Is the threat of a cyber attack keeping you awake at night?
Take action **NOW** to protect your business.

Book your

Cyber Security Risk Assessment

Cyber threats continue to increase. Cyber criminals are becoming more sophisticated and scams are getting harder to spot.

The processes and technology that would have protected your data and systems in the past are no longer sufficient.

Optimal cyber security requires companies to be constantly updating and assessing their security defences.

We all need to do more. But where do you start?

The first step to doing more is understanding where you're at, and the best way to do this, is to carry out a Cyber Security Risk Assessment.

What is a Cyber Security Risk Assessment?

Identify, assess, and prioritise risks

A Cyber Security Risk Assessment will help you accurately evaluate your company's security posture and understand where you need to apply additional resources and attention.

It is an **essential** component of developing a coherent and mature cyber security strategy.

The TFS Cyber Security Risk Assessment involves a high-level set of 80 – 250 questions, expertly explained in non-technical terms that generate your personalised heat map of risks.

We'll guide you through an easy-to-digest report, identify your biggest risks and present options to mitigate them. You will have the information you need to make informed decisions.

How often should you assess your risk?

Due to the ever changing nature of the cyber security landscape, we recommend a Cyber Security Risk Assessment is carried out **at least once a year**.

The Final Step.
Professional IT

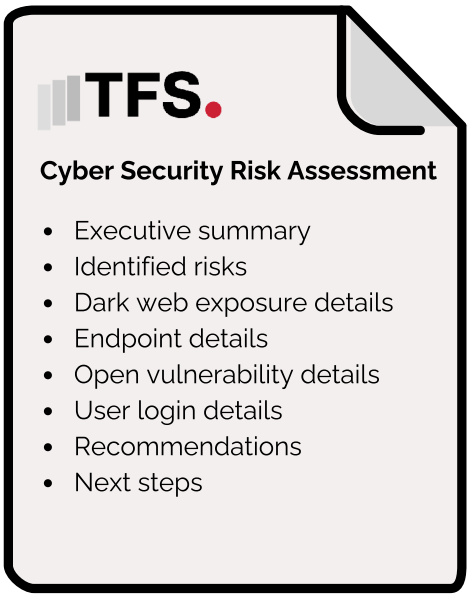
A TFS Cyber Security Risk Assessment

Will give you:

- A broad, high-level understanding of current security risks.
- The ability to assess those risks and consider options for technical, training, insurance or other mitigations.
- A benchmark against which to review security regularly.
- The ability to set a roadmap and a budget for security.

What is included in a Cyber Security Risk Assessment?

The TFS Cyber Security Risk Assessment includes a comprehensive audit covering all areas of your business. You will receive a concise, easy to digest report identifying risks and threat level, along with tailored recommendations.



A complete breakdown of identified risks

From devices, document storage and staff cyber awareness training to dark web exposure, password policy and email filtering, everything in your business will be assessed for security risks. No stone will be left unturned.

These security risks are then classified as low, medium, high or critical risk.

We recommend remediation actions and help you take steps to reduce this risk and ensure resilience in the event of an attack.

Dark web exposure details

We will scan the dark web and detail the specifics of your dark web exposure, including the users affected, the source of the exposure, its severity and recommended next steps.

Endpoint details

We will assess each of these elements for all your endpoints:

- Operating system
- Firewall protection
- Basic anti virus protection
- Advanced endpoint protection
- DNS protection
- Remote desktop access
- Open vulnerabilities
- Asset age

What is an endpoint?

An endpoint is any device that is physically an end point on a network.

Desktops, laptops, smartphones, tablets, virtual environments and physical servers can all be considered endpoints.

Duty of care

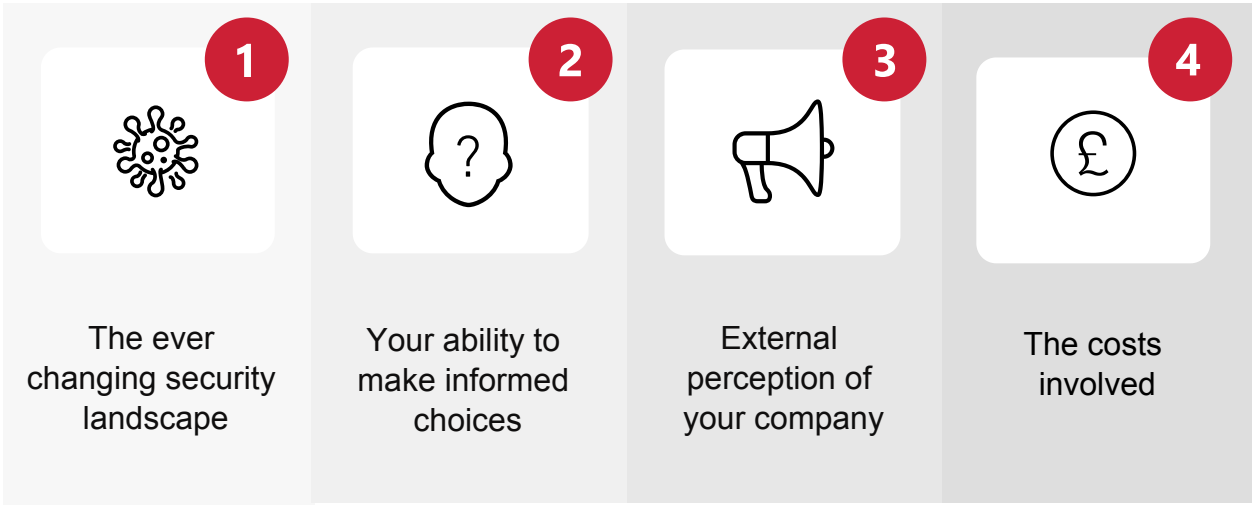
When it comes to technical details of a risk assessment it's easy to think about security in an abstract sense.

It is important to remember that cyber security is about more than just meeting certain technical criteria. It's also about performing a duty of care, that if unfulfilled has an impact on how your clients, staff and shareholders perceive your business.

A risk assessment is an essential part of meeting that duty of care. Here's why it's so essential.

Why is a Cyber Security Risk Assessment so essential?

There are four key reasons why having an annual security risk assessment is critical to the success and survival of your business.



1 The cyber security landscape is constantly evolving

Cyber criminals are becoming more sophisticated and are continually developing new ways to breach and extort companies.

Older technology and processes that still work, and thus still appear to keep you secure, may not be sufficient to the threats that currently exist.

A good example of this is logins and Multi-Factor Authentication (MFA). While MFA is an invaluable security tool that should be mandated for every organisation, it is no longer as effective at protecting our data as it used to be.

This also applies to official cyber security requirements. Take Cyber Essentials Plus for example, the UK Government's minimum-security standard. It says it will help protect against 80% of threats. However, the standard changed significantly in January 2022, and will inevitably change again.

An annual risk assessment will show you the extent to which your processes and protections are working and highlight how drastically the cyber security landscape can change in short periods of time.

It will help you develop planned responses to potential crises that fit your circumstances and budget.

2 Good choices = good governance

People tend to think of cyber security as tech barriers. If cyber security were, then human error wouldn't be every organisation's number one security risk.

In reality, cyber security is about people. It's about the way people interact with technology, the choices they make and how it puts organisations at risk.

To make good choices when it comes to cyber security, people need a specific mindset and set of behaviours (which we call having a 'security-first mindset'). This comes from education, best practices and consistent behaviour modelling from the higher-ups within an organisation.

They also need knowledge. Knowledge about their security posture, to make informed choices and decisions.

Our risk assessment involves a high-level set of 80 – 250 questions, expertly explained in non-technical terms that generate your personalised heat map of risks.

With an easy-to-digest report of your biggest risks and options to mitigate them, you now know enough to make informed decisions.

The worst possible position you can be in with security is in the dark. Making good choices comes from knowing what your cyber risks are before they happen, rather than after.

3 Perception is reality

Companies are ever-increasingly facing the public fallout of a breach or security incident. Security incidents can topple trust in companies so deeply that they never fully recover, financially or reputationally.

The ones that come out the other side unscathed, are those who handled the fallout confidently and competently. People will judge you based on your actions, not your intent.

With a security risk assessment and action plan, you can now be on the front foot in terms of making decisions, controlling the budget and talking confidently to clients.

It will help you communicate effectively with the police and the ICO, having put essential policies into place to protect yourself and your staff.

You can show hard evidence to your clients and staff that you have never ignored security risks, and have always worked to mitigate them as much as possible. Keeping notes on your reviews and decisions will prove your due diligence, and make you stand out compared to competitors.

This allows you to avoid taking full responsibility in the eyes of the public, for incidents beyond your control.

4 The financial stakes are high

If you avoid spending on security now, you're likely to spend more on it later.

The cost of ransomware, fines, staff inability to work etc. after a breach can add up to extortionate amounts. Far more than the amount you were considering investing in your security.

Cyber insurance is essential and once you have had a comprehensive Cyber Security Risk Assessment it will be so much easier to judge what level of protection you require. But remember, you must have the basic policies and procedures in place to ensure your insurance is not invalidated.

Our approach to Cyber Security

At The Final Step, we offer cyber security solutions tailored to your needs. Your budget, business objectives and security requirements are carefully considered each step of the way.

We take a hands-on approach, investing significant time, resources and technology into evaluating the security stance of your company.

We strive to provide you with an expert consultancy that allows you to make informed decisions and demonstrate your good governance.

Full range of security services

We provide a comprehensive range of cyber security solutions for small and medium sized businesses. You are not forced into buying a package but can pick the services your business requires.

Working in partnership

We work with your in-house IT to provide easier licensing and running of enterprise security tools that otherwise may be beyond reach.

Risk assessment

We offer an easy, cost-effective Cyber Security Risk Assessment process from which to start or review your cyber security journey.

Continuous improvement

We work with you to continuously improve your security and resilience, adjusting to the latest threats in line with your needs and budget.

Take action today!

Every industry and every company face unique security risks, that cannot be accounted for in a generic 'one size fits all' plan.

To enhance your security, and ensure resilience in the event of an attack, you must understand your risks.

Book your Cyber Security Risk Assessment today!
Call 020 7572 0000 or email contact@thefinalstep.co.uk

020 7572 0000
contact@thefinalstep.co.uk
www.thefinalstep.co.uk

Gold Microsoft Partner

CYBER ESSENTIALS CERTIFIED PLUS

The Final Step. Professional IT