Identify threats and define a security strategy to protect your business

How serious will a security breach be? It can cost millions to deal with the consequence of a cyber security incident – and more attacks are likely if you don't take action. Our Cyber Maturity Assessment will help support your security posture and cyber defence capabilities. Drawing on our unrivalled experience and expertise and using established frameworks, we will assess your defences, identify threats and define your strategy.

A cyber-attack won't announce itself or happen when it's convenient for you. It's far more likely that you'll be unaware of it until a supplier or customer notices a problem and raises the alarm. Chances are, you'll then discover the source of the problem has been hidden deep within your organisation for months, or even years.

With your security constantly evolving to meet new threats, it can be easy to lose track of what's in place, or where your weak spots are. Your business could be open to serious risk and you might not even know it. Even when you're aware of the risks, you might not have the right solution. While you can never remove risk completely, you can manage it, get the measure of it and spot what's coming next.

Staying secure is about staying one step ahead

Our front line position means that we see how and where attacks come. We're constantly watching, learning, predicting and responding to the latest threats to protect both our customers and BT.

Focusing on dynamically managing business risks across your whole organisation, we work with you to conduct a Cyber Maturity Assessment, which will:

- identify the threats to your organisation
- map out security threat scenarios to help you with planning and future analysis
- determine the current maturity of security controls in relation to your threat landscape
- define a multi-year strategy and a security program to allow the stakeholders to follow-up situation and improvements.

Supporting your cyber defence capabilities

- understand your threat landscape
- create a high-level view of the threat your organisation faces; which allows you to focus on how to deal with it
- create threat scenarios that detail where threats are coming from, their likely impacts and how they can be dealt with
- provide advice in how you can use threat scenario planning to feed into strategic security control development
- define a multi-year strategy and a security program including budgets to allow the stakeholders to follow-up situation and improvements.

"Nearly a third of CEOs list cyber security as the issue that has the biggest impact on their company today, yet only half feel prepared for a cyber-attack."

Taking the offensive, disrupting Cyber Crime, a recent report by KPMG and BT

Put your compliance and risk management needs in expert hands

We are one of the world's leading and most trusted security brands, derived from a set of credentials that have been earned over decades of experience in the field.

For the Security Control Analysis, we recommend using an industry standard framework to understand the maturity of your cyber security strategy.

CIS Critical Security Controls or NIST Cyber Framework are both recommended choices which we can apply when analysing security controls. Using one of these two frameworks will allow your organisation to better structure your cyber security governance, management and operations.

Cyber controls are wide ranging and complex; it is not always easy to work out where to start. Using the CIS Critical Security Controls or NIST Cyber Framework provides a prioritised and focused approach that means organisations spend their time and resources where they are most effective.

We use these frameworks to assess where potential shortfalls may exist and then work with you to understand which controls should be implemented first and at what level. Our risk management approach is used to build remediation or improvement plans tailored for your situation. This helps you to build a clear business case to improve your overall cyber security posture.

Why choose BT?

Take advantage of a partner with **a broad view and enormous experience** in every market segment. Our global Security Consulting capability consists of **500 security specialists** with expertise in every cyber area. Our highly skilled consultants hold industry certifications like CISSP, CISA, CISM, CGEIT, QSA, CCEP, CCEP-I, CIPP, CIPT and ITIL.

We are **accredited for performing consulting services on a global scale** by Lloyd's Register Quality Assurance for the ISO9001:2008 quality management system. Holding the ISO9001 certification since July 2003 shows our long-term commitment to continuously improve the quality of our services.

We are **one of the largest security and business continuity practices** in the world, with more than 2,500 security consultants and professionals globally that has been offering security and business continuity expertise to our customers for many years.

We are one of only a few organisations **providing integrated network and security solutions** both commercially and technically. We operate with local presence in more than 180 countries. This global reach also covers 14 global Security Operations Centres (SOC's), 45 data centres and 250+ customer specific operations.

Scope	Activity	Deliverable
Review and analysis of threat landscape	• A time-boxed review to: • determine as-is cyber defences. • determine baseline assets, actors, topology and volumes.	An agreed number of document targeted threat assessments and key threat scenarios against critical services and channel gaps.
Review of current security controls	• A time-boxed review to: • identify required controls and processes against known threats. • provide a gap analysis of controls against industry best practices. • identified threats to the business.	A report of the current maturity of the Top 20 Critical Security Controls or NIST Cyber Framework with a set of prioritised recommended mitigations.
Executive report	A final report outlining our finds and observations.	A report providing our recommendations, an overall maturity level assessment for the organisation, a strategic plan detailing how gaps should be addressed and a high level roadmap show how the strategy would be deployed.

What could Cyber Maturity Assessment do for you?

Visit bt.com/globalservices

Offices worldwide.

December 2019