OPTIMISING IT

CYBER-SECURITY
& INFORMATION SECURITY

UNDERSTANDING **YOUR RISKS**

At its core, good Information Security practice is based on knowing the answer to the four questions:

- **WHAT**
  information assets do you have?
- **WHERE**
  are your organisation's information assets?
- **HOW**
  important are they from a business perspective?
- **IF**
  the current level of protection in place (for CIA) is adequate to protect each asset?

Only then can you put in place appropriate controls to reduce your risk.

Cyber-security and Information Security Consultancy

Information Security is the art of protecting Confidentiality, Integrity and Availability (CIA) of any type of information (digital/electronic like the internet and physical like paper documents in a safe), by preventing the unauthorised Disclosure, Alteration or Destruction (DAD) of it.

When we think about 'Cyber' in the context of preventing cyber-attacks, we are talking specifically about protecting digital/electronic information which (particularly for internet-connected systems) is a risk for virtually all businesses:

> **"There had been a "sharp increase" in the number of cyber-attacks this year, with more than 60% of firms having reported one or more attacks - up from 45% in 2018."**
>
> HISCOX CYBER READINESS REPORT 2019

Pragmatic Steps To Reducing Your Cyber Risk

It's easy to recognise that you realistically can't reduce risk to zero and will probably waste significant amounts of time and budget by trying to do so by focusing on reducing risks by using controls on one or two containers (like Firewalls and Antivirus alone). However, you can learn how to reduce risks to the correct level for your business-critical information assets by employing our Information Security professionals, to carry out a well-informed, balanced and pragmatic review of your estate using our tried and trusted methodology.

It doesn't need to cost you the earth: our Cyber-Fit review is a comprehensive and cost-effective starting place to find the right answers to the four questions 'what', 'where', 'how' and 'if' collectively.

Supply Chain Vulnerabilities

Vulnerabilities which can affect critical information not only in your IT estate but also within your supply chain, means you cannot rely on unqualified claims from your suppliers that they are adequately protecting your information. The ICO issues fines to businesses who use third-party suppliers (e.g. Datacentre Providers) that get compromised, and so to avoid fines and reputational damage you can engage Optimising IT to assess and report on the adequacy of the information security controls key suppliers have, to verify your business is not subject to hidden risk.

CYBER SECURITY
SERVICES

CYBER FIT
A comprehensive on-site Cyber-security review

CYBER TEST
Pen testing, one off or ongoing vulnerability scanning services, technical security reviews or a tailored combination

CYBER TRAINING
Cyber-security awareness workshops for business leaders or employees

CYBER COMPLY
Achieve & maintain compliance with Cyber Essentials

How Optimising IT Can Help

Our customers benefit from a range of our Cyber-security services to help reduce the risk of an attack to having measures in place to recover from one.

Cyber Fit

Cyber Fit provides a comprehensive on-site Cyber-security review, understanding where your risks are right now, and importantly, what you need to do to reduce those risks.

We provide a real-world view of how your current security approach stacks up against standards like Cyber Essentials and industry best practice and crucially, provides key advice about what actions to take to safe-guard your business. Reviews typically take a day to conduct but this is dependent on the shape and size of your organisation. We'll provide a focussed report detailing key areas for improvement as well as the actions required to improve. The output from the vulnerability scan will be presented in a management friendly report, with the detail available for your technical teams.

Cyber Test

Cyber Test takes care of the technical testing of your environment across on-premise, user devices and cloud hosted systems. We can provide pen testing, one off or ongoing vulnerability scanning services, technical security reviews or a tailored combination.

Cyber Training

Staff are the number one risk. With easy access to your systems and data they (by making simple and avoidable mistakes) can allow hackers to gain access to your data.

- **Staff Training**
  To cost-effectively mitigate the risk from your own staff, we offer our regularly refreshed, engaging and pragmatic staff cyber awareness training. We will analyse your threat profile and discuss this with you prior to the training day, making our training tailored and flexible to fit with your business needs.

- **Business Leaders Training**
  Our half-day practical cyber awareness workshop for business leaders will show you how to approach Cyber in the right way, with a risk management led approach.

Email cyber@optimisingit.co.uk to request our detailed Cyber-security training summary sheet.

Cyber Comply

Cyber Comply can help you to achieve, and crucially maintain compliance with Cyber Essentials (a 'badge of confidence' from the U.K. National Cyber Security Centre). Government and Defence suppliers must be certified by an independent accredited assessor and other organisations are highly recommended to hold to give confidence to customers and partners.

Cyber Comply can also assist your organisation to prepare for or assess compliance against the ISO27001 Information Security Management Standard, which increasingly is seen as the 'gold standard' information security certification standard that customers and partners expect other organisations dealing with them to hold, and enabling you to tick the essential 'external security governance check box' on your latest tender submission.

CYBER SECURITY
SERVICES

CYBER ADVANCE
Everything to help safeguard your business from cyber-threats, including our Staff Cyber Awareness Training

DISASTER RECOVERY
Massively reduce recovery and restore times for everyday peace of mind

Cyber Advance

Cyber Advance is a bespoke and tailored service for organisations who may already have mature Cyber-security protection but require specific gaps that need filling by external expertise. Our bespoke service includes:

- Information Security Management
- Virtual and fractional CISO services
- Staff technical training
- Security Architecture design
- Requirement definition, tender review
- Staff selection services
- Due diligence /acquisition activities
- Breach investigation and forensics
- Breach response services

Disaster Recovery

In the event of a business-impacting disaster, you want to know that you can get your business back up and running as quickly as possible, reducing the impact on the service you deliver and ultimately on your bottom line. Our services can offer:

- Massively reduced recovery and restore times
- Scalable solutions that grow with your business
- Resilience to localised issues due to being physically remote from your business
- Regular disaster recovery tests – leaving you with no nasty surprises
- 24×7 invocation plans

With 60% of SMEs that suffer a major cyber-attack ceasing to trade within 6 months, make sure you are doing everything you can to avoid being another statistic.

> **"Small businesses are collectively subject to almost 10,000 cyber-attacks a day, according to new findings from the UK's largest business group."**
>
> FEDERATION OF SMALL BUSINESSES (FSB) RESEARCH

Any questions?

We're happy to answer any questions you may have about Optimising IT's Cyber-security and Consultancy services:

01242 505 470
contact@optimisingit.co.uk
www.optimisingit.co.uk/cyber-security
@optimisingit

OPTIMISING IT