CYBER SECURITY
Helping you protect your business
The evolution of technology during the last decade, particularly during recent years, has provided the opportunity for organisations and financial institutions to adopt more digitalised environments both for client services and to support new, redesigned internal processes. In this increasingly sophisticated and complex technological environment, new security challenges are constantly arising, making it harder to protect valuable intellectual property and business information in digital form against theft and misuse.

Companies must be prepared to fend off external attacks (hackers, hacktivists and nation sponsored attacks) as well as internal attacks (such as disgruntled employees).

Seemingly every day, a major new cyber security breach occurs, even at large, well-protected companies and we have seen a number of high-profile breaches splashed across the media. Cyber attacks have far-reaching economic consequences for organisations; beyond financial, reputational and legal ramifications. No industry is immune. Being breached is becoming the new ‘normal’ for many institutions.

As these breaches continue, cyber security has become one of the largest concerns for investors, boards and audit committees.

Technology-related risks from both external sources and from within the company must be understood and effectively managed if they are to succeed in our ever more technology-centric world.
Cyber security starts with the board

Today, business relies on information assets produced by increasingly sophisticated systems and technology from various sources.

In this more complex ‘cyber-world’, investors and regulators call for more transparency relating to boards’ oversight of cyber risks. Boards need to appreciate the key issues around cyber security and adopt best-practice approaches not only for cyber risk management but also for the purposes of disclosure.

An increasing number of board and audit committee members are starting to consider cyber security risks as part of the Enterprise-wide Risk Management (ERM) process. Yet, in some organisations, the management and oversight functions regard cyber risk as nothing more than just an IT issue.

Numerous surveys quote cyber risks amongst boards’ top risks; however the level of understanding of the implications of these risks to their organisation - reputational, legal and supply chain risks - is not necessarily sufficient.

HOW CAN MAZARS HELP?

Mazars’ cyber security experts provide comprehensive training to boards and audit committee members tailored to an organisations maturity in order to:

• Improve understanding of the latest cyber threats that can impact their organisation
• Increase their understanding of the roles and responsibilities of the board and audit committee regarding cyber security
• Provide the board with access to cyber security expertise to facilitate discussion related to cyber risk management
• Help develop a plan to assess their cyber security posture and then help to define the target state for cyber security
Cyber risks assessments and programme review

Cyber risks should be integrated as part of the on-going ERM process, information security strategy, business continuity plan and supply chain management. Although, organisations and financial institutions tend to include cyber risks in these plans and strategies, they do not necessarily align their cyber programme to the business risks with the objective of resilience. A strategy towards resilience ensures that information assets are adequately protected and makes sure that security investments are properly targeted and that they provide the expected benefits.

Mazars helps organisations and financial institutions to assess their cyber security programmes and their cyber resilience using a proprietary tool which integrates a bespoke approach, best practice and requirements from several jurisdictions.

Our four step approach:
1. Review of the inherent risk profile related to the organisation, technology, delivery channel and external environment
2. Determination of the organisation/institution cyber security maturity level addressing the following five functions: identify, protect, detect, respond and recover
3. Assessment of the critical controls
4. Proposition of pragmatic road map to achieve desired maturity level

Regulators across the world are pushing for more cyber security capabilities for critical infrastructures such as financial institutions, energy and utility companies, (e.g. EU NIS Directive early 2016). Organisations need to elevate their cyber security posture and look beyond compliance.
An organisation’s cyber security is only as strong as its weakest link.

In recent years, the weakest link has more often than not been the supplier(s). The credit card fraud case suffered by American retailer Target, demonstrates how easily a multi billion company with weak IT security procedures can be placed at risk by their supplier; in that case an air conditioning company. Over the past decade outsourcing, providing sensitive information and giving access to IT assets to external parties has become increasingly common. Organisations should assess and rank their suppliers and the partners who are authorised to access the company’s network or IT assets, or retain copies of company owned data, according to the potential risk to information security.

In practice, this exercise has been very difficult due to lack of an objective measurement of the supplier’s security posture. Each department involved in the supply chain from legal, to sourcing and information security, should work together to develop a common security program that will offer the required coverage of the information risk. Both the frequency of the security assessment and the effort taken to assess should be proportionate to the risk.

In order to build a trust in the supply chain, a risk-based, transparent and agile approach to IT security should be embraced by all stakeholders.

**Key steps to information security**

1. Create inventory of IT assets with their location
2. Rank the vendor / partner risk
3. Incorporate IT security requirements and assurance in the agreements
4. Train and educate vendors
5. Test and monitor vendor’s IT security programmes
6. Survey the vendor / partner regarding its information security

**Stakeholders:**

vendors, partners, legal, sourcing/purchasing, IT, compliance
Have you moved to the Cloud? Are you aware of potential risks and benefits?

Cloud computing is becoming the new Eldorado for business leaders as they seek to move toward faster systems of engagement using customer centric systems. This trend is further reinforced by companies wanting to reduce their technology costs and risk exposure by adopting a “cloud first” policy (as adopted by UK government in 2011). Cloud is seen as a good means to outsource continuity risks, the objectives being both zero downtime and obtaining a secure environment with cost benefits.

However, while some of the risks are being attenuated, new risks are arising. Security policies and controls are not systematically enforced in this new environment, putting sensitive customer information at risk. Every day employees violate corporate data security policies by using public cloud applications which expose organisations to the risk of data breaches and non-compliance. Cloud providers are typically lacking in transparency when it comes to performance, security and data ownership and recovery. And finally, organisations do not necessarily adapt their incident response plans to take into consideration this complicated environment where the business impact could be unanticipated.

HOW CAN MAZARS HELP?

Mazars can assist you in ensuring your transition to a Cloud based IT ecosystem will not be to the detriment of cyber security and will not put the organisation at risk.

Our solution includes:

• Assisting during the selection process under “cloud first” policy
• Assessing the risk carried by the contract signed with the Cloud providers, from both a business and cyber security point of view
• Analysing and developing policy and procedures
• Providing independent assessment of the cloud provider security to ensure alignment with recognised standards and best practices such as ISO 27001, NIST and CSA CCM
• Assessing privacy through impact analysis and regulatory requirement gap analysis
Cyber Essentials and Cyber Essential Plus

With increasing cyber threats and the significant number of cyber breaches during the last few years, the UK government and security not-for-profit organisation 'Cyber Streetwise' have issued guidance on how organisations can protect themselves in cyberspace.

Cyber Essentials and Cyber Essentials Plus

Since October 2014, companies need to be compliant with Cyber Essential controls if bidding for government contracts involving sensitive and/or personal information. This scheme was developed to encourage small and mid-size organisations to adhere to good practices regarding information security. While Cyber Essentials offers a foundation level, Cyber Essentials Plus offers a higher level of assurance around five areas:

1. Boundary firewalls and internet gateway
2. Secure configuration
3. User access control
4. Malware protection
5. Patch management

IASME Gold certification

The IASME standard (first published in 2015 and revised in May 2015) was created to achieve a cyber security standard for small and medium sized companies. This standard was built along the same lines as ISO27001 and NIST 800. The Gold standard of IASME demonstrates baseline compliance with ISO27001. This standard complements the Cyber Essentials domain with risk management, governance, training, procedures, incident management and business continuity aspects. A certified IASME Gold organisation will also receive the Cyber Essentials certification. IASME is a realistic and affordable way for small and medium sized companies to prove that they are adopting information security best practice.

HOW CAN MAZARS HELP?

Mazars’ cyber security experts help organisations to successfully pass the IASME Gold certification, Cyber Essentials (CE) and Cyber Essentials Plus (CE+) certification.

Mazars assistance can be broken down into two services:

- **READINESS:** using the same methodology and framework as used during the examination, we will assess the organisation’s cyber security not only around the key five domains of CE and CE+ but also against best practices. We will issue a comprehensive report including pragmatic recommendations to pass the certification and also offer additional recommendations for ‘best in class’ cyber security.

- **CERTIFICATION:** as an authorised assessor for IASME, CE and CE+, Mazars will certify that the organisation is compliant with the requirements.
Would your organisation be resilient against a cyber breach?

Recently in the US, the US Federal Communication Commission (FCC) fined telecoms and television provider Cox Communications for not taking data security seriously and for lacking a cyber incident response plan. Common thinking is moving from “if” the organisation will suffer a cyber breach to “when” it will be breached.

Preparation and planning is more critical than ever before. In a breach situation speed is essential. Organisations need to be well prepared to react quickly in order to limit potential damage, not only in financial terms but also in potential loss of reputation. Shortfalls exist in most incident-response plans.

Organisations should implement and maintain a cyber security incident plan in order to limit damage, increase the confidence of external stakeholders including investors, clients and regulators, and reduce recovery time and costs.

**HOW CAN MAZARS HELP?**

Mazars helps organisations to prepare for a security breach by:

- Independently assessing readiness for cyber breach through penetration testing, policy, procedure and control review
- Assisting in the development and implementation of an incident response plan
- Assistance during the testing phase of the plan
Why Mazars?

1. **Expertise and knowledge** Mazars provides clients with access to best-in-class people and innovative cyber security consulting services to enable organisations to better execute their business strategies.

2. **Highly qualified** The team includes experienced professionals who carry professional, vendor neutral, certifications such as CISSP, GPEN, CISA, CRISC, CISM, ISO 27001, CEH with backgrounds in technology, engineering and computer sciences.

3. **International reach** The UK Cyber Security team is part of the Mazars global Cyber Security Group encompassing excellence centres around the world.

4. **Strength and depth** A team with experience in dealing with complex environment and projects.

5. **Senior and experienced engagement team** Substantive involvement of Partners and Senior Managers.

6. **Tailored approach** We devise a bespoke service approach for each client.

7. **Solutions orientated** Provide realistic and pragmatic solution.

8. **Value driven** Highest quality of service at a fair price.

9. **Responsive and accessible** Client responsiveness is our highest priority.
Meet the experts

Nicolas Quairel, Partner and Head of Cyber Security UK

Nicolas Quairel leads Mazars’ Cyber Security practice UK. With more than 15 years of experience with Mazars Group in France, in the US and in the UK, he has experience providing IT advisory services across various industries. He has worked with global, commercial and investment banks, insurance companies, retail and manufacturing groups to deliver a wide range of IT security related services. Nicolas’ experience includes cyber security program development and review, IT risk assessment, architecture review, penetration testing, defence, in depth implementations and assessment reviews, he is a Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA) and is Certified in Risk and Information System Control (CRISC).

Francisco Sanches, Senior Manager, Cyber Security

Francisco Sanches is a Cyber Security Senior Manager that has been working within information security and IT audit for over 14 years. He is a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM) and a Certified Information Systems Auditor (CISA).

Francisco has been responsible for IT security related projects of audit, advisory and consulting in the financial services, telecommunication and utilities industries, working for major players in UK, Portugal, Angola and Cape Verde. Francisco’s experience includes design and implementation of security frameworks in alignment with ISO 27001, various security audits, penetration testing, data privacy audits and business continuity / disaster recovery plan development and review.
Please get in touch...

For more information please contact:

**Nicolas Quairel**
Partner
- **T:** +44 (0)20 7063 4965
- **M:** +44 (0)7469 034 238
- **E:** nicolas.quairel@mazars.co.uk

**Francisco Sanches**
Senior Manager
- **T:** +44 (0)20 7063 4871
- **M:** +44 (0)7920 535 238
- **E:** francisco.sanches@mazars.co.uk