

The new culture of security




inner circle

Protecting your  
data, your  
brand and your  
business in the  
age of mobility







Of course, you take cyber security very seriously. It's a top priority for all big organisations. It's odd, then, that we're still hearing of catastrophic data loss, affecting some of the world's most respected brands. Perhaps cyber security is not quite as high on the boardroom agenda as it ought to be.

At the September Blue Door event, Tom Mullen, Head of Cyber Response for Telefónica UK, gave the gathered executives a salutary lesson in corporate cyber security. He highlighted the elusive nature of the threats and the biggest challenge you face when implementing your security strategy: getting your people to take it seriously.

It may be as simple as a statement from the CEO, making it clear that cyber security is one of the organisation's most important priorities. The key point is that there must be no doubt about how seriously the organisation takes questions of security.

But even the most charismatic CEO can only have so much impact. You have to top up the message regularly. Complacency creeps insidiously into everything, and busy people can easily let their guard down.

#### **Minor breaches matter**

One of the most effective ways of doing this is to highlight minor breaches when (not if) they occur. Making an example of the employee involved may be an overreaction, but gently pointing out what has happened just nudges the need for vigilance back up the priority list. At least for a while.

Spotting these minor breaches should be relatively easy if you have all your security safeguards in place. It doesn't have to be complicated. Basic defences such as firewall protection, anti-virus, server-patching and intrusion prevention will be enough to flag any number of potentially harmful breaches.

The alarming thing is that some of the more high-profile incidents reported recently show that the basics are not always in place. Often, what began as an almost impregnable suite of defences is not properly maintained and vulnerabilities begin to appear. The first you hear of it is when a canny hacker siphons off thousands – or millions – of valuable customer records.

#### **Understand the real risks**

In some organisations, there is an inclination to accept breaches like these as inevitable. They assess the likelihood and possible impact of an incident against the cost of putting adequate protection in place, and decide that the risks are worth accepting.

The logic is that cases are being reported so regularly these days that people take them for granted. Customers will not judge an organisation too harshly if it's hacked; it's just one of the inevitable hazards of living in a connected world.

It's a dangerous strategy. And it's usually based on a less-than-adequate understanding of the real risks.

Financially, the consequences of serious breaches are about to get much worse. In the EU, your organisation can be fined 2% of its gross annual turnover – note, it's the gross – which is set to rise to 5%.

#### **Protecting customer trust**

But even that swingeing cost can pale before the catastrophic damage to public trust that can befall you. In highly regulated sectors such as financial services or healthcare, any hint of vulnerability can compromise client relationships irretrievably.

For a cool technology brand, a hole in the security system can be acutely embarrassing. It calls into question the technical acumen of the business and, worst of all, strips away the patina of street credibility on which so much of the corporate reputation may depend.

These less tangible consequences can have far deeper impact than a huge, high-profile fine. A hard slap from the regulator might make the share price wobble for a bit; a loss of customer confidence might cost you the business.

All this assumes, of course, that the threats are real. While even the most stubborn of security cynics will acknowledge that viruses and other malware need to be kept at bay, they will argue that the chances of a serious breach are negligible.



Cultural change has to come from the top. If you want to embed security consciousness into the everyday routine of your organisation, then your CEO and the rest of the C-suite have to lead by example.



### Spotlight on dark web

A glance at the dark web, or deep web, may be sufficient to illustrate the true nature of the risks. For example, if you want to rent some hacked servers to run a botnet for a few hours, you'll be pleasantly surprised at how cheap the going rate is. Ideal for a disgruntled employee who wants to harm your organisation, or for a consumer group with a hostile agenda.

More significantly, organised criminals are leading the way in the evolution of cyber crime. As master business people in their own right, they have recognised that the risks and rewards of online crime are far more appealing than crime committed in the physical world. Why rob a bank at gunpoint when you can simply buy a few thousand stolen account details and pick your way in from the comfort of your moll's chaise longue?

### Publish and be safe

Still, you can spare yourself any despair. For all the threats circling your organisation, there are well-defined steps you can take to mitigate the worst of them and eliminate the rest.

Publishing your policy and issuing gentle reminders will help to remove any confusion there may be about what is expected of your employees. They need to know what constitutes a breach, how to tell when they are at risk of infringing the policy and what to do to prevent any harm.

They also need to know that if something does go wrong, then their first responsibility is to alert everyone that needs to know. For this to happen, they need to understand that recriminations will not be on the agenda, unless they have been blatantly negligent.

As with any culture change, fear is far less effective than education. The more people understand, the easier it is for them to buy in to what's required of them.

A good strategy for keeping security on the daily agenda is to appoint champions in each department, who can be the first points of contact in the event of an incident. They can also be the conduits for any updates that need to be communicated. It's better coming from a colleague than from those anonymous folk in the depths of the IT department.

### Coping with cloud and BYOD

Two other key factors have emerged as critical security concerns: the rise of bring-your-own-device (BYOD) and the emergence of cloud. These two phenomena share the underlying characteristic of mobility. For security-minded people, the challenge is becoming less about securing fixed points, or even devices, and more about protecting data in the wild.

A key line of defence in this liberated, agile world is to regulate installation, rather than downloads. Your policy can give employees enough freedom to access the resources they need on the move, while still protecting the infrastructure from the invasive danger of a rogue app.

Mobility and agility are becoming essential capabilities for today's enterprises. This makes end-to-end security a positive business enabler, not just a necessary constraint. If your security deployment allows employees to work freely wherever and whenever they need to, your organisation can get the full rewards of productivity and lower costs that flexible and remote working can deliver.

### Essential agility

The analogy of the knights of old expresses the notion nicely. A full suit of heavy armour may have afforded plenty of protection, but it made the wearer clumsy and slow. They learned that good defensive weapons and lighter body protection could actually be more effective.

For today's enterprises, the message is that cyber security is not an optional extra, or a box to tick. It's an essential defence and, more importantly, an asset that unlocks new capabilities of agility and productivity that make you ready to compete in the fastest-moving markets.



To find out more about strategies and solutions for cyber security, and to discuss any of the topics covered here, please contact your account manager or go to [o2.co.uk/enterprise](https://o2.co.uk/enterprise)



