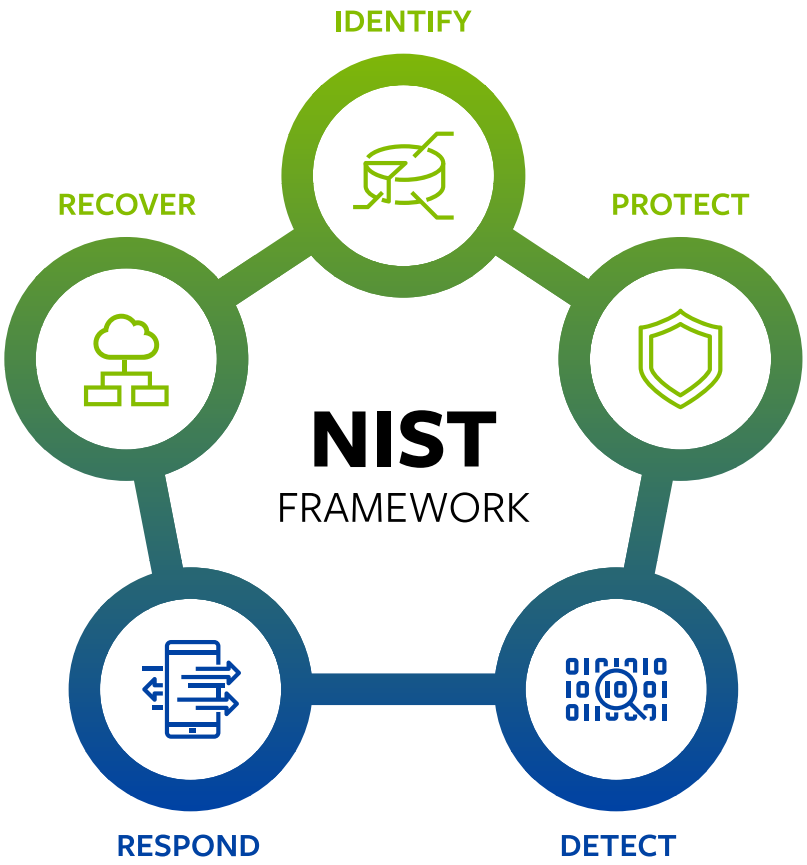
As such, there's never been a more crucial time to review your cyber security – and while it may seem overwhelming, you don't have to tackle it alone. By the end of this eBook, you'll better understand your options for better business security, as well as how CMI helps perfect your business protections.

In this eBook, you'll learn:

- The 5 Stages and 7 Layers of a cyber security strategy
- How to build an effective response plan
- Protecting your business in a Cloud-enabled workspace
- What to look for in a Cyber-Insurance policy
- The importance of staff training in any cyber security plan

5 Stages, 7 Layers: The Frameworks to Your Security Strategy

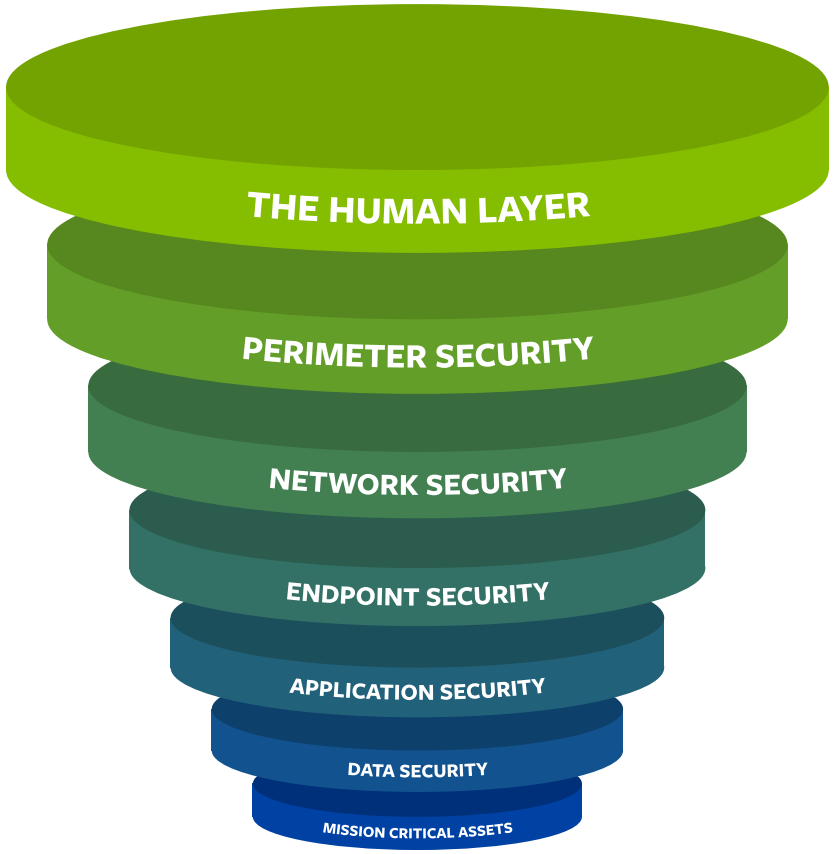
At CMI, we adopt two renowned methods for your cyber security - the NIST (National Institute of Standards and Technology) Framework and the 7 Layers. These common methods are among the most effective, covering your people, your processes and technologies respectively:



NIST is a framework detailing your planning and response to potential threats. On a basic level, this can be broken down into the following:

- **Identify** details the risks to your people, systems, assets, data and capabilties, now and in future.
- **Protect** outlines your defensive safeguards and techniques for ensuring full defence and continuity.
- **Detect** details your methods for monitoring and identifying threats, and raising continual awareness around them.
- **Respond** defines your approach before and after an event, including communicative, analytical and mitigating responses.
- **Recover** identifies your recovery processes, the development of your incident response strategy and event logging procedures.

5 Stages, 7 Layers: The Frameworks to Your Security Strategy



The 7 Layers details the multiple protective barriers of your cyber security, each as crucial as the last and spanning your entire system journey.

- **The Human Layer** is the first barrier, comprising your users' knowledge and awareness of threats.
- **Perimeter Security** comprises hardware and software protections that protect the business overall.
- **Network Security** details the surveillance and security of network traffic.
- **Endpoint Security** protects the connection between your network and its associated devices.
- **Application Security** protects the access and internal security of your business applications.
- **Data Security** controls the safe access, storage and transfer of data.
- **Mission Critical Assets** are integral data that need ultimate protection.

Throughout this eBook, we'll explore the threats to your business security, expand upon the NIST framework and explain how these steps help you respond to incoming threats - unknown or otherwise.

The Key Stages of Cyber Security

STAGE 1: IDENTIFY

Identifying isn't only about knowing your business threats; it's about knowing your role in cyber security. Allocating roles for any cyber security incident, developing a cyber security Incident Response Team (CSIRT) and raising the right alerts are all part of the Identify process.

Of course, it helps to start on the ground level. As part of The Human Layer, how familiar are your users with threats such as:

- **Drive-by downloads?**
- **Phishing / Whaling?**
- **Spear-phishing / Spear-phishing via service?**
- **MITM (man in the middle) attacks?**
- **Removable media?**
- **Supply chain compromise?**
- **Social Engineering?**
- **And many, many others?**

The Human Layer is your first and arguably most crucial security barrier against these threats. It's also, unfortunately, the most regularly underdeveloped.

Though phishing emails are one of the earliest, crudest methods of infiltration, they prey on unaware users and – thanks to the volume of your average phishing scheme – are often successful enough to work. It only takes one unwitting recipient to let malicious files into a network, after all.

The **Identify** stage is also about the quick and efficient improvement of your protections. You'll note that the NIST process is circular; not only because the threat cycle is never-ending, but because after a successful **recovery**, you'll immediately return to the identify phase to assess the threat, scope and impact of any breaches you've suffered or prevented.

YOUR CYBER PROTECTION CHECKLIST:

- **Regular Security Awareness Training**, which helps users spot and deter intruders at the point of entry, keeps users updated on evolving cyber-crime techniques, and helps users identify their role in protecting against data breaches
- **Vulnerability Assessments**, which identify exploitable areas of entry on your network, highlight any gaps in your human or technical defences, and help you prioritise your next security improvements.
- **Risk management plans**, which establish your priorities, weaknesses, points of contact and procedures before, during and after an incident.

The Key Stages of Cyber Security

STAGE 2: PROTECT

Once you're familiar with the risks uncovered during the Identify Phase, the Protect phase helps you evaluate your protections, and implement the appropriate strategies and technologies.

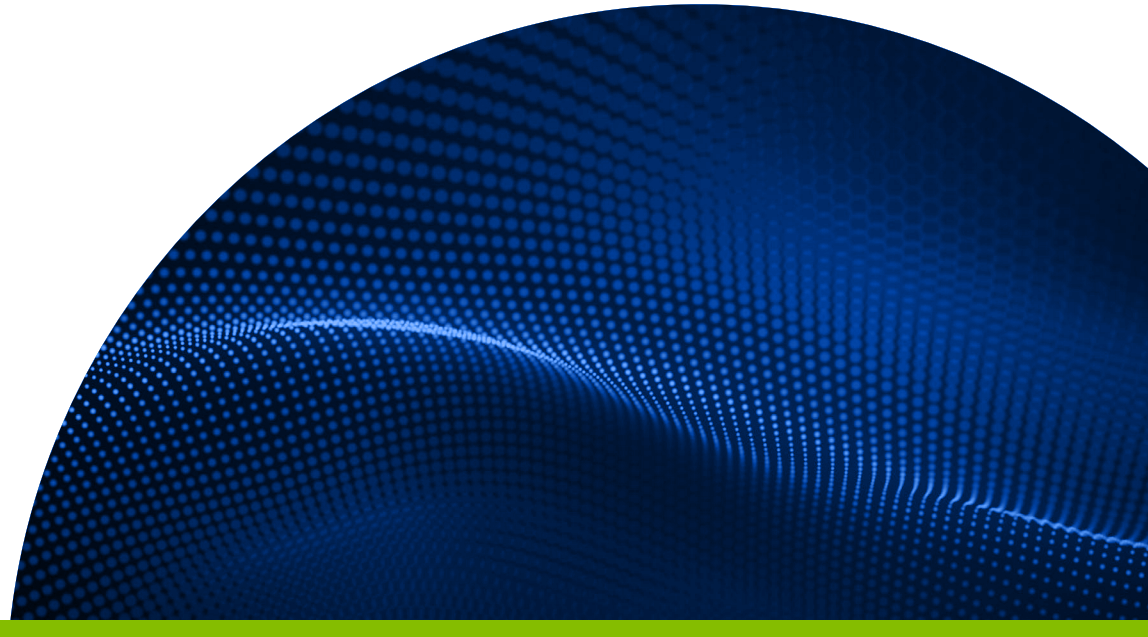
These will include:

- **Ongoing Training and Awareness**
  keeping your teams engaged, aware and in accordance with your compliance requirements.
- **Information Protection Procedures**
  including how your business secures data at rest and during an incident.
- **Maintenance**
  including regular upkeep, logging and repairs to keep systems in line with your protective policies.
- **Data Security**
  with a fully risk-assessed strategy that keeps personal, operational and confidential data fully protected.
- **Technologies**
  the all-important tools of the trade, these comprise your technical defences and solutions.
- **Access Control**
  which outlines access privileges for each and every user on your network.

Protecting incorporates a multitude of technical solutions which we'll cover shortly, including firewalls, conditional access and advanced endpoint protection. However, there's still unautomated work to be done; the risk management plans and training outlined in the identity phase are ongoing, requiring regular reviews and technical upkeep. A **Security Operations Centre (SOC)** can simplify this process.

You should also adopt a **Zero-Trust** security approach. This strategic philosophy treats all network connections as suspicious, with data traffic needing to pass strict and stringent security checks at every stage of your 7-layer security setup. It's drastic, but equally effective at keeping you protected.

The **Protect** stage is a broad one, covering all **7 Layers of your Cyber Security** - but it isn't conclusive, and you'll continue strengthening those 7 layers over the remaining three stages of NIST.



The Key Stages of Cyber Security

CYBER INSURANCE

You're not just protecting your data with a Cyber Security strategy. You're protecting the whole business.

When sensitive data is at stake, a breach could incur the following severe costs:

- Business interruption in the form of revenue loss
- Legal fees
- Reputational damage
- Data Restoration Costs
- Mandatory Notification Costs

Without being able to demonstrate appropriate cyber resilience, you could suffer more than financial and operational losses; not least when 60 percent of smaller enterprises are forced to close within 6 months of a debilitating attack. That's why an accredited, government-approved security assessment, such as Cyber Essentials Plus, is instrumental to demonstrating your specific security provisions and having your Cyber Insurance policy pay out.

Are you protected by Cyber Insurance?
If you've not reviewed yours recently, you might not be maintaining the mandated requirements – invalidating your policy. Talk to CMI today about your Cyber Insurance policy requirements

YOUR CYBER PROTECTION CHECKLIST:

- **Advanced endpoint protections** that help keep phishing emails and malware away from your systems.
- **A Security Operations Centre**, offering early detection and response to incoming threats before an incident can occur, with 24x7 eyes on your systems.
- **Zero-Trust Security**, for the most concise protection against malicious, unrecognised or unknown network traffic.
- **Firewalls**, to protect user connections to the internet.
- **Virtual Private Networks**, to encrypt network traffic for off-site users and remote workers.
- **Cyber Insurance**, to lessen the reputational, financial and legislative impacts of a breach.

The Key Stages of Cyber Security

STAGE 3: DETECT

The **Detect** phase is an ongoing and responsive one. In the event of a threat, it should not only identify anomalies on your network but track them, identify them where possible and keep relevant parties informed.

Detect the Threat,
inform the relevant parties
and begin the respond phase.

Monitor the Threat,
including any anomalous effects
on sensitive data or systems.

Maintain your detection processes,
to ensure yours are updated and anticipating
new or unknown threats.

During this stage, consider your GDPR responsibilities too. If any compromised personal data is identified, it MUST be reported to the Information Commissioner's Office (ICO) within 72 hours.

The Key Stages of Cyber Security

FOR YOUR DETECT PHASE, CONSIDER A SOC SOLUTION

A SOC is your all-seeing eye on your network traffic, offering early detection and response to incoming threats before an incident can occur.

At CMI, our SOC solution incorporates:

Next-Gen Malware & Ransomware Protection

Spot malicious files in transit and stop them from ever slipping through the cracks.

Network, Endpoint and M365 Monitoring

Log monitoring with 1 year storage protection.

Intrusion Monitoring and Breach Detection

Real-time threat detection, identifying suspicious activity in process and preventing catastrophic breaches.

Incident Response and Remediation

Identify, resolve and repair the damage following a security incident.

Threat Intelligence

Ever-evolving analytics on your threats, weaknesses and security inhibitors, with support for new and emerging threats'

Continuous Security Monitoring

24/7 security, 365 days a year across your cloud, your network and your endpoints. There's never a chance to let your guard down.

The Key Stages of Cyber Security

STAGE 4: RESPOND

How quickly can your business react to a cyber breach, phishing attempt, or a successful social engineering scam? The Respond phase helps you to estimate, then optimise your response times.

Responding to cyber threats quickly is essential – not least when you consider the high cost of downtime to the small to medium business in the UK:

ON AVERAGE:

The Average revenue cost of downtime is estimated to be:

£2.1 million
per hour

*(IBM Global Services)

Compounding this, 47% of mid-sized British Businesses estimated losses of:

£77,000
per hour in productivity

*(ITC Reliability and Hourly cost of Downtime Trends Survey)

These lost revenues are stated as the top business challenges of downtime by:

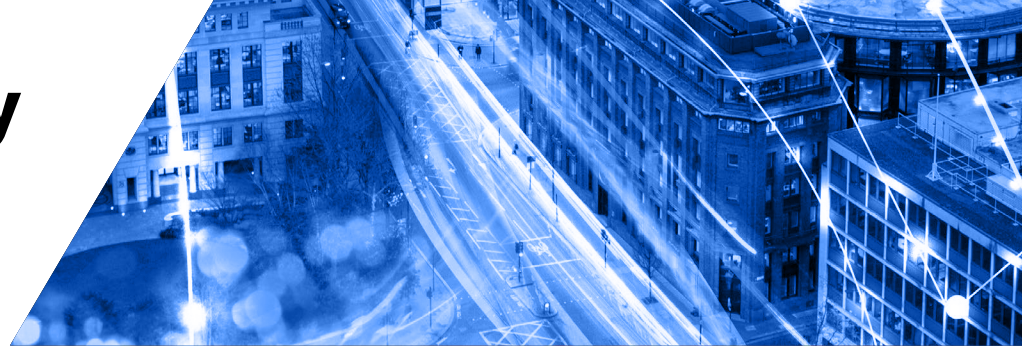
53%
of British businesses

*(IBM Global Services)

Reacting to a data disaster is equal parts technology and procedure.

Your recovery plan should ensure that your teams respond responsibly to any incidents, your every affected technology is accounted for, and you're able to transition quickly into your Recover stage following the response.

The Key Stages of Cyber Security



Below is a simple breakdown of the CMI response plan, which we use to assist clients in the event of any cyber incidents.

THIS RESPONSE PLAN SHOULD COVER:

1. **Preparation for the event**

   Step one is to identify your Cyber Security Incident Response Team (CSIRT). All employees must report any suspected or confirmed data breach or other cyber incident to their managers, appropriate personnel and SOC.

2. **Identification and Assessment**

   Conduct a vital assessment to confirm an incident or eliminate any false positives. Determine the scope, impact and extent of any potential or subsequent damage and try to preserve digital evidence for potential review – either by third parties or as part of your legal requirements, such as GDPR.

3. **Control and Containment**

   This stage, more than any other, requires an open channel with all stakeholders as events can unfold rapidly. Make notes, as these will help influence your future detection processes. Steps must then be taken to prevent damage to other systems or resources.

4. **Removal of Effected Systems**

   The affected systems will most likely need to be removed or isolated for the rest of the network. All other symptoms should be noted, addressed and confirmed to no longer be affecting the rest of the service or systems. A focus on looking for secondary compromises that may have been installed will also be addressed.

5. **System and Service Recovery**

   This stage requires various steps needed to bring the system or service back to a working and healthy state. This may be restoring from a previous backup (after confirming the backup works in isolation) or may require the client's disaster recovery process to be invoked. Once completed, the incident should be declared as resolved and communicated as such.

6. **Root Cause Analysis**

   Post incident, business should detail their findings and, if possible, declare the root cause analysis (RCA) of the incident. In some instances, a specialised third party will be required to review the evidence of this RCA and following the incident, users should provide future guidance and identify areas of concern going forward.

The Key Stages of Cyber Security

STAGE 5: RECOVER

Recovery is for everything after an incident, be that recouping data, reinstating any compromised solutions, returning to operational capacity and beyond.

The **Recover** phase may occur after a major event, but it is arguably the most crucial stage of your response: time lost in this stage affects your services, bottom line, resources and reputation.

It's important that your recovery stage is thoroughly tried and tested, as this is often the best way of estimating an accurate recovery time.

This is only a fraction of what your **Recovery** strategy should entail.
A well-planned recovery strategy keeps your business operational, your people safe and your cyber defences improving. Though it often occurs after the dust has settled, one should never discount the importance of the Recovery phase.

Thankfully, recovery options are designed for fast, full correction of any data disasters, and are essential in any recovery process.

YOUR CYBER PROTECTION CHECKLIST:

- **Data Backup**, which regularly stores copies of your work, files and apps throughout the day, ready to recall should they be compromised.
- **Disaster Recovery**, ensuring you're able to get your people and processes up and running in the face of a technical disaster.

YOUR RECOVERY STRATEGY SHOULD COVER:

- **Your GDPR responsibilities,** including the recouping of any lost data discovered in the Identify stage.
- **Staff responsibilities** leading up to, during and after any recovery procedure.
- **Strategies, gap analyses,** recovery options and technical requirements.
- **Orientation exercises,** learning and training around your recovery strategy.
- **Client-specific requirements,** including safety precautions before and after sensitive data breaches.
- **Your Recovery Point Objective:** The maximum data loss your business can endure before drastic repercussions.
- **Documentation of incident response plans,** including manual workarounds.
- **Your Recovery Time Objective:** The length of time your business has to restore essential processes before drastic losses.
- **Cyber Insurance details,** policies and liabilities.

The Security Concerns of the Modern Workplace

Your workplace has changed. So too have your technologies, your day-to-day work and the way you communicate with users. It only makes sense that your security should reflect these changes.

THE CLOUD

The Cloud has delivered many business benefits worldwide, not least the ability to work remotely, effectively, and efficiently.

Yet with these benefits come responsibilities. How do you protect your people, data and devices when they're so much more mobilised? How do you maintain security and compliance when users are connected to numerous external networks from a range of compatible devices?

When reviewing your Cloud security, ask yourself:

- Are your SaaS solutions, such as Office 365, protected from infiltration or data loss?
- Is any work not saved to your company devices supported by regular Cloud backups?
- Are users accessing your network protected behind a Virtual Private Network?
- Is Endpoint Security standardised across all remote devices and users?

It's important not to assume any typical business security is offered by default when working in the Cloud: remember that Microsoft has no obligation to backup anything you save to its servers.

GDPR

It's by no means new – nor especially business friendly – but the UK's exit from the EU hasn't shaken the shackles of the GDPR. Couple this with the transformative arrival of the Cloud-connected workplace, and your GDPR concerns are no less prevalent.

Remember that failing to report and respond adequately to a data breach can carry catastrophic consequences under GDPR, with fines of up to £17.5 million or 4% of annual global turnover – whichever is greater.

YOUR GDPR RESPONSIBILITIES:

- **Data Processing Principles**
- **Lawfulness of processing**
- **Conditions for consent**
- **Processing of special categories of data**
- **Data Subjects Rights**
- **Data transfers to third countries or data organisations**

YOUR IT SECURITY

At CMI, we assess your security across several crucial categories, each just as relevant to the Modern Workplace as they were to years prior. With our assistance, you'll be able to strategize and maintain your:

- **Physical Security**– Including access to server rooms, hardware and all on-prem devices.
- **Identity** – Including securing accounts, verifying users at login and protecting credentials behind a robust authentication policy.
- **Endpoint Devices** – Standardising devices, building secure BYOD policies, encrypting hard drives and implementing mobile device management.
- **Malware and Threat Detection** – Providing regular threat scans, 24x7x365 threat monitoring and web content filtering.
- **Internet Protection** – with firewalls, email authentication and regular vulnerability testing.
- **Patch Management** – Managing software upgrades centrally, updating unsupported software and keeping hardware operational with firmware upgrades.
- **Certification and Compliance** – Including Cyber Essentials Plus accreditations, regular onsite training and adherence to ISO-27001 or equivalent standards.
- **Backup & Recovery** – Including scheduled backups, a documented recovery strategy and full testing of your backup timeframes.

Conclusion

The Modern Workplace has transformed the way we work, and the way we manage our businesses. It has also made cyber crime more prevalent and more determined than ever.

Whether it's sensitive data, GDPR fines or your organisation's reputation, an ill-prepared business has too much to lose to enter the Modern Workplace unprotected. Yet by embracing your technical future – not fearing it – your business is arguably more prepared than ever to combat the cyber threat.

By prioritising your cyber security today, you're securing your business for tomorrow – and on a far greater scale than ever before.

HOW CAN CMI HELP?

With 25 years' experience serving businesses from our London, Thames Valley and Belfast offices, CMI are leaders in IT Infrastructure Planning, Implementation and Support.

Recognised among the World's Most Elite Managed Service Providers by the MSP501 and accredited by such regulators and providers as **Microsoft, Mimecast and ISO9001 & 27001**, we deliver complete security compliance and product knowledge to our partners' high service standards.

OUR CYBER SECURITY SERVICES INCLUDE:

- **Backup and Disaster Recovery**
- **Vulnerability Assessments**
- **Risk and Compliance Assessment**
- **Cyber Security Training**
- **24/7 Detect and Respond**
- **Managed Cyber Security and Zero Trust Security**

Why not book a FREE Cyber Security Consultation now and receive impartial advice on the solutions best suited to your business.

Book a Cyber Security Consultation today, including:

1. 47-point IT Security Risk Assessment
2. Dark Web Credential Theft Scan
3. External vulnerability scan
4. Simulated Email Phishing attack

Contact CMI

Belfast / London / Thames Valley

0800 023 2696

hellocmi@newcmi.com

cmi The business IT experts