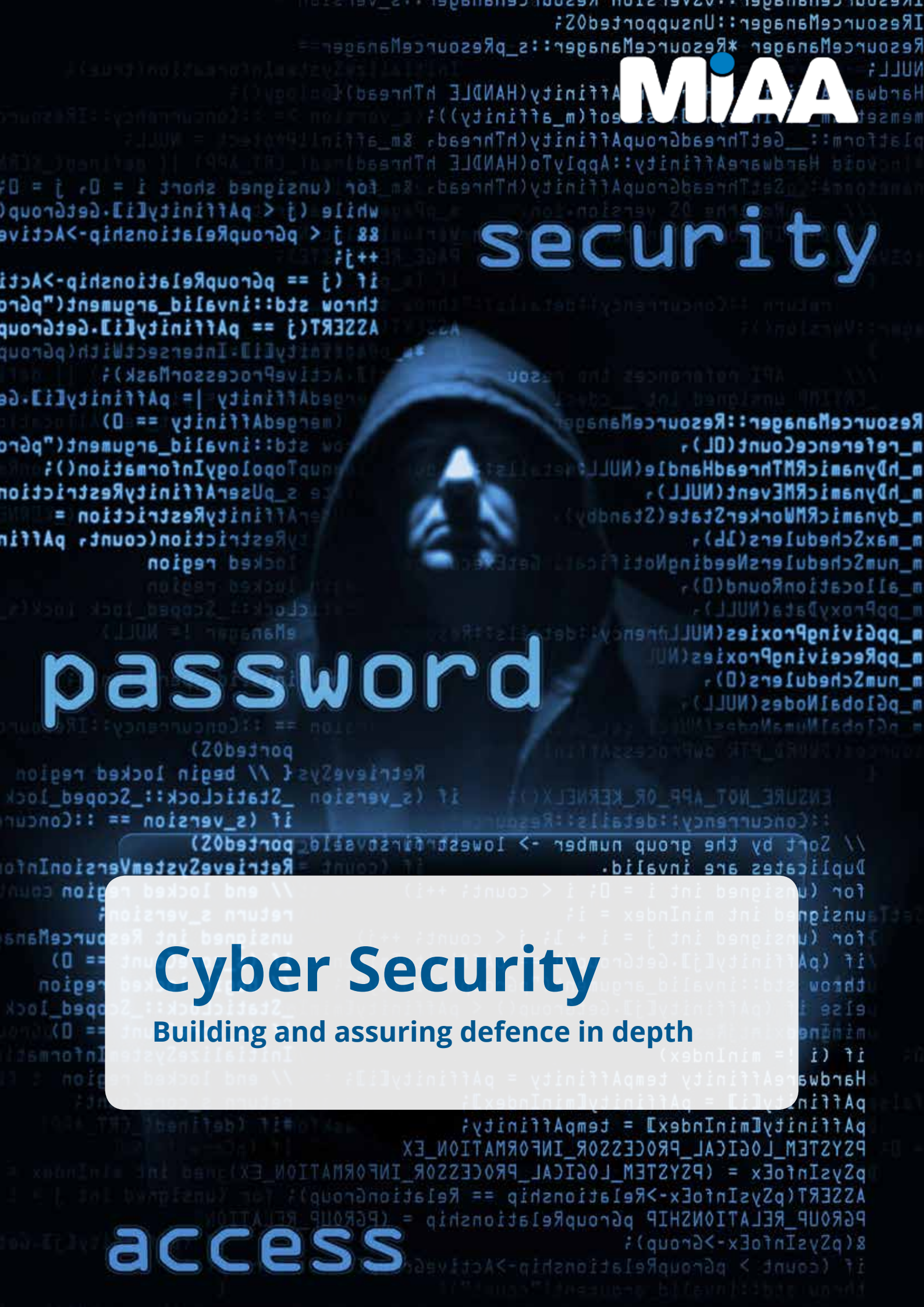


Cyber Security

Building and assuring defence in depth

The Cyber Challenge

Understanding the challenge

We live in an inter-connected world that brings a wealth of information to our finger tips at the speed of light. It provides the intelligence that we need to deliver excellence and to manage complex organisations. It allows us to share "big data" across organisational boundaries, to support research and to further improve services and outcomes; and it does this in a way that has become so engrained within our day to day processes that the thought of working without it is, well, unthinkable!

90% of large businesses

74% of small businesses

had a security breach in the last year [1]

This inter-connected, data driven, world, however, also brings significant operational risk. Recent events have reminded us that the internet is also being used to perpetrate a wide range of crimes, all of which have substantial human and economic consequences, including significant reputational damage.

These, however, are not one off events. More and more often, organisations are being targeted for the data that they possess, to acquire it for profit or hold it to ransom, to disrupt services or simply for the kudos. Malicious hackers, hacktivists and script kiddies are constantly knocking at the door, trying to penetrate networks, using ever more intricate and diverse approaches to gain entry.

69% of large businesses

38% of small businesses

were attacked by an unauthorised outsider in the last year [1]

Gone are the days when "the hack" was a dark art; more and more the intrusion will begin through social engineering. Getting employees to divulge key information, either directly or by providing their credentials which can then be exploited, is often a more successful route for the hacker.

Whether using phishing emails or simply entering buildings wearing a hi-vis jacket, social engineers create an aura or plausibility that encourages us to let our defences down.

But not all data loss or disruption is at the hands of the outsider, it remains the case that incidents are more likely to be the work of an employee.

75% of large businesses

31% of small businesses

suffered staff related security breaches in the last year

In times of austerity, insider related incidents rise, whether the result of dissatisfaction, personal circumstances or the pressures that we put on staff when we reduce headcounts.

All together, this represents a hazardous world in which to operate but the benefits are worth it if we control it.

Building and assuring defence in depth

Protecting data requires a multi-faceted approach to reflect the myriad of systems, vulnerabilities and threat vectors. Organisations cannot depend solely on education of users, nor can they focus on simply locking the doors and windows of the perimeter or even relying on system access controls. The threat horizon is more complicated and defence in depth is required.

Developing, implementing and testing a defence in depth model will provide an organisation with confidence that it has protected its core internal networks, applications and databases; it has secured the perimeter of the network where it touches multi-organisational WANs and CoINs as well as the internet; and, that its users and system managers are aware of their responsibilities, how to detect threats and, importantly, how to react to them.

Implementing a robust process of testing, auditing and continuous improvement will provide the assurance that the organisation and its wider stakeholders require.

20% of NHS Trusts

are fully confident that their board has a complete and accurate picture of cyber risks

At MIAA we have extensive experience working with clients to develop, test and assure their cyber security defences and supporting them to achieve certifications.

With a team of professional architects, testers and auditors, and with a track record of successful delivery, we are able to provide a service that combines industry leading expertise with value for money to create a compelling offer.

1 - HMG 2015 InfoSec Breaches Survey

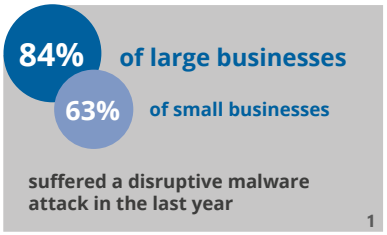
2 - NHS Digital Maturity Survey

Our services

Protecting the core

Your network provides the means for accessing systems and data. It is the heart of your digital nervous system and it should be protected by design.

Our team of security experts are able to support clients by providing a range of services from technical security design to policy and process development and support to achieve certification to acknowledged security standards.



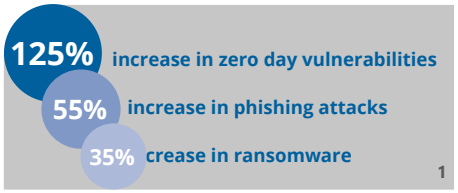
Typical support for clients includes:

- **Security architecture design**, helping clients to build, configure and deploy new and upgraded networks which are designed with security as a cornerstone;
- **Security management assessment**, assessing the capacity and capability of internal information security functions and their ability to deliver organisational requirements;
- **Information risk assessments**, identifying and assessing risks to the organisation's information assets and delivering risk remediation plans for local action;
- **Information asset management documentation**, creating system level security policies and privacy impact assessments;
- **ISO27001 compliance**, identifying the extent to which the organisation complies with the international information security standard, creating action plans and developing compliant policy and procedural frameworks.

Protecting the perimeter

No organisation is an island, however, and the connection of organisations to one another and to the internet creates further vulnerability at the perimeter of the network.

It is essential that organisations understand and manage the risks at the boundary of their infrastructure.



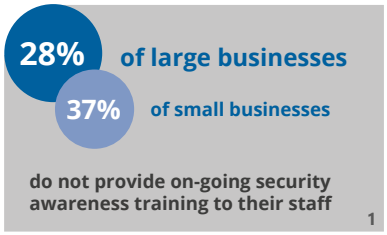
Key support provided to clients includes:-

- **Cyber Essentials base lining and certification**, undertaking assessment against the UK government's Cyber Essentials and Cyber Essential Plus standards and supporting organisations to achieve certification to these;
- **Regular vulnerability assessment**, providing low cost, high speed testing to clients who wish to proactively identify and address issues within their infrastructure. The assessment comprises four main elements; port scanning, service identification, vulnerability identification and reporting. The service is typically delivered on an annual, quarterly or monthly basis;
- **Firewall rule base assessment**, to determine the packet flows and implied access with a view to highlighting any rules that could facilitate external to internal access in order that these can be assessed and, if necessary, removed.

Embedding the culture

People are often described as the weakest point in the security of an organisation; ensuring that they are aware of risks and attacks and training them in how to respond are crucial.

Our security awareness workshops, which can be tailored and delivered to all levels and disciplines within an organisation, can include a live hacking demonstration, provide presentations on security threats and how individuals can spot and react to them, and can include structured discussions with IT teams to identify controls and weaknesses and prepare action plans.



In addition, to support security professionals and system administrators in securing their infrastructures, through our website and a free alerts service we provide regular security advisories relating to vulnerabilities in vendor products.

Testing, probing, improving, assuring

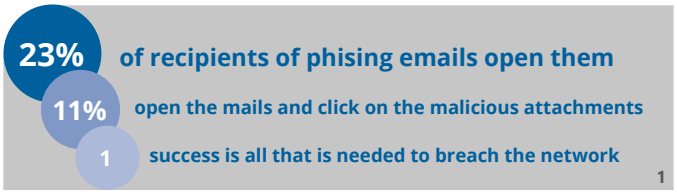
Testing is critical in the assurance and improvement processes. Only by testing the organisations' cyber defences can an accurate assessment of the arrangements be made.

An effective and robust assurance strategy will marry technical review with active testing of the defence mechanisms, looking for the weak points and trying to exploit them.

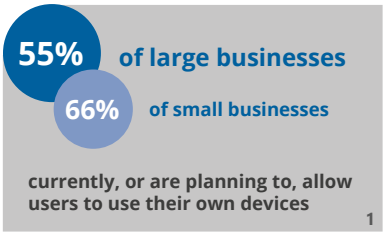
Working with clients we are able to develop co-ordinated testing strategies to meet assurance needs through assignments including:-

- **Penetration testing**, using industry leading tools and techniques we aim to identify weakness in your defences and expose the potential for them to be exploited. Weaknesses identified are risk assessed and prioritised and remediation plans are provided in order to improve security and learn lessons.

- **Social engineering and phishing**, exploiting what is often the weakest point by creating a false position of trust with an end user in order to get them to unwittingly expose credentials or introduce malware is an increasingly common attack vector. Our exercises mimic these approaches allowing the organisation to assess its exposure, identify training needs and deliver effective awareness raising.



- **Web application testing**, as organisations increasingly use web interfaces to present applications to users from multiple locations, on differing platforms, so data is potentially more widely exposed. Our testing is typically delivered in two stages, with no authentication to the application and then with a valid user account for testing privilege escalation vulnerabilities, in order to identify weaknesses in the authentication and authorisation mechanisms.
- **Remote access & VPN testing**, supporting the mobile workforce requires secure entry points to the corporate network. Starting with reconnaissance to determine the type of remote access or VPN implementation we identify known attack vectors against specific vendors. This is followed by the use of a variety of tools to capture hashes which are run through password crackers to harvest passwords which could be used for malicious access to the RAS/VPN.
- **Mobile device and own-device management**, aimed primarily at mobile devices such as laptops, tablets and smartphones we are able to test the security of individual devices and assess the configuration of mobile device management solutions.



- **Red/tiger team exercises**, representing an all-out attempt to gain access to a system or data by any means necessary. This can include penetration testing, physical breach, testing phone lines for modem access and also testing employees through several scripted social engineering and phishing tests. They can be undertaken as a combined exercise or can be delivered in a phased approach as part of a structured security assurance programme.
- **Core infrastructure assessments**, covering the platform upon which systems run and data flows and which enable information to be delivered to the right people when and where needed, our reviews seek to provide an opinion on the arrangements in place across a range of areas including:

- Network monitoring	- Server management
- Incident management	- Domain policies
- Change management	- Server baseline policies
- Physical security	- User management
- Back-up and recovery	- Patch management
- Vulnerability management	- Malware protection

- **Asset management reviews**, considering the extent to which the organisation has a clear understanding of the totality of its hardware and software assets and the extent to which these are managed and monitored in order to ensure effective deployment and legal compliance. In particular, the reviews seek to establish the accuracy of asset inventories, the effective processes for recording asset data, the secure disposal of equipment and the reconciliation and management of, often complex, software licences.
- **Application security**, assessing the security of systems including access control, logging and monitoring, resilience, back-up and recovery and change control.

Monitoring, identifying, responding, resolving

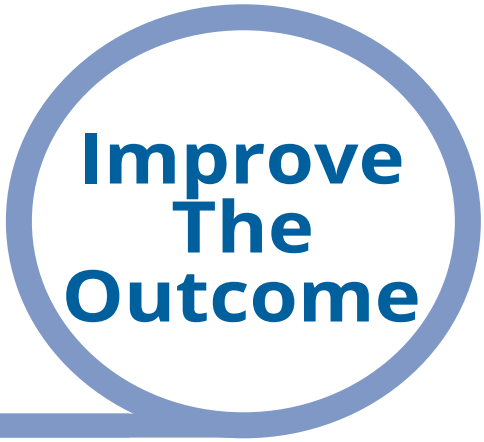
We are able to provide an incident response service that can respond quickly, determine the best recovery strategy with you, and then work together to get you back up and running.

Alongside, we can provide a full digital forensics service from initial response, through secure acquisition to investigation and reporting.

The service is delivered in accordance with all relevant legislation, standards and guidance and can be complemented by the provision of expert witnesses at disciplinary hearings or court cases if required.

Improve the outcome

With a comprehensive service offering, delivered by experienced professionals, we are able to provide the support you require to meet your cyber security needs. From helping to build security into designs, through testing and ultimately responding to events, you will find that working with MIAA will improve your defences and provide the meaningful assurances that you require in these challenging times.



To discuss how MIAA can support your organisation to improve and assure its cyber defences please contact:-

Tony Cobain - Assistant Director (Informatics & Infrastructure)

Tel: 07770 971006

Email: tony.cobain@miaa.nhs.uk

To discuss how MIAA can support your organisation to improve and assure its cyber defences please contact:-

Tony Cobain - Assistant Director (Informatics & Infrastructure)
Tel: 07770 971006
Email: tony.cobain@miaa.nhs.uk