



Means  
Business

# Don't let a cyber attack hold your business back

Our security sets you free

BT Security Whitepaper:  
Embedding a cyber conscious culture



# Contents

---

# Foreword from Tristan Morgan



## Can you confidently say that your own organisation has a robust cyber conscious culture?

Businesses are now transforming at record speed, connecting everything, everywhere to better serve their employees and customers. With transformation comes a balance of reward and risk.

82% of businesses rate cyber security as a ‘very high’ or ‘fairly high’ priority.\* And in a recent survey, commissioned by BT in partnership with Sapio Research, over a quarter of respondents say their biggest pain point is keeping security up to date against latest threats. However only 59% are currently offering cyber security awareness training to their employees.

It’s clear that businesses are trying to tackle ever-evolving threats against a backdrop of skills gaps, employee awareness and a raft of new and evolving technical solutions. It’s hard to know where to turn. We believe the answer lies in driving truly integrated, cultural change through the heart of your business.

As a people-focused company we put our customers, their customers and our own people at the heart of everything that we do, and we understand the level of cyber awareness, practical guidance and tools necessary to survive and thrive as a modern enterprise.

Our own culture of cyber awareness helps every one of our 80,000+ UK employees protect themselves, our business and most importantly our customers. We extend our learning and support beyond the workplace, fostering a culture of training and engagement that increases collaboration and personal accountability.

We use this lived experience to bolster our advisory expertise. This, alongside our deep experience in managed security services, allows us to work meaningfully with our customers, advising them through their own challenges as they work to build a robust cyber awareness culture within their organisation.

Our whitepaper brings together industry opinion and BT’s own experts to explore the key themes around the cyber conscious culture recommended for every organisation – to safeguard your people, your assets and ultimately your reputation. We examine the foundational building blocks we believe necessary to help drive this transformative culture. Providing you with a practical methodology, key steps and tactics to adopt as you progress through each foundational element.

Read on to find out how you can prime your business – opening up new potential to harness the best in tech to innovate and grow – by locking in security at your core.



**Tristan Morgan**  
Managing Director, BT Security

# Executive summary



---

“Companies today are totally reliant on their IT systems and networks – so protecting these assets is absolutely critical. By aligning your security strategy with your business strategy, you can not only defend against cyber threats and risks, but also start to see the benefits of security as an enabler to your business outcomes. The start of this journey is embedding a cyber conscious culture throughout your organisation and business practices.”

**Tristan Morgan**, Managing Director, BT Security

---

## The rising wave of cyber crime

Escalating levels of cyber crime are an inevitable by-product of our increasingly sophisticated lives. Emerging tech has catapulted us forward but has also created more opportunity for cyber criminals. As businesses invest in digital transformation, the internet and cloud have become indispensable to many organisations and their supply chains. Security teams have to work much harder to verify the technologies they use across their organisation as well as validate their supply chain safety, as the increased attack surface highlights weaknesses and creates potential gaps.

With the distribution of workforce, machines, data, assets, apps and devices across new and exposed gateways, we've all had to change the way that we think, work and behave.

In 2022,

**31%**

of UK businesses and

**26%**

of charities estimated they were attacked at least once a week.

2022 Cyber Security Breaches Survey

## Matching the threat with innovation

To meet the escalating threat, technology, working practices and security protocols have developed quickly, and the speed of response is as critical as ever. Alongside rising consumer expectations, the need for continuing transformation, addressing escalating costs, and complex supply chain issues mean that organisations have had to invest in new systems and skills, while facing difficult economic circumstances.

Yet as soon as existing gaps are closed, new ones reveal themselves. Digital transformation brings huge benefits to our working practices but also exposes organisations to new risks. The rise of generative AI will add increasing sophistication to cyber threats on all fronts. We're faced with the inescapable conclusion that we need to stay ahead of the hacker's continuous innovation in order to survive.

With the huge increase in the number and type of security threats – identity theft, ransomware, phishing scams, malware, DDoS – the risk of attack is rising. But less quantifiable and possibly more dangerous is the cost to reputation from the hacking of personal details or the downtime resulting from a successful attack.

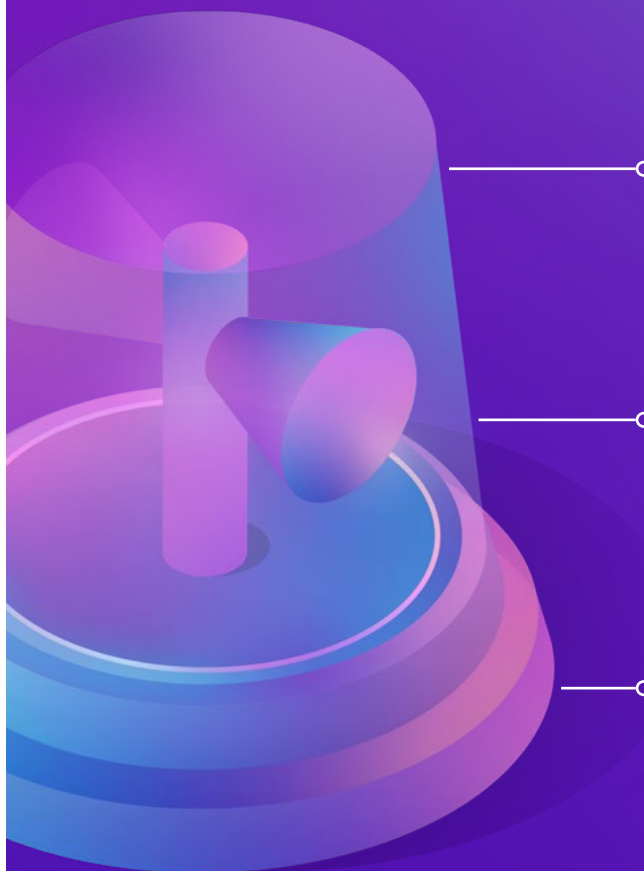
Protection against data loss and breaches is the top priority for

 **51%**  
of organisations

Sapio Report, BT Global Cyber Security Research, May 2023

## The foundations of a cyber conscious culture

Embedding a cyber conscious culture relies on bringing together three foundational building blocks. These building blocks form the basis from which to drive the necessary transformation across an organisation:



### Quantifying and understanding cyber risk

Application of proven methodologies to determine risk exposure and potential impact.

### Building a culture of cyber security

The understanding and quantification of cyber risk clears the way to bring together people, processes and technology to secure an organisation from the inside.

### The journey towards zero trust

With the first two foundational elements in place, a zero trust mindset can help organisations identify the right strategies, technologies and behaviours to embed zero trust into their business wide processes and customer service programmes.



## Optimising the outcomes – our point of view

We know we need to be better able to identify and mitigate ever-evolving cyber threats and to better equip and train our people to recognise these new threats. And we're also all looking to zero trust as a supporting strategy on our path to better authenticate, continuously validate and confidently secure our business, inside and out.

### What we know

Through first-hand experience of protecting our customers and ourselves – championed by the CISO, with the proactive support of the Board, HR, L&D and internal comms departments – together these three building blocks enable a **progressive and joined up strategy**. They support a robust methodology greater than the sum of its parts. And they open the door to embedding a cyber conscious culture that unites people, technology, machines and process.

We'll unpack each of these blocks individually and then examine the power of their combined roll out to help organisations drive effective cultural change and stay on top of cyber security. Understanding cyber risk is the starting point on their journey.

# Understanding and quantifying cyber risk



## Translating fear of risk into positive action

Today, risk is part of everything we all do. But it needn't be a barrier to growth. The right approach to risk can create a cyber conscious culture that informs business strategy and transformation.

As organisations adopt new technologies such as Edge and Cloud to reinforce infrastructure, improve customer experience and streamline operations, they're potentially exposed to more risk.

**“Understanding cyber risk helps the CISO understand the board’s appetite for risk. Understanding where to spend money and how much to spend is a useful conversation to have”**

**Lee Stephens**, Director of Security Services, BT

Every organisation has a unique level of cyber risk. Successfully building a culture of cyber security awareness can be realised by not only understanding, but also by quantifying exactly what cyber risks an organisation is facing. The convergence of network and security is also driving the merging of security strategy with business vision, enabling the move beyond business as usual.

Once a leader knows what they're dealing with – what their unique threat landscape looks like and what individual silos might be compromising their attack surface – they're in a much better position to close the gaps.

A business can use a range of different options to accurately determine the scale of the risk that they face. Consultancy in tandem with tools that interrogate and quantify the risk – in terms of impact to business as usual and to the bottom line – intelligently define the nature of the security threat, degree of vulnerability and likelihood of breach.



**“To address the risks, CISOs need to transition their roles from technologists who prevent breaches to corporate strategists who manage cyber risk.”**

**Peter Firstbrook**, VP Analyst at Gartner



## A shared lens and a shared language

It can be difficult, tedious and sometimes overwhelming to bring every cloud, network, endpoint, system, app and device into a single clear pane of glass view.

We can help organisations understand their cyber risk and put a financial figure on it by viewing their complex threat landscape through a single lens.

Firstly, we help the security leader pinpoint key issues and prioritise their focus, offering advisory expertise and the innovative tools to help them evaluate their threat landscape. The resulting report subsequently enables them to talk to the board in a language they understand. The board may not always understand cyber risk, but they always understand financial and reputational risk.

We've developed a number of tools which can help our customers identify their risk and vulnerability. They've worked well for harnessing our own cyber conscious culture. They include:

- **BT's Security Advisory Services** to frame and understand the nature of risk.
- Dedicated resources such as **SAFE (Security Assessment Framework for Enterprises)** to carry out a tailored security health check.
- The use of **our own threat intelligence** to create Threat Priority reports with detailed reporting offering recommendations for action and investment.
- Our sophisticated **cyber defence platform Eagle-i** which combines our network insight with automation to predict, detect and neutralise security threats, helping organisations optimise their capabilities and spot any holes in their defences without having to replace existing investments.

With appetite for risk identified, security leaders can confidently push for the level of investment they need. Increasingly an accurate cyber risk score is also needed to get a favourable rate from the insurance provider.

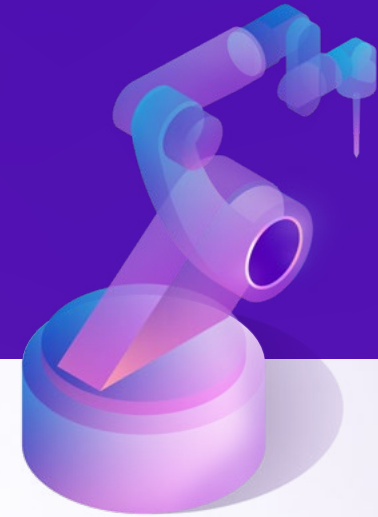
De-mystifying or un-masking the very real risk is the first step to managing it.

**Suddenly security's a business enabler – saving money, streamlining operations, supporting secure network transformation, and bolstering hybrid working.**

By understanding, measuring and addressing any weaknesses across their attack surface, organisations can harness that intelligence to build a culture that prioritises cyber security.



# Building a culture of cyber security



## Defence in depth



Cultural change is hard. It needs personal buy-in from everyone across the organisation, from the top down. In short, it needs board-level leadership and workplace buy-in. The CISO or security leader is the obvious sponsor for change.

Given increasing boardroom investment in cyber security, today the effective CISO isn't just a security expert. Breaking out of the silo, they're much more focused on strategy and risk. In addition to boardroom aptitude, they demonstrate the key skills of leadership, change management and the ability to develop and nurture relationships.

Today 91% of CISOs report to the full board or a committee. With a place at the top table, a close working relationship with the CFO, and stronger links with HR, L&D and internal comms departments, 80% agree that they're now able to invest in the leadership and development needed to build or enhance team capabilities.\*

Establishing cyber conscious behaviours at the core of an organisation also needs the buy-in of the board, individual departments and every member of the workforce. Comprehensive alignment with corporate goals and investment in shared outcomes enables the CISO to successfully make this cultural change.

---

By 2025,

**40% of boards**  
will have a member who is a CISO  
or who comes from a cyber security  
background, up from 10% in 2021.

**Gartner**

---

# 35%

of IT decision-makers said security awareness is one of their biggest cyber security pain points.

**Sapio Report**, BT Global Cyber Security Research, May 2023



## Employee engagement holds the key

Humans are unpredictable and their behaviour isn't uniform. When it comes to cyber security, people rather than systems are the most vulnerable aspect of every organisation. Our own employees adopt the principle of the human firewall: people create the first line of defence at the edge of our network and need to both be vigilant and practice good cyber hygiene.

Fostering employee engagement with effective training is a good starting point to address any potential lack of cyber awareness. By sharing stories, highlighting how owning up to individual mistakes is better than hiding away, making flagging issues or concerns easy, and rewarding those who put security first, the CISO can build trust among the workforce and get the business ready for a deeper level of cyber resilience.

Over a 12-month period, ransomware attacks affected 73% of UK organisations.

**2022 Cyberthreat Defense Report**

Social engineering – where criminals manipulate people to retrieve sensitive data, account credentials, or gain access to networks or systems – plays a part in over 90% of attacks. With ransomware becoming one of the biggest threats that organisations face, it's important to convey the personal impact that every employee can have – whether that's helping it to thrive or inadvertently exposing it to significant financial or reputational damage.

Creative use of behavioural psychology, using the same capabilities that threaten all of us, are useful tools in the CISO's armoury – bringing awareness, collaboration and personal accountability. The good news is that phishing, which accounts for 20% of all data breaches, can be used for cyber awareness programmes; in fact it's often the ideal method to validate the effectiveness of security awareness training, as evidenced by our own 'Don't feed the Phish' programme. De-mystifying and harnessing the power of AI/ML for good is behind some of the other social engineering initiatives practised by our own internal offensive security team who have an ear to the ground and listen to the chatter from the dark web. Central to this is our CISO and his team, working with our L&D teams to drive training that's measured, tested and embedded in the day-to-day.

# 93%

of users who had demonstrated certain unsecure behaviours were aware that their actions would increase risk to their organisation.

**CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework**

---

**“Your employees can be your biggest asset or your biggest liability. With the right culture, awareness and training, they will become your greatest defence against cyberattack.”**

**Tristan Morgan**, Managing Director, BT Security

---

The training we offer our own employees in how to deal with any form of phishing, scamming and other increasingly sophisticated attempts to get through the corporate cyber security walls can also help secure their personal interactions beyond the workplace. They can apply the messages and practical steps to their own personal data protection and also extend these to their family and friends.

---

**“Ethical hackers think differently to the rest of us, and love nothing more than running amok trying to find the holes, gaps and issues so we can improve security overall and that rising tide lifts the organisation as a whole.”**

**Lee Stephens**, Director of Security Services, BT

---



**We block 17 million SMS spam and phishing messages per month.**



## Secure by design

At BT, our agreed security protocols are non-negotiable. Yet, it's human nature to find workarounds if the experience isn't frictionless. While organisations are focused on minimising any tension on their customer and employee journeys, they also need to keep their people safe. Single sign on and biometrics help speed up user access, and innovations to further reduce friction and enhance security are already in the pipeline. At Adastral Park, home to BT's global Research and Development centre where we trial and showcase new technology, we're

working on the truly innovative concept of continuous authentication, seeking to authenticate users by assessing their behaviour patterns on an ongoing basis.

Beyond the immediate working environment, organisations need to develop cyber security protocols that extend across their entire ecosystem – to involve and protect their workforce, suppliers, and customers. Effective CISO-led, board-backed and HR driven cultural change embeds security into its foundations, so that it's simple and straightforward – a methodology of 'secure by design'.

**“We need to do everything that we can to keep people safe without putting gates in their way. We need to bring behaviour and security protocols together and ease of use has to be the priority.”**

**Lee Stephens**, Director of Security Services, BT



A Gartner survey conducted in May and June 2022 among 1,310 employees revealed:



of employees have bypassed their organisation's cyber security guidance in the past 12 months.

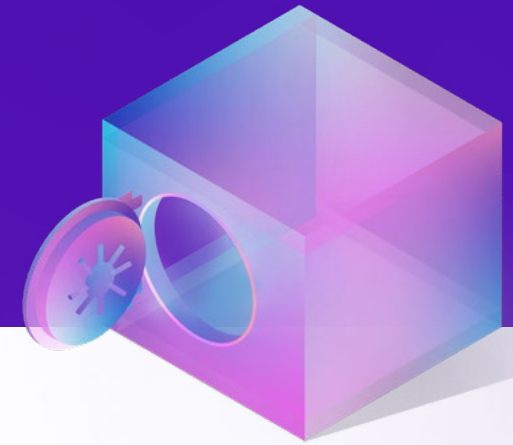


said they would be willing to bypass cyber security guidance if it helped them or their team achieve a business objective.

Gartner

By making security everyone's business, the CISO is fast becoming the ambassador for trust at a time when the concept of zero trust is on everyone's lips – the next step on our road towards the cyber conscious culture.

# The journey to zero trust



With the previous building blocks in place – business strategy, culture, people and process working in harmony as a unified defence – organisations can now confidently extend and protect their borders by harnessing zero trust.

## A journey not a destination

Zero trust is not a box to be ticked, an end state or a product to be bought. Instead it's a collection of concepts, ideas, and component relationships or architectures. Often affected by legacy network limitations, it's an ongoing journey for every organisation to find the zero trust protocols that work. And keep working.

## But what exactly has zero trust to do with culture?

Zero trust is more than a purely architectural concept. It's a key element of our three foundational building blocks, and is ultimately there to authenticate and protect users – both inside and outside an organisation. Thoughtfully applied, it creates a positive user experience, working symbiotically with wider business purpose. With other foundational elements in place, zero trust provides an empowering line of defence.

The collective move away from the office to hybrid and remote working led to teams creating their own security tactics, driving a new layered, consolidated approach to security. Zero trust is all about verifying before trusting and verifying again at every security layer. It supports the defence in depth that's fundamental to effective cyber security strategy.

If organisations can identify the right approach for their business, zero trust can bring efficiencies and more value by automating some of the labour-

**“60% of organisations will embrace zero trust as a starting point for security by 2025. More than half will fail to realise the benefits.”**

**Build a Cyber Security Strategy | Gartner**

intensive tasks that distract our cyber security professionals from the high value tasks that really protect us.

## Effective zero trust strategy

However, zero trust can be a huge investment, especially for the (many) organisations that can't afford to update their files, systems or processes, and don't have the manpower to carry out the compliance audits needed. Unsurprisingly, most

can't afford to start from scratch, and the prospect of ending up with a hybrid or a half-baked solution which doesn't work is a real one.

Continuous monitoring and management of assets is a critical step on the journey towards effective zero trust, supported by an agile strategy which helps different technologies talk to each other and bring more value. An effective zero trust solution authenticates and protects users, so they can't move through the network without being caught at various gates.

How can organisations make zero trust work for them? Again this is where a culture-first approach, can play a critical role – ensuring our journey to zero trust becomes a journey to success. By identifying one business case and designing a zero trust strategy around it – keeping the user journey front of mind – they can create a contained model to test and streamline before scaling.

---

**“Businesses need to better understand zero trust before putting their hands in their pockets and investing. To channel the right expertise and resources into areas and projects that make the most difference, organisations need to transcend this buzzword and prepare themselves for the realities of a perimeter-less IT environment.”**

**Tristan Morgan**, Managing Director, BT Security

---

**“If an organisation can leave the tedious, mundane tasks to a trusted service provider that will take care of it using tools and automation, it will free them up to do the things that are fundamentally more important.”**

**Lee Stephens**, Director of Security Services, BT

---

### **We've developed a four-step roadmap to help our customers develop an effective zero trust strategy:**

**1**

**Hold a business conversation about a specific business challenge and how zero trust can resolve it.** This might be something as simple as poor performance of the corporate wi-fi or rogue printers which prompt risky user workarounds – such as emailing work home – immediately exposing organisations to breach.

**2**

**Ensure basic security hygiene measures** – such as identity, segmentation and endpoint protection – are properly set up. This is one of the most important aspects of a layered security approach.

**3**

**Understand exactly what needs to be protected** – people, applications, data – across servers, devices and cloud environments.

**4**

**Identify a specific use case to try out the selected zero trust methodology**, then refine and retest to improve outcomes, ease of use, and visibility and access.

**Trust is an iterative process. So once the first business case has been tackled, organisations can learn, refine and test before moving on to the next.**

---

**‘Zero trust isn't a destination, it's a journey – and importantly, you don't have to do it alone.’**

**Tristan Morgan**, Managing Director, BT Security

# Bringing it all together – our methodology



“Developing the right culture is a continuous process. It takes time, investment, and buy-in from senior leadership. You can encourage behaviours that create the right cyber security culture. You can’t simply ‘change’ a culture to create the right behaviours around cyber security. Culture is an outcome, rather than an input.”

NCSC

With the CISO in charge, supported by the Board, the wider business and every staff member, your organisation can bring together these three building blocks – quantifying and understanding cyber risk, building a culture of cyber security, and embarking on the journey to zero trust – to create a powerful cyber security conscious methodology that optimises the outcomes for every organisation that joins us on this journey.

## Applying our methodology




By harnessing this methodology, we can uniquely tailor our solution to every organisation’s unique business needs. Our approach is underpinned by the strength and depth of our long-established – and agnostic – managed security services.



## Bringing our methodology to life

Every organisation can enhance this approach with some practical initiatives for their own business by:

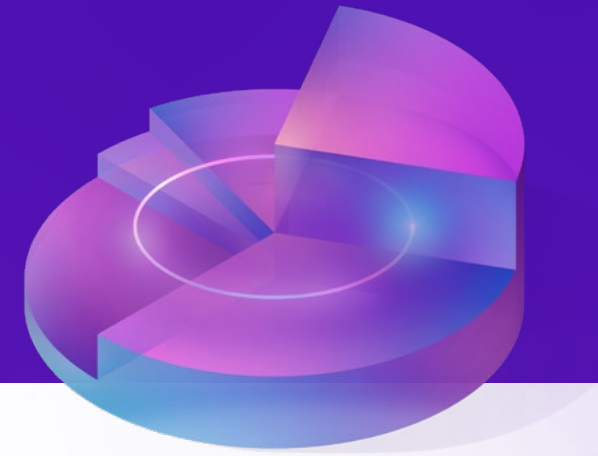
- 
-  Incorporating security measures onto the individual score card of every role.
  -  Building security awareness into every job specification.
  -  Testing and behaviour analysis of internal cyber awareness activities to determine what works and what doesn't.
  -  Making security one of their core cultural values, underlining the collective commitment to prioritise safety and security, and our mutual need to protect one another.
  -  Introduce regular annual cyber awareness training for all staff.
- 

These measures can help ensure everyone's accountable and committed to meeting their specific security targets, lay down strong security protocols, and identify what needs to be tightened up, extended or replaced. Together they can drive the cyber secure behaviour every organisation needs, realising a vision of the future in which commitment to cyber awareness and practice of robust cyber hygiene is the norm, for everyone.

For the CEO and the board in particular, their high profile positions make it easy for hackers to extract a lot of data and use it to develop fake, targeted messages. With every senior leader properly equipped to understand and actively support their cyber secure culture – setting the visible benchmark for their people, suppliers and customers, they're much better positioned for cyber secure behaviour to permeate every aspect of their business.



# Conclusion



## The business of transformation, innovation and growth

Most organisations are aware of all the things they need to do. But with ever-evolving threats, tighter budgets, skill shortages, growing hacker expertise and the increasing sophistication of AI, they've got an ongoing balancing act just to keep the lights on. All of this can be a distraction from developing the growth and innovation behind a cyber conscious culture.

Although the CISO's focus on bringing security strategy in line with business outcomes is a huge step towards embedding a cyber conscious culture, many organisations struggle to keep up with and implement the ever-evolving security protocols and regulations. The situation is made worse by the shortage of top talent and constant barrage of cyber attacks. Different regions have different obligations which makes compliance even more taxing.

The threat is constantly evolving, but so are the available, skilled resources to address it. As machine intelligence adds new sophistication to cyber threats, a move towards flexible managed security services can more strongly repel the threat.

Organisations no longer need to rely on their own internal capabilities and solutions to successfully embed a culture of cyber security.

Partnering with a managed security services provider can be a lifeline as they:

- Bring the depth of innovation, cutting-edge skills and tools organisations need.
- Take the strain of the daily fight against cyber attacks.
- Support automation of time-consuming manual tasks.
- Reduce human error.
- Free up IT resource at a time when skills are in short supply.
- Enforce consistent security protocols.
- Co-manage areas where they need additional support or augmentation.

**“We’ve tested all the solutions that we sell, and we use our own products to protect BT. We know what they actually do. Our own experience and learnings mean we know how to drive customer success.”**

**Deborah Moir**, Principal,  
Security Advisory Services, BT

As a trusted partner to our customers, we understand and share their challenges. We can help them adopt the right methodology and practices to manage their risk, and get on with the business of transformation, innovation and growth.

# Why BT?

## Our security sets you free



At BT, we bring together innovation, technology and our own advisory capabilities to identify vulnerabilities and create practical, powerful solutions which demystify cyber threats and security for all of our people.

Our ambition is to become the world's most trusted connector of people, devices, and machines. We have the technology, the intelligence, the people and the deep expertise to spot and tackle cyber security threats before they become the stuff of headlines and the destroyer of reputations.

### Every month we:

- ✓ Detect around **two billion malicious events** on our network.
- ✓ Deter **seven million international spam calls** that spoof UK numbers.
- ✓ Automatically **block 700 million phishing emails** and links for our broadband customer.
- ✓ **Repel 17 million SMS phishing** and spam messages.
- ✓ **Remediate 6,000 DDoS attacks** on us and our customers.

---

**‘We use data intelligence from the Security Operations Centre. It helps us see how data and cyber threats move, where they propagate, who they target and how they impact. This is one of the ways we devise protection of our security customers from cyber threats.’**

**Tristan Morgan**, Managing Director, BT Security

---



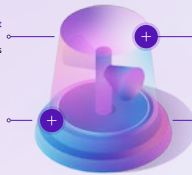
# Embed a cyber conscious culture in 5 simple steps

Our tried and tested five step guide to driving cultural change across your organisation



## 1. Understand your cyber risk

View your complex threat management landscape through the single lens offered by BT Security Advisory Services



Assess your unique security threat, degree of vulnerability and likelihood of breach

Examine every aspect of the landscape – cloud, endpoint, system, app and device – to understand everything connected to your network and identify vulnerabilities

Prioritise your security touchpoints and necessary spend with a security health check and a roadmap for change

Did you know? +

## 2. Align your security strategy with your business strategy

Translate your identified cyber risk to financial risk and talk to the board in a language they understand



Position security as a business enabler – saving money, streamlining operations and freeing up your people to focus on business growth

Make a business case to the board for the investment you need, based on your appetite for risk and prioritised spend



With clear understanding of your risk, secure buy-in for your required security investment

Top tip +

## 3. Ensure cyber security is everyone's business



Appoint a senior security leader with change management skills, the ability to nurture relationships and the drive to lead from the front

Bring your HR, L&D and internal comms departments on board to help develop an open culture where employees are supported and engaged



Harness cyber awareness training and hacker techniques, like faux phishing, to embed the human firewall approach and drive personal accountability among your employees

Create frictionless security protocols that speed up user access while keeping your workforce and your customers safe

Common pitfall +

## 4. Make robust security the baseline on your journey to zero trust

Identify your business drivers  
[Learn more >](#)

Establish security hygiene  
[Learn more >](#)

Know your landscape  
[Learn more >](#)

Test, iterate, scale  
[Learn more >](#)

1

## Understand your cyber risk

View, understand and quantify your unique threat management landscape.

2

## Align your security strategy with your business strategy

Translate your identified cyber risk into financial risk and leverage right risk thinking as a positive enabler for transformation.

3

## Ensure cyber security is everyone's business

Integrate people, tools and processes to develop employee accountability, reduce user friction and enhance security touchpoints across your estate.

4

## Make robust security the baseline on your journey to zero trust

Understand the business needs that drive your security strategy, embed security hygiene and identify the zero trust methodologies that drive growth for your business.

5

## Choose a managed security partner that sets you free

Monitor, authenticate, outsource and automate your security protocols to focus on improved business outcomes.

An integrated approach can bring people and processes together with the best of innovative technology. Based on secure, flexible foundational principles and intelligent consultancy, managed security services from BT can open up new opportunities for you to protect, innovate and grow your business.

Find out more by downloading our **Five Steps Guide to Embedding a Cyber Conscious Culture**.

# Start your journey towards embedding a cyber conscious culture today.



Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

© British Telecommunications plc 2023. Registered office: One Braham, Braham Street, London, England E18EE. Registered in England No. 1800000.

October 2023