BT

It’s time to make security integral to your business. Here’s how.

Threats to your business are going nowhere

Billions of devices connect to the internet every day with little or no security. At the same time, cybercriminals are arming themselves with sophisticated and innovative malware. The threat to your business remains high and it's going nowhere. Attacks can happen to anyone, or any business, at any time. No system or network is 100 per cent secure.

It's your job to protect your company against threats like these. Many execs treat security like a static problem. They view each business unit or technology platform as a separate entity, which can lead to inconsistent security with dangerous gaps. Some still see the public cloud as unsafe and miss out on all its advantages as a result. Or they assume the cloud provider they choose is responsible for making everything safe, which can open their business up to attack. Others buy specific products in response to the latest known threats, creating a fragmented web of different programmes.

Too many businesses think security is a fixed problem that's simply solved by technology. But the opposite's true. In the words of Facebook CEO Mark Zuckerberg: "Security isn't a problem that you ever fully solve."[1]

> "Many high-profile breaches show signs of significant planning by attackers who carefully identify weak packages and tools on targeted servers before making a move."[2]

Security – just like learning – is an ongoing process

At some point, you will be breached. And when that happens, you'll have to move fast to contain the problem and repair the damage. If you can't, you risk damaging your brand, losing IP, your people will appear less credible, and of course it can stop your progress in its tracks. Worse yet, if you don't react fast, others in your business might buy and use their own security systems, creating what's known as "shadow IT" – and that means even more risk for the business.

You must treat security as a part of your strategy that's always evolving and work to improve it as threats shift and your needs change.

So, how do you do this? First you've got to map your desired business outcomes against the network and systems you already have. Then you need to look at your security requirements. What do you need to protect? Where are your gaps? What controls and actions do you need to protect yourself? Next, look to strategically outsource activities, so your staff – the people who know your business best – have more time to see what works and fine-tune your security strategy as you go along.

Stop wondering and start doing

What if you could:

- Be confident that your cloud decisions were rooted in your security strategy?
- Know where to align your defences to send resources?
- Continually improve your security?

If you work with us, you can.

You'll be able to make security central to your business by understanding your current security strength and how it measures up against the likely threats you'll encounter. You can then use these insights to create the right balance between your internal staff and outsourced resources. At the same time, you can make sure your security policies are consistent and in use, no matter what your network environment is like or where your apps and data live. And you'll easily be able to keep up with latest attacks around the world, as well as discover the most effective means to prevent and fix any intrusions you might suffer.

Here's how...

Challenge: Moving to the cloud

If you're like most CIOs or CISOs, you'll want your business to make greater use of the cloud, but each new platform you use can make things more complex and put you at greater risk. And if your organisation is adopting software-defined networks because you need more bandwidth, you could be creating even more weaknesses without realising it.

You're stuck between a rock and a hard place: if you assume the public cloud is safe you could expose your organisation to risk, and if you assume it's not, and you don't use it, you can fall behind your competitors.

One thing's certain: if you don't move to the cloud fast enough, other parts of the business will – and that can create problems for you. Whether it's exchanging files on an unsanctioned Dropbox account or creating entirely new applications, you risk losing control to shadow IT.

> "77 per cent of CISOs working with BT are actively moving to the cloud or planning to adopt cloud services. Of these, 71 per cent said they have some policies, but 30 per cent admitted they don't understand what they are."

Solution: Make cloud decisions based on your business needs

With our monitoring and policy enforcement service, you'll be free to choose the cloud provider you want, without worrying about compliance or where your apps and data live. You can rest assured your business is protected because we've tested our services in one of the most demanding environments there is – our own global network. So you can meet the demands of regulators while enhancing your organisation's ability to innovate and stay ahead of the competition.

- **Make the most of your existing security investments to build the right cloud solution for you.** With us, you'll have an integrated network and security environment you can use across the globe. We'll be the only people you need to turn to for answers. And with our cloud services, you no longer need to invest in on-premises equipment, simplifying your set-up and saving you money.
- **Cut the risk of moving to the cloud.** We thoroughly vet third-party products so you can trust them. That means you don't have to guess whether the individual elements in your security portfolio will work together. Choose the cloud platform you want – AWS, Azure or other public clouds – without weakening your security.
- **Move to the cloud at your own pace.** Now you can maximise mixed environments and evolve them over time as the business demands. You'll know where your data is stored at all times – and how it's transmitted – so you can meet data sovereignty and compliance requirements. Plus, you can move workloads based on your business without being rushed into the wrong environment because of security concerns.

Read more about how to secure your business from network to cloud.

Challenge: Doing enough to protect your business and comply with regulations

Post-GDPR you have to do more to play by industry rules. You also have to compete against a backdrop of geopolitical uncertainty, data divides between countries and a growing number of attacks. Guarding against these attacks is no longer enough. You must respond fast and within the rules laid out in your industry. Is your approach good enough and can you prove the effectiveness of your efforts?

For many organisations, there's a gap between their known set-up and their actual infrastructure open to attack. Even a basic level of system organisation is difficult when you don't know all the devices connected to your network, how your data is stored and managed, or what security gaps your supply chain is creating.

Without a full understanding, it's impossible to put the right controls in place, stop attacks, or even develop the required skill sets to protect your business. And without confidence in the strength of your security, it's hard to move forward.

> "Although 97 per cent of organisations we surveyed have experienced a breach, only around 20 per cent believe they are equipped to deal with intrusions effectively."

Solution: Know where to align your defences and send resources

Stop straddling the line between too little and too much. Take a step back and assess your strengths and weaknesses. We'll help. Start by taking stock of your set-up and – using the latest advances and tested solutions we've learned from our customer base – build the policies and controls you need to protect what's important to your business. By outsourcing basic tasks, you can reallocate your staff to more strategic activities, putting their knowledge of your business to better use. When you partner with us, you can:

See your whole infrastructure.
Through our 15 security operations centres across the globe, you'll have a complete view of your security health and be able to report on where you're most likely to be attacked and your current defences against likely intrusions.

Know what you need to protect – and how to do it.
By using our tips – including activities such as ethical hacking – you'll understand your greatest weaknesses and how effective your methods are. We have a large client list and strategic partnerships with world-leading security vendors – and we'll use them all to help judge your security strength.

Make sure you're compliant quickly.
We can help you create a proven, disciplined process to assess your level of compliance and figure out how to plug any gaps. Our team will help you stop spending valuable time scouring numerous and often conflicting sources for regulatory updates.

Find out if you're doing enough to secure your business.

Challenge: Staying ahead of changing threats

Threats to your business are always evolving. The internet has spawned new commodities and marketplaces – from stolen passwords to ransomware – for highly-motivated criminal entrepreneurs to monetise. Increasingly innovative attacks, targeted at specific organisations has seen signature-based detection become less and less effective.

Sometimes threats can come from things beyond your control. Organisations in your supply chain may open gaps you can't spot. Not all attacks will be caught at the firewall. Detecting sophisticated intrusions once they've occurred - and then fixing them without disrupting your business – is critical. Falling short means you risk losing ground to a more prepared rival.

Solution: Continually improve your security

We can help make sure you stay on top of the latest discovered threats, so you can spot whether your network and systems are under assault. If you're breached, you can contain and fix the intrusion fast and effectively. And you'll be able to do this in a fraction of the time if you were to try assembling point-products on your own.

By working with us, you will:

- **Respond before new dangers become an issue.** Spot new intrusions to your network and systems and know about new threats before they reach you – in the cloud or in your internal environment. This early warning gives you more time to isolate and solve problems, cutting any potential damage.

- **Fix attacks faster.** Thanks to our scale, client base and relationships with law enforcement and cybersecurity authorities, we're often the first to spot new trends and learn of new attacks. We protect ourselves against thousands of attacks each day – and that just makes us better at spotting and stopping them. We publish what we learn in our Daily Threat Intelligence report, which you can use to stay up to date.

- **Analyse suspicious behaviour to discover new threats.** Our artificial intelligence and machine learning programmes sift through millions of events per second and uncover strange activities. You can use this and our experience to hunt for threats, catch not-yet-defined attacks and then stop them before they start.

Discover how to stay ahead of changing threats.

Proven results

Before working with us...	After working with us...
Nationwide wanted to take a fresh look at threat management to keep information secure as members increasingly use more digital services along with traditional channels.	Nationwide can now give customers more personalised services on the move. The company's security is covered at every stage – from design and implementation to 24-hour proactive and reactive monitoring.
Hotelbeds Group wanted to expand its capacity to keep the entire operation secure while managing hundreds of millions of online transactions every day – a number that continues to grow.	Hotelbeds has near-limitless capacity and the assurance that our security products and experts are keeping cyber-threats at bay. Their websites are now protected in the cloud from denial of service attacks and it can move and redirect traffic in case of cyber-attack.
Noble Group wanted to realign its worldwide infrastructure. As a commodity trader its business revolves around real-time, online global trading, so it's crucial to have a secure and dependable network. Its challenge was to find a business partner that could safeguard its network in Asia and every other place they operate in around the world.	It's protecting vital information across the globe and probing its network to test for vulnerabilities, which means it can fix any issues long before they become a problem.

Let us protect your business, the way we do ours.

We're helping customers thrive by delivering world-class security solutions. We have operations in more than 180 countries and support some of the world's largest companies, nation states, and critical national infrastructures. That gives a unique perspective on cybercrime. Our team of 2,500 security experts in 15 global centres use unique tools and insight to stay one step ahead of criminal entrepreneurs.

We're constantly watching, learning, predicting, and responding to the latest threats to protect our customers. Join us and you'll be protected too.

To learn more, visit **bt.com/security**

[1] Mark Zuckerberg quoted in Facebook Has a Problem That Not Even Mark Zuckerberg Can Solve, Chris Cillizza, CNN, March 21, 2018
[2] 2018 Trustwave Global Security Report, Trustwave Holdings, 2018.
[3] Taking the Offensive Report, BT and KPMG, 2016.
[4] Taking the Offensive Report, BT and KPMG, 2016.