CYBER SECURITY SOLUTIONS

Defending you from cyber attacks.

HLB IRELAND

Together we make it happen

Ensuring Business Security - Comprehensive Cyber Security Solutions to Safeguard Your Data, Systems and Networks

In today's digital world, cyber threats are widespread and becoming increasingly sophisticated; organisations must assume that they will be breached at some point. A cyber breach can have far-reaching and severe consequences, such as the theft of sensitive data, financial loss, damage to reputation, and legal and regulatory ramifications.

By assuming that a breach will occur, businesses can take proactive measures to mitigate the risk and minimise the impact. This means implementing robust cyber security measures, such as regularly updating software, training employees on best practices, and conducting regular vulnerability assessments.

By using a globally recognised cyber security audit framework on your business, our cyber team can provide you with a clear picture of current cyber risk posture and capabilities, giving management and directors a view of how, where and why to invest in managing cyber risks.

Experience the Power of Our Security Engagement Model to Mitigate Threats

Backed by our expertise and extensive experience in this specialised area, our services are classified into three distinct solutions.

Audit

Know the strength and maturity of your current cyber security posture, and where you need to be.

Remediation

Implement the right solution at the right scale for your business, and you will be confident nothing is left to chance.

Manage (Cyber as a Service)

Management of your ongoing security requirements to enhance detection and response capability.

Cyber Security Solutions

1. Cyber Audit

We proactively search for and identify credible cyber threats to help businesses discover and remediate potential risks. Our team undertake a systematic evaluation of a business's information systems, processes, and controls to identify vulnerabilities, assess risks, and ensure compliance with security policies and regulations. The purpose of a security audit is to determine the effectiveness of an entity's security measures and to provide recommendations for improvement. A Cyber Audit can be carried out fully remotely.

2. Cyber Remediation Process

A key deliverable from the Cyber Security Audit is a report detailing the findings, including any identified vulnerabilities and non-compliance issues. The remediation process involves taking appropriate actions to mitigate the identified risks and strengthen the business's security posture. This can include us carrying out the remediation, managing the process or overseeing the process that is being carried out by the existing IT Partner.

3. Cyber As a Service

This provides clients access to a wide range of Cyber Security solutions and expertise. This service allows clients to choose the specific Cyber Security Services they need based on the result of the audit. It provides the flexibility to scale up or down as needed, depending on changes in the entity size, operations, or threat landscape.

By partnering with us, businesses gain access to our team of Cyber Security experts with specialised knowledge and experience. Our team of professionals are equipped with the latest tools, technologies, and methodologies to address various security challenges effectively.

1. Cyber Security Audit

This fundamental starting point allows a business to gain a comprehensive view of its security landscape and identify any vulnerabilities. This professional security audit, conducted to a global standard, is known as a CIS Audit (Centre of Internet Security). This approach determines the risk profile and provides valuable insights into potential vulnerabilities.

Our team of experts specialises in conducting thorough security audits and risk assessments that cater to business-specific needs. This approach allows for a clear view of the current position and, in turn, outlines what are the key priorities in terms of protecting the commercial interests of the business.

Our audit focuses on a set of 18 actions that make up the best practices to tackle major attacks against systems and networks. These CIS Critical Security Controls* provide a highly practical and useful framework for every organisation to use for both implementation and assessment. The CIS Controls are considered to be an international-level collection of best security practices.

Because the Controls are developed by the cyber community and based on actual threat data, they are an authoritative, industry-friendly, and vendor-neutral approach to the assessment and auditing of security.

**The CIS Controls were originally developed by the U.S. National Security Agency (NSA). After several organisations contracted by the U.S. Department of Defense (DoD) suffered major data loss incidents. The "DoD" asked the NSA to identify the most important security controls to protect against common attacks. Implementing the six basic controls has been reported to decrease the chance of suffering a cyberattack by 84%.*

2. Cyber Remediation Process

The Cyber Remediation Process refers to the steps taken to address and resolve the issues identified during a cyber audit. This process aims to mitigate the risks and vulnerabilities identified during the audit and ensure the security and integrity of your organisation's systems and data.

Identify and prioritise vulnerabilities

Review the findings and recommendations from the cyber audit report. Identify and prioritise the vulnerabilities based on their severity and potential impact on the business's operations, data, and systems.

Allocate necessary resources

Determine the resources required to implement the remediation plan effectively. This may include allocating budget, personnel, and technology resources to address the identified vulnerabilities.

Conduct user training and awareness

Provide training and awareness programs to employees to educate them about the risks and best practices for cyber security. This helps ensure that employees understand their role in maintaining a secure environment and are aware of potential threats..

Develop an action plan

Create a detailed action plan that outlines the specific steps required to address each identified vulnerability. Assign responsibilities to the appropriate individuals or teams within the organisation.

Implement security controls

Implement the necessary security controls to address the identified vulnerabilities. This could involve applying software patches, configuring firewalls, updating access controls, enhancing encryption, or implementing multi-factor authentication, among other measures.

Review and update policies and procedures

Evaluate and update existing policies, procedures, and protocols to align with best practices and address the identified vulnerabilities. This includes incident response plans, data backup and recovery procedures, access controls, and security awareness programs.

Document and report

Maintain documentation of the entire remediation process, including the actions taken, responsible parties, and results. This documentation can serve as evidence of compliance with regulatory requirements and assist in future audits or assessments.

3. Cyber As a Service

Once both the Cyber Security Audit and the Cyber Remediation Process are complete, it's important to ensure that the business is protected on an ongoing basis, given the nature in which cyber threats are ever-evolving.

We provide Cyber as a Service to businesses on an ongoing basis to ensure the business stays up-to-date with emerging threats and industry best practices. We use a number of key services to do this, depending on the nature of the specific business.

Cyber as a Service includes the following suite of services:

Monitoring and Management

Continuous monitoring of systems, networks, and applications for security threats, as well as management of security tools and technologies. Monitoring runs on a 24/7, 365-day basis.

Vulnerability Assessments and Penetration Testing

Identification of vulnerabilities in systems and networks through security assessments and simulated attacks to evaluate their resilience.

Data Protection and Encryption

mplementation of data protection measures, such as encryption and data loss prevention, to safeguard sensitive information.

Security Consultancy

Expert advice and guidance on cybersecurity strategy, risk management, compliance, and regulatory requirements.

IIncident Response

Assistance and support in responding to and mitigating Cyber Security incidents, including investigation, containment, and recovery.

Security Awareness Training

Education and training programs to enhance users' understanding of cybersecurity best practices and promote a culture of security within a business.

Darkweb Monitoring

We use specialised tools and techniques to identify and track illegal activities, as well as the presence of sensitive or compromised information that may be relevant to the business.

Ongoing Audits

Scheduled audits to ensure the CIS controls are operating effectively and the implemented tools are functioning as intended.

Quarterly Intelligence briefing

Keep the business informed about the latest cyber threats. Report on incidents over the last quarter and advise on the threat landscape and potential risks so that the business can make informed decisions regarding its cyber security posture.

Why choose HLB Ireland

HLB Ireland is a leading advisory & accounting firm working with ambitious domestic and overseas businesses in Ireland. We take a strategic approach to our market and are focused on listening to our clients and anticipating their future needs. This anticipation of needs was the key driver to the addition of Cyber Security Services.

In 2020, HLB Ireland acquired FutureRange, a specialist-managed technology business; the business has grown its Cyber Security services significantly since the addition of several key senior resources.

We provide a full range of IT Consulting and Professional IT Support Services to businesses in all industries and market sectors. Our highly skilled team of IT specialists includes Cyber Security and Digital Transformation Experts with many years of experience and a commitment to delivering first-class solutions that exceed our client's expectations.

Cyber Security is a top priority in today's digital landscape. We appreciate the critical importance of safeguarding business-sensitive data and ensuring robust protection against ever-evolving cyber threats. Our Cyber Security Experts work diligently to implement robust security measures, conduct thorough risk assessments, and design tailored strategies to mitigate potential vulnerabilities.

Cyber Security Solutions

You can take the first step on a path to a more secure IT infrastructure.

Contact us today to schedule a consultation.

HLB Ireland

Phone: +353 (0)1 291 5265

Email: info@hlb.ie

Website: www.hlb.ie