INFORMATION SECURITY

Services to support and protect your organisation

MAZARS

In todays connected IT environment, small and medium size organisations are being targeted by ‘threat actors’ such as hackers, hacktivists and criminals because they typically lack the security defences, resources, time to support and expertise to effectively protect their information assets. The confidentiality, integrity and availability of data which resides on their applications, systems and networks is therefore at significant risk of being compromised.

Financial institutions, in particular, are facing an increasing number of challenges on multiple fronts in a fiercely competitive and rapidly changing industry. Increased global regulatory oversight and scrutiny have increased requirements for security, compliance and transparency. Customers expect financial institutions to be able to protect their data from being compromised by both external and internal parties.

Vulnerability assessment and penetration testing

Our information security specialists can provide ethical penetration tests of computer systems, networks and websites, employing a variety of tools and techniques, either from inside or outside your organisation. In addition to these comprehensive vulnerability assessments, we can identify the potential impact of a targeted attack to the organisation and recommend technical and procedural countermeasures.

Penetration testing

Penetration testing services evaluate the security of your organisation's systems by simulating real attacks. These services are conducted by skilled and experienced information security specialists who employ a variety of attack techniques (manual and automatic) to identify any areas of exposure and analyse the consequences of a targeted attack in a safe and controlled manner.

Penetration testing can be conducted from "Black, White or Grey Box" perspectives, depending on your requirements and can either be performed remotely to simulate an attack over the internet, or internally to simulate an internal threat.

Mazars' penetration testing methodologies are comprehensive and drawn from CREST, OSSTMM, NIST and other best practices. These are designed to offer our clients maximum assurance whilst ensuring that testing is safe and non-disruptive.

Vulnerability assessment

Vulnerability assessment services evaluate the security posture of your infrastructure by reviewing implemented security practices, including, processes, security policies, guidelines and standards alongside a technical assessment of vulnerabilities.

Vulnerability assessments should be conducted regularly, along with other security evaluations such as network penetration testing.

HOW CAN MAZARS HELP?

Mazars' penetration testing services include

- Internal and external network penetration tests
- Web application penetration tests
- Wireless penetration tests

Mazars' vulnerability assessments are designed to proactively identify exposures to known security vulnerabilities, insecure default settings and misconfigurations.

As a result of a penetration test or vulnerability assessment exercise, our team will provide the tested organisation with a comprehensive report including an assessment of the existing risks carried and pragmatic recommendations addressing those risks. The executive summary on the report uses non-technical jargon so it can be easily understood by management.

Code review

A key driving force behind most software (commercial or in-house developed) is time to market (or production lead time). This time pressure tends to contribute to a situation where code is rarely vetted for security. System protections that are embedded on the most recent coding languages/ frameworks alongside the use of secure coding practices limit the exposure to code flaws but the assumption should still be that all software may harbour a security flaw.

During a source code security review, our experts inspect the source code of your new or existing application for security weaknesses or insecure coding practices. This service focuses on key elements of the coding structure such as authentication processes, data validation and session management.

The existence of design level flaws present a high risk to applications. Such flaws are hard to find in static or dynamic application scans and instead require a deep understanding of application architecture and layout to uncover them manually. Design level security is crucial and must be adopted at an early stage of an application's development in order to ensure a robust system.

HOW CAN MAZARS HELP?

Mazars can review the source code to validate its security and alignment with secure coding best practices such as those from OWASP, CWE and SANS. Our specialists will identify insecure code, provide a recommendation for change including a perspective with "real risks" for the organisations. Our focus will be on identifying known vulnerabilities and ensuring countermeasures and security controls have been implemented. We will also ensure that the developers are following secure development methodologies and technics.

HOW CAN MAZARS HELP?

Mazars provides a customised range of services to ensure that any social engineering undertaken is realistic, relevant and comprehensive. The service includes open source profiling of your organisation, identifying targets and allowing the construction of pertinent pretexts and scenarios.

Upon completion of the social engineering exercise, a report including the findings and detailed prioritised recommendations will be issued.

Social engineering

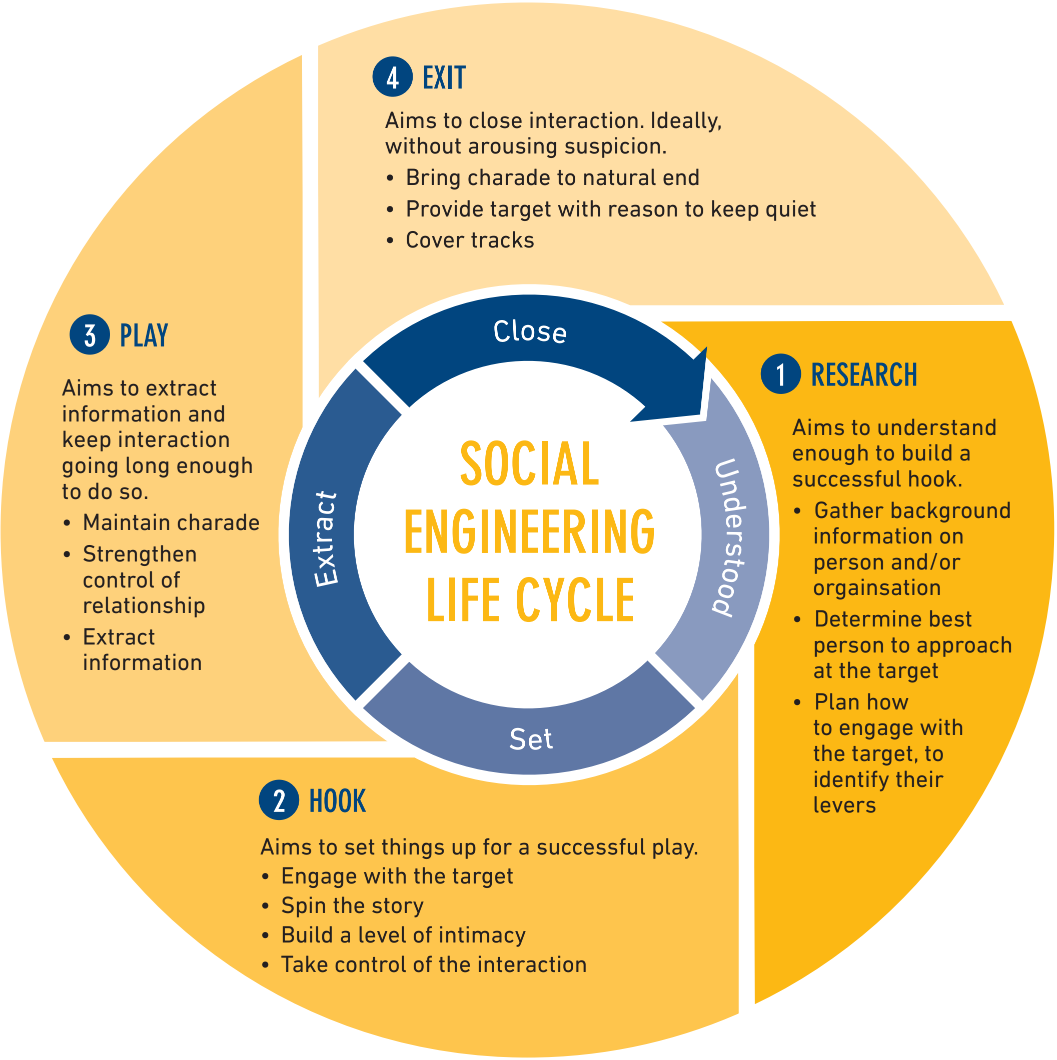
Company staff are still the biggest information security threat due to both lack of awareness and lack of accountability. Mazars helps organisation to increase employee awareness through comprehensive training programs, tested by social engineering (including email phishing, phone pretexting and baiting).

When assessing the security of any system or organisation, it is important to factor in the human and physical elements. Combining periodic physical penetration testing with social engineering exercises promotes security awareness, provides a practical understanding of your security posture and allows for the identification of areas where greater control may be required in order to stay within the tolerance of the organisation's risk appetite.

Social engineering includes the testing of the following typical types of threat:

- PHISHING – masquerading as a trustworthy entity (e.g. through email or website), attempting to acquire sensitive information such as usernames, credit card numbers and passwords.
- BAITING – leaving malware infected media as USB flash drives in a location where they are sure to be found and waiting for the targeted victim to use the device.
- VISHING – eliciting information or attempting to influence action via phone.
- IMPERSONATION/PRETEXTING – using a fictional situation (the pretext) to engage a targeted victim for the purpose of obtaining sensitive information or performing a particular action. This is usually done over the phone.

Targeted attack



1 RESEARCH

Aims to understand enough to build a successful hook.

- Gather background information on person and/or orgainsation
- Determine best person to approach at the target
- Plan how to engage with the target, to identify their levers

2 HOOK

Aims to set things up for a successful play.

- Engage with the target
- Spin the story
- Build a level of intimacy
- Take control of the interaction

3 PLAY

Aims to extract information and keep interaction going long enough to do so.

- Maintain charade
- Strengthen control of relationship
- Extract information

4 EXIT

Aims to close interaction. Ideally, without arousing suspicion.

- Bring charade to natural end
- Provide target with reason to keep quiet
- Cover tracks

HOW CAN MAZARS HELP?

Mazars ISO 27001 services include:

- Business impact analysis and risk assessment
- ISO 27001/2 gap analysis
- Solution design and implementation support
- Security policy review and development
- Security awareness training
- Technical design review
- Incident response plan review and development

Mazars PCI-DSS services include:

- Gap analysis
- PCI-DSS readiness review

ISO 27001 / PCI-DSS readiness assessments

ISO 27001

Information security certification and compliance is a major concern for all organisations and features prominently on the boardroom agenda, alongside cyber security. ISO 27001 is the information security standard that is accepted as best practice both within the UK and globally. By achieving ISO 27001 certification, your business demonstrates that it takes information security seriously.

Mazars provides consultancy, security testing and other services to help organisations achieve ISO 27001 Certification. Our team of ISO 27001 auditors will work with you to assess how you are currently managing information security. We will identify key risks and areas of non-compliance, and provide clear prioritised and pragmatic recommendations.

PCI-DSS

PCI DSS is the Payment Card Industry Data Security Standard – a worldwide standard that was set up to help businesses process card payments securely and reduce card fraud. Compliance with PCI DSS is required for organisations that handle credit cards from the major card schemes including Visa, MasterCard and American Express.

Security architecture review

As the needs of your business continue to change, people, processes and technology change accordingly. To combat this evolving environment, you will need a concise understanding of your security infrastructure to identify areas that may be vulnerable to cyber-attacks. The design of the network architecture and the security controls that have been implemented to segment and protect the network are a key component in protecting an organisation.

A security architecture review is a review of an organisation's infrastructure in order to determine its security posture by examining the topology and deployment of the security boundaries within an organisation. It will identify weaknesses within the architecture and make recommendations for improving the security posture and reducing the attack surface area. This type of service is recommended during the deployment of new infrastructure elements, or after changes and upgrades have been made. Examples of the areas that can be evaluated as part of a security architecture review include:

- Internet/ perimeter gateways
- DMZ segregation
- Wireless infrastructure
- Remote access facilities
- Third party connectivity

HOW CAN MAZARS HELP?

Mazars' security architecture review services include:

- Reviewing your security infrastructure to understand the risks and identify required controls
- A gap analysis against best practices to identify security vulnerabilities that need to be addressed
- Clarification on which infrastructure items need attention immediately and rank how to address additional areas of concern

HOW CAN MAZARS HELP?

Mazars' information security experts have developed a comprehensive security program that can be tailored to your organisation. The core part of this program includes:

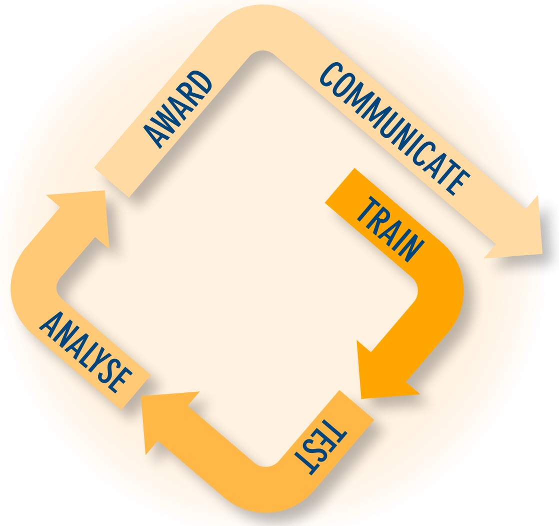
- Comprehensive information security training tailored to your organisation and roles (e.g. board, management or personnel)
- Information security awareness programme development or review alignedwith ISO 27001 and best practices
- Assessment of the current posture on information security by performing test social engineering attacks
- Design of a communication programme around IT security matters
- Assessment of the programme's impact through periodic testing
- Employee engagement initiatives ie. use of a recognition/award scheme

Training awareness programme

The traditional approach to information security relies on three core resources for protection: people, processes and technology. Technology is managed through security processes, practices, procedures and policies. Both technology and processes are dependent on people to operate them and this dependency takes special relevance when current information security studies state that the 'human element' accounts for the majority of data leaks and security breaches.

Organisations need to have an information security awareness program in place to ensure employees are aware of:

1. the importance of protecting sensitive or confidential information;
2. what they should do to handle information securely, and
3. the risks of mishandling information.



Business Continuity Management / IT Service Continuity Management

In the modern world, business success is heavily dependent on the continued operation of its business processes, services, technology and infrastructure. History shows that an unplanned interruption of any kind can have a serious impact on brand value, reputation, revenue and profit.

Business Continuity Management (BCM)

Business Continuity Management (BCM) is a proactive process which minimises the likelihood of a major disruption of your business and also implements effective measures to reduce the impact to your business should a disaster occur.

IT Service Continuity Management (ITSCM)

IT Service Continuity Management (ITSCM) is a process that deals with disasters which impact IT services and infrastructure. ITSCM allows a business to understand the continuity weaknesses within their IT services and take measures to ensure that services are recovered as efficiently as possible when required.

HOW CAN MAZARS HELP?

Mazars' security architecture review services include:

- Reviewing your security infrastructure to understand the risks and identify required controls
- A gap analysis against best practices to identify security vulnerabilities that need to be addressed
- Clarification on which infrastructure items need attention immediately and rank how to address additional areas of concern

Mazars' services include:

- Management level analysis - identifying the critical IT Services for recovery and the risks to the ability of these services to support effective business resumption and customer ITSC requirements
- Supporting the development of Disaster Recovery / IT Service Continuity plans
- Tailored training sessions or a wider programme of awareness activities aiming to improve the level of knowledge and understanding of ITSCM within the business

Why Mazars?

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.

STRENGTH AND DEPTH

A team with experience in dealing with complex environment and projects.

HIGHLY QUALIFIED

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

INTERNATIONAL REACH

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

SENIOR AND EXPERIENCED ENGAGEMENT TEAM

Substantive involvement of Partners and Senior Managers.

SOLUTIONS ORIENTATED

Provide realistic and pragmatic solution.

TAILORED APPROACH

We devise a bespoke service approach for each client.

VALUE DRIVEN

Highest quality of service at a fair price.

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).

Stelios Vogiatzis, Director, Business Consulting, Tech & Sustainability

Stelios Vogiatzis is a Director at Mazars with over 20 years of experience and know-how on strategy implementation, business performance improvement and digital technology applied in various industries such as Banking, Food & Beverages, Energy & Utilities, Construction, Industrial and Commercial. Prior to Mazars, he held various managerial positions in local and multinational companies, including some of the biggest consulting firms. He has extensive experience in Project & Change Management, gained through international assignments in U.K., Denmark, Italy, U.S.A., Japan, Kenya, Romania, Germany & Saudi Arabia. He has also specialised in IT projects related to enterprise wide systems and security.

Please get in touch...

For more information please contact:

Nicolas Quairel
Partner
T: +44 (0)20 7063 4965
E: nicolas.quairel@mazars.co.uk

Ilias Zafeiropoulos
Partner
T: +30 210 6993749
E: ilias.zafeiropoulos@mazars.gr

Stelios Vogiatzis
Director
T: +30 210 6993749
E: stelios.vogiatzis@mazars.gr